Матеріали і методи. Як показав попередній аналіз, існуючі системи мають певні недоліки (таблиця 1), такі як: можливість реєстрації тільки всією школою, відсутність системи повідомлень, інформаційна перевантаженість, відсутність багатомовності.

На основі аналізу цих та деяких інших недоліків було вирішено розробити нову систему оперативного контролю успішності учнів у школі, яка допоможе вирішити такі питання:

- Ведення електронної звітності успіхів дитини
- Контроль виконання домашніх завдань та успіхів дитини
- Інформованість батьків про шкільне життя дитини та важливі події
- Відображення діаграм успішності
- Простий та зрозумілий інтерфейс користувача
- Багатомовний інтерфейс
- Можливість впровадження системи в окремих класах

Таблиця 1

Аналіз систем-аналогів

Функції та характеристики	shodennik.ua	e-schools.info	www.ukrschools.com.ua	smls.com.ua	Власна система
Система сповіщень про шкільні події	-	-	-	-	+
Батьківський контроль	+	+	-	+	+
Актуальный User friendly інтерфейс	+	-	+	+	+
Система звітності	-	-	-	-	+
Можливість користування у окремих класах	-	-	-	-	+
Діаграми успішності	-	-	+	-	+
Багатомовність	-	-	-	+	+

Завдання,які постають перед розробником проекту:

- Вибір PHP фреймворку для створення web-додатку;
- Установка та налаштування;
- Розробка web-додатку з урахуванням особливостей фреймворку;
- Розробка інтерфейсів користувача .

Результати. За основу ми обрали фремворк з відкритим кодом Laravel. Оскільки він відповідає таким характеристикам:

- Наявність вбудованих функцій , таких як: аутентифікація користувача, маршрутизація, кешування, та інші;
- Можливість доповнювати власними функціями;
- Легкий та зрозумілий синтаксис;
- Можливість інтеграції з сторонніми платформами та бібліотеками;
- Популярність .

Для розробки web-додатку ми обрали такі інструменти:

- Мови програмування PHP, JavaScript
- Бази даних MySQL
- Dompdf - для формування електронної звітності

УДК 004.056.5

СИСТЕМА МОДЕЛЮВАННЯ СЦЕНАРІЇВ ВЗАЄМОДІЇ УЧАСНИКІВ КІБЕРПРОСТОРУ

Ровник О.С., студ. гр. ПІ-151,
Трунова О.В., к.пед.н., доцент
Чернігівський національний технологічний університет

Забезпечення захисту інформації в кіберпросторі в даний час є одним з пріоритетних питань безпеки держави, саме тому воно є актуальним та важливим для кожного підприємства і організації.

27 червня 2017 року, день, що став «чорним вівторком» для кібербезпеки нашої країни. Протягом одного дня комп'ютерний вірус «Ransom:Win32/Petya» атакував приватний і державний сектори економіки України, зокрема банки, аеропорти, державну залізничну компанію, телекомпанії, телекомунікаційні компанії, великі мережеві супермаркети, енергетичні компанії, державні фіскальні служби, органи державної влади і місцевого самоврядування і т. п. Вірусом були вражені також приватні та державні суб'єкти інших держав, але фахівці в цій галузі сходяться в тому, що найбільше постраждала

Україна. Службою безпеки України були прийняті міри, які були спрямовані на захист електронних ресурсів, відновлення роботи закладів та служб, пошуку кіберзлочинців.

Для контролю кібербезпеки та запобігання кібератак, аналізу ризиків та критичних ситуацій ефективним є збір статистичних даних, моделювання таких ситуацій та розробка стратегій для успішного захисту від кібератак.

Важливим питанням є створення системи моделювання сценаріїв взаємодії учасників кіберпростору, яка має стати важливим засобом в процесі моделювання критичних ситуацій у напрямку кібербезпеки, створення моделі прийняття рішень для учасників кіберпростору. Для цього потрібно вирішити такі задачі:

– проаналізувати існуючі аналоги і визначити архітектуру створюваної системи;

– обґрунтувати вибір і застосування окремих компонентів системи;

– розробити програмне забезпечення системи;

– розробити модулі для створення та вирішення критичних ситуацій.

