Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Дрожева Артема Владиславовича*

академічної групи *125м-22з-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Обґрунтування методів протидії загрозам інформаційної безпеки школярів в соціальних мережах*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Сафаров О.О.			
розділів:				
спеціальний	к.т.н., доц. Сафаров О.О.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Дрожеву Артему Владиславовичу* **академічної групи** *125м-22з-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Обґрунтування методів протидії загрозам інформаційної безпеки школярів в соціальних мережах*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання. Постановка задачі	02.10.2023
Розділ 2	Спеціальна частина	06.11.2023
Розділ 3	Економічна частина	04.12.2023

Завдання видано _____ Сафаров О.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Дрожев А.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи містить: 87 сторінок, 6 рисунків, 3 таблиці, 4 додатки, 23 посилання.

Об’єкт дослідження: забезпечення інформаційної безпеки (ІБ) громадян України шкільного віку в соціальних мережах.

Мета кваліфікаційної роботи: захист громадян України шкільного віку від загроз інформаційної безпеки в соціальних мережах.

В першому розділі кваліфікаційної роботи наведена характеристика, функціонал та класифікація соціальних мереж; наведені результати досліджень щодо активності школярів у соцмережах та проведено аналіз загроз ІБ з боку соцмереж, в тому числі школярів.

У спеціальній частині проведено аналіз існуючих методів захисту громадян України шкільного віку від загроз ІБ в соціальних мережах та запропоновано комплекс організаційних методів протидії загрозам ІБ школярам різних вікових груп при використанні соцмереж.

В економічному розділі проведено розрахунки витрат на реалізацію запропонованих заходів щодо підвищення рівня інформаційної безпеки у школі.

Наукова новизна результатів даної кваліфікаційної роботи полягає у розробці комплексу організаційних методів підвищення рівня обізнаності громадян України шкільного віку з питань ІБ в соціальних мережах.

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СОЦІАЛЬНІ МЕРЕЖІ, ЗАГРОЗИ ШКОЛЯРАМ В СОЦІАЛЬНИХ МЕРЕЖАХ, ОРГАНІЗАЦІЙНІ МЕТОДИ

ABSTRACT

The explanatory note of qualification work consists of: 87 pages, 6 figures, 3 tables, 4 appendices, 23 references.

The object of the qualification work: information security of Ukrainian schoolchildren in social networks.

The purpose of the work: protection of Ukrainian schoolchildren from security threats on social networks.

The first section of the qualification work gives the characteristic, functional and classification of social networks; the research on the activity of schoolchildren in social networks and an analysis of threats to information security from the social networks, including schoolchildren, was conducted.

The special section includes the analysis of existing methods of protecting citizens of Ukraine of school age from informational security threats in social networks; the set of organizational methods to counter information security threats for schoolchildren of different age groups using social networks was made.

The economic section calculates the costs of the proposed measures to improve the level of protection of schoolchildren in using social networks.

The scientific novelty of the qualification work consists in developing of the set of organizational practices to raise awareness of the Ukrainian citizens of school age on information security in social networks.

INFORMATION SECURITY THREAT, SOCIAL NETWORKS, THREAT OF SCHOOLCHILDREN IN SOCIAL NETWORKS, ORGANIZATIONAL METHODS

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ЗМІ	–	засоби масової інформації;
ІБ	–	інформаційна безпека;
ІКТ	–	інформаційно-комунікаційні технології;
КЗ	–	контрольована зона;
США	–	Сполучені Штати Америки.

ЗМІСТ

ВСТУП

В сучасному світі інформація розповсюджується надзвичайно швидко у зв'язку з особливостями нинішніх засобів масової інформації (ЗМІ). Інформація в більшості сучасних джерел інформації майже не фільтрується та не перевіряється, і має великий вплив на ще несформовану свідомість неповнолітніх.

Значної популярності в останні роки зазнали соціальні мережі, як спосіб віртуального спілкування та обміну інформацією поміж користувачами. Середній вік користувачів соцмереж зменшується з кожним роком і це означає, що все молодші користувачі отримують постійний доступ до великої кількості майже нефільтрованої інформації. Спілкуючись в віртуальних соцмережах, користувачі забувають про реальне життя, що має поганий вплив на їхній фізичний та психічний стан здоров'я. Також особливої популярності в соцмережах набуває шахрайство та кіберзлочинність, при чому більша частина жертв таких злочинів є неповнолітні через їхню довірливість та необачність. Юні користувачі часто навіть не здогадуються про небезпеки, що приховують в собі соцмережи.

Нинішні школярі є підростаючим поколінням українців, тому набуває актуальності питання забезпечення інформаційної безпеки користувачів соціальних мереж, особливо шкільного віку.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про соціальні мережі

Соціальна мережа - це структура, що базується на людських зв'язках або ж взаємних інтересах. В якості інтернет-сервісу соцмережа може розглядатися як платформа, за допомогою якої люди можуть здійснювати зв'язок між собою та групування за специфічними інтересами. Завдання такого сайту полягає у тому, щоб забезпечити користувачів всіма можливим шляхами для взаємодії один з одним - відео, чати, зображення, музика, блоги та інше [1].

Сам термін «соціальні мережі» був введений до наукового обігу в 1954 році соціологом Джеймