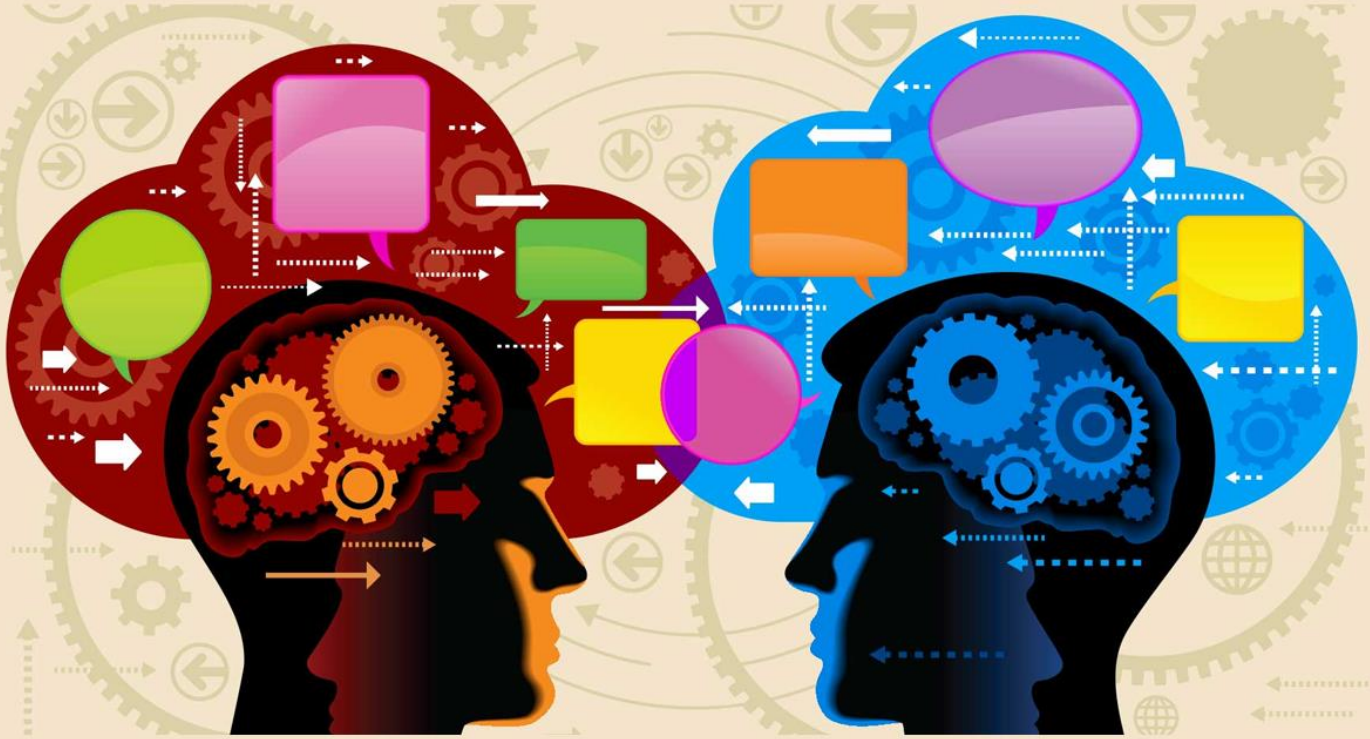
SCI-CONF.COM.UA

SCIENCE, SOCIETY, EDUCATION: TOPICAL ISSUES AND DEVELOPMENT PROSPECTS



ABSTRACTS OF VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE MAY 10-12, 2020

KHARKIV
2020

SCIENCE, SOCIETY, EDUCATION: TOPICAL ISSUES AND DEVELOPMENT PROSPECTS

Abstracts of VI International Scientific and Practical Conference

Kharkiv, Ukraine

10-12 May 2020

Kharkiv, Ukraine

2020

UDC 001.1
BBK 29

The 6th International scientific and practical conference "Science, society, education: topical issues and development prospects" (May 10-12, 2020) SPC "Sci-conf.com.ua", Kharkiv, Ukraine. 2020. 1125 p.

ISBN 978-966-8219-83-2

The recommended citation for this publication is:
Ivanov I. Analysis of the phaunistic composition of Ukraine // Science, society, education: topical issues and development prospects. Abstracts of the 6th International scientific and practical conference. SPC "Sci-conf.com.ua". Kharkiv, Ukraine. 2020. Pp. 21-27. URL: http://sci-conf.com.ua.