В рамках дослідження виявлено, що програми Infection Monkey, Thretcare, Caldera, дають змогу моделювати атаки, але моделювання є статичним, тобто без урахування прийняття та зміни рішень сторін, які приймають участь у моделюванні. Програма Tabletop Simulator хоч і дозволяє оцінити взаємодію учасників, але не має інтегрованих інструментів для моделювання саме кібератак.

Створювана система має достатньо складну архітектуру (див. рис. 1) і складається з декількох апаратних та програмних компонентів.

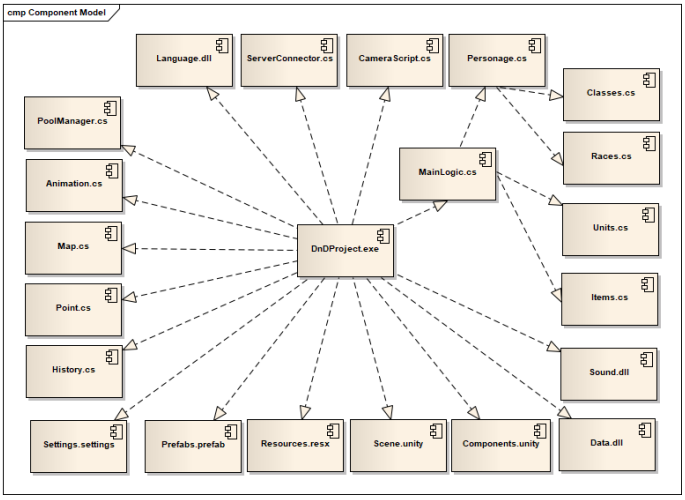

Рис.1. діаграма компонентів системи

Програмний інтерфейс складається з двох частин: меню користувача та простір відображення моделі. Один з учасників створює модель та сценарій критичної ситуації. Інші учасники спільними діями повинні знайти вирішення проблеми за певний час та обмежену кількість дій (ходів). Правила, необхідні для моделювання, повинні бути описані в модулі, який використовується для створення моделі. У залежності від прийнятих рішень обох сторін результатом буде перемога або атакуючої сторони, або сторони захисту.

Програмне забезпечення розроблюваної системи повинно мати універсальний інтерфейс, модульну структуру для додавання нових модулів, повинне забезпечувати можливість зберігання даних створюваної моделі.

Для створення системи були обрані наступні технології:

- Unity 2017 – графічний рушій для створення інтерфейсу системи;
- Photon – сервіс для створення багатокористувацьких додатків;
- мова програмування C#

Оскільки для моделювання ситуацій важливим є не тільки функціонал, а ще й графічне відображення, Unity є гарним засобом для створення інтерфейсу та графічного представлення моделі. Створення префабів та модульних об’єктів взаємодії дасть змогу ефективно використовувати засоби для моделювання подій. Сервіс Photon дає змогу створювати сеанси для проведення сесій, де можуть приймати участь декілька учасників. Оскільки Unity має тісну інтеграцію з Photon, то такий вибір є доцільним. Для написання модулів сценаріїв обрана мова C#. Об’єктно-орієнтована мова дає змогу чітко описати правила сценаріїв, розробити модель та підключити до графічного модуля, оскільки Unity використовує скрипти саме на мові C# для керування графікою.

Принципи, втілені у запропонованому застосунку, можуть бути використані для створення та подальшого аналізу кібератак для запобігання та передбачення критичних ситуацій які виникають у кіберпросторі. Подальша робота може бути спрямована на створення нових модулів, зокрема розробці

нових способів взаємодії між учасниками, додавання та підтримку різних мов, оскільки проблеми кіберзахисту є проблемами суспільства вцілому.

Список використаних джерел

1. 8 инструментов для моделирования кибератак для повышения безопасности [Електронний ресурс]. – Режим доступу до ресурсу: https://itsecforu.ru/2018/12/11/8-инструментов-моделирования-кибератак/
2. Приниятие решений в условия частичной неопределенности [Електронний ресурс]. – Режим доступу до ресурсу: https://studbooks.net/29425/ekonomika/prinyatie_resheniy_usloviyah_chastichnoy_neopredelennosti.
3. Вирус Petya в Украине: Британия официально обвинила Россию [Електронний ресурс]. – Режим доступу до ресурсу: https://fakty.com.ua/ru/svit/20180215-virus-petya-v-ukrayini-brytaniya-ofitsijno-zvynuvatyla-rosiyu/
4. Грабовый А. Закон о кибербезопасности и стратегия кибербезопасности Украины [Електронний ресурс]. – Режим доступу до ресурсу: http://uz.ligazakon.ua/magazine_article/EA010553
5. Защита киберпростанства в разных странах [Електронний ресурс]. – Режим доступу до ресурсу: http://www.inf74.ru/safety/ofitsialno/zashhita-kiberprostranstva-v-raznyih-stranah/

UDC 004.738.5 : 004.77

ADVANTAGES AND DISADVANTAGES OF INTRODUCING IOT DEVICES

Skliarova D.Y., student the group CE-162 ,
Svetenok L.K., senior lecturer
Chernihiv National University of Technology (Chernihiv, Ukraine)

The Internet of Things (IoT) is a network concept consisting of interconnected physical devices that have embedded sensors as well as software that allows transmission and exchange of data between the physical world and computer systems by means of standard communication protocols. In addition to the sensors, the network may have actuators built in physical objects and interconnected via wired or wireless networks.

The main concept of IoT is the ability to connect all kinds of objects (things) that people can use in their everyday life, such as refrigerators, air conditioners, cars, bikes and even sneakers. All these objects (things) have to be equipped with built-in sensors capable of processing the information received from the environment, exchanging it and performing various actions depending on the information received. [1].

According to Statista, over 23.14 billion devices are connected worldwide using IoT technology. Figure 1 shows the number of connected devices (IoT) worldwide from 2015 to 2025. By 2020, the installed base of IoT devices is forecast to have reached almost 31 billion worldwide. [2]

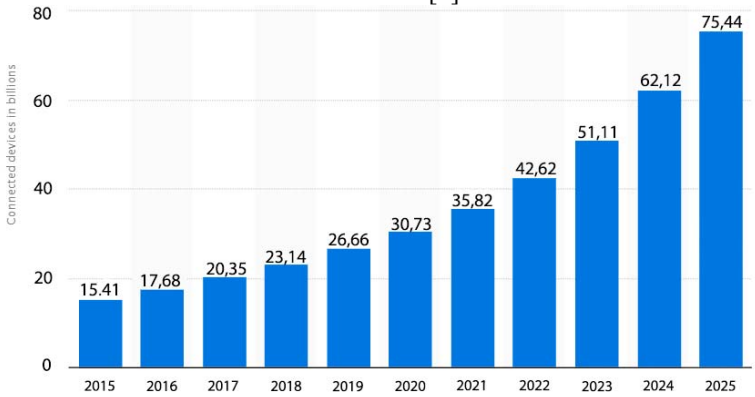

Figure 1. The statistics of connected IoT devices

3 ways of interaction with the Internet things are direct access, access through gateway and access via server.

In the case of direct access Internet things must have their own IP addresses or network alias, accessible from any client application and they must perform the functions of a web server. The interface with such things usually looks like a web resource with a graphical interface controlled by a web browser.

If Internet things do not have built-in support for IP and HTTP protocols, but support private protocols, such as Bluetooth or ZigBee, a special Internet gateway can be used to interact with them.

The third form of interaction of devices in IoT via server implies the presence of an intermediary between Internet things and a user and can be implemented with the aid of an intermediary data platform. This approach assumes the presence of a centralized server or a group of servers the main functions of which include receiving messages from the Internet of things and transferring them to users, storing and processing the received information and providing a user interface with the possibility of two-way exchange between the user and the Internet thing.

A complete system of interaction is displayed in figure 2.