Collection of scientific articles published is the scientific and practical publication, which contains scientific articles of students, graduate students, Candidates and Doctors of Sciences, research workers and practitioners from Europe, Ukraine, Russia and from neighbouring coutries and beyond. The articles contain the study, reflecting the processes and changes in the structure of modern science. The collection of scientific articles is for students, postgraduate students, doctoral candidates, teachers, researchers, practitioners and people interested in the trends of modern science development.

e-mail: kharkiv@sci-conf.com.ua
homepage: *http://sci-conf.com.ua*

КІБЕРБЕЗПЕКА В ЦИФРОВОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ

Криворучко Інна Ігорівна,
викладач-стажист
Ковтанюк Максим Сергійович
викладач-стажист
Уманський державний педагогічний університет імені Павла Тичини
м. Умань, Україна

Питання про кібербезпеку гостро стоїть з того часу, як комп'ютерна техніка перестала бути лише прерогативою великих наукових центрів. З появою та поширенням локальних і глобальних мереж змінилося розуміння кібербезпеки, відповідних трендів, проблем і задач.

Під'єднання до цифрової інформаційної мережі стало невід'ємною частиною нашого повсякденного життя. Багато державних та приватних організацій, такі як медичні, фінансові та заклади освіти, використовують мережу для збору, обробки, зберігання та обміну великою кількістю цифрової інформації. Оскільки велика кількість цифрових даних збирається та спільно використовується, захист цієї інформації стає ще більш важливим для нашої національної та особистої безпеки.

Викрадення персональних даних, коштів з карток, акаунтів соціальних мереж – ось наслідки роботи кіберзлочинців. Якщо раніше було достатньо мати антивірус на комп'ютері для того, щоб захиститись від будь-якого шкідливого програмного забезпечення та не стати жертвою кіберзлочинності потрібно мати базові знання з цифрової кібербезпеки.

Чим більше часу ми проводимо в Інтернеті, тим більший вплив він має як офлайн, так і онлайн. Людина, як офлайн персона – це особа, з якою ваші друзі та сім'я взаємодіють щодня дома, у школі, університеті чи на роботі. Вони знають вашу персональну інформацію, таку як: ім'я, вік або місце проживання. Ваша онлайн персона – це та особа, якою представляєтесь іншим в Інтернеті. В мережі Інтернет ви повинні розкривати лише обмежену кількість інформації

про себе, інакше, ви можете стати жертвою кіберзлочинця та втратити свої кошти або цінну персональну чи корпоративну інформацію.

Будь що розміщене в Інтернеті може залишатись там назавжди, навіть якщо ви змогли стерти всі копії, що є у вашому розпорядженні. Якщо сервери були зламані, конфіденційна інформація про персонал може бути оприлюднена. Хакер може пошкодити веб-сайт компанії, розмістивши неправдиву інформацію та зруйнувати репутацію компанії, яка будувалась багато років. Хакери також можуть вивести з ладу веб-сайт компанії, через що компанія втратить дохід. Якщо веб-сайт виходить з ладу на тривалий період часу, то компанія може здаватися ненадійною та втратити довіру. Якщо веб-сайт або мережа компанії були зламані, то це може призвести до витоку конфіденційних документів, розкриття комерційних таємниць та викрадення інтелектуальної власності. Втрата всієї цієї інформації може заважати росту та розширенню компанії.

Кіберзлочинці для досягнення своєї мети використовують багато методів та засобів. Одним із таких засобів є шкідливе програмне забезпечення: шпигунські програми, рекламне ПЗ, програми-вимагачі, псевдоантивірус, руткіт, вірус, троянський кінь, черв'яки або хробаки. Крім того, існує ще багато методів викрадення інформації, серед них найпоширенішими є поєднання фішингу та методу соціальної інженерії.

Детальний опис подано у таблиці 1 [1].

Всі перераховані методи та засоби використовуються зловмисниками дуже активно, саме тому постає питання як боротися з шкідливим ПЗ.

1. Бути уважним. Більшість шкідливого ПЗ встановлюється користувачами через їхню неуважність, адже невірно вибраний пункт в меню при встановленні якої небуть програми може призвести до зараження всього ПК.

2. Оминати підозрілі сайти. Часто зловмисники створюють сайти з шкідливим ПЗ, яке вони видають за ліцензійне. Саме тому, варто замислитись

чи завантажувати ПЗ із сайту, який наповнений рекламою або ж підозрілим доменним ім’ям.

3. Використовувати складні паролі або користуватись ПЗ, які автоматично генерують вам складний пароль.

4. Використовувати спеціальні розширення в браузерах та антивіруси для захисту вашого ПК.

5. Нікому не розголошувати паролі та логіни соціальних мереж, пошт та персональних кабінетів на різних веб ресурсах.

6. Не вказувати свою пошту або номер телефону на сумнівних веб-сайтах.

Таблиця 1

Шкідливе програмне забезпечення та деякі методи викрадення інформації

Назва	**Опис**
Шпигунські програми	зловмисне програмне забезпечення, призначене для стеження та шпигування за користувачем
Рекламне ПЗ	призначене для автоматичного поширення реклами. Рекламне ПЗ часто встановлюється разом з деякими версіями програмного забезпечення. Іноді рекламне ПЗ призначене лише для поширення реклами, але досить часто з ним поширюється шпигунське ПЗ.
Програми-вимагачі	це шкідливе ПЗ призначене для блокування комп’ютерної системи або розміщених на ній даних до моменту здійснення викупу. Такі програми зазвичай шифрують дані на комп'ютері за допомогою невідомого користувачу ключа.
Псевдоантивірус	тип шкідливого ПЗ, що переконує користувача виконати конкретну дію, використовуючи його страх. Scareware створює спливаючі вікна, схожі на діалогові вікна операційної системи. Ці вікна відображають підроблені повідомлення про те, що система знаходиться під загрозою або необхідне виконання відповідної програми для повернення до нормальної роботи.
Руткіт	зловмисне програмне забезпечення, призначене для змін в операційній системі з метою створення чорного ходу (backdoor). Після чого нападники використовують цей чорний хід для віддаленого доступу до комп’ютера.

Вірус	шкідливий виконуваний код, який прикріплюється до інших виконуваних файлів, часто легітимних програм. Більшість вірусів вимагає активації з боку кінцевих користувачів і можуть спрацьовувати у певний день або час.
Троянський кінь	зловмисне ПЗ, яке здійснює шкідливі дії під виглядом бажаної операції. Цей шкідливий код використовує привілеї користувача, який його запускає. Часто трояни містяться в файлах зображень, аудіофайлах або іграх.
Черв'яки або хробаки	шкідливий код, який клонує себе, самостійно використовуючи вразливості в мережах. Хробаки зазвичай уповільнюють роботу мереж. Вони використовують вразливість системи, мають здатність до самостійного розповсюдження і виконання дій на користь зловмисника.
Фішинг	вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних. Прикладом є ситуація, коли зловмисник надсилає шахрайського електронного листа, який виглядає як повідомлення від легального надійного джерела. Мета цього повідомлення – змусити одержувача встановити зловмисне ПЗ на своєму пристрої або розкрити особисту чи фінансову інформацію.
Соціальна інженерія	спеціальна методика маніпуляції, яка допомагає змусити людину віддати зловмисникам необхідні дані використовуючи людські слабкості – тобто емоції та природну поведінку жертви. Зловмисники можуть «маскуватися» під установи, яким довіряє людина. Наприклад, прикидаючись представниками оператора мобільного зв'язку або працівниками банку, вони можуть надсилати електронні листи з додатком або посиланням, за яким людина має ввести свої особисті дані.

Кібербезпека – це постійні зусилля спрямовані на захист мережевих систем та всіх даних від несанкціонованого використання або заподіяння шкоди. На особистому рівні вам потрібно захистити вашу ідентичність, ваші дані та ваші електронні пристрої.

З кожним днем росте кількість жертв цифрової кіберзлочинності. Саме тому важливо знати як боротися із шкідливим ПЗ. В статті детально описано види шкідливого ПЗ, методи та засоби боротьби з ним, правила безпечної поведінки в Інтернеті та можливі наслідки кібератак. Ці базові знання цифрової безпеки в Інтернеті дозволять вберегти ваші дані, кошти на картках та акаунти в соціальних мережах від зловмисників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Найпоширеніші загрози безпеці комп’ютерних систем [Електронний ресурс]. – Режим доступу :https://sites.google.com/site/zagrozu/project-updates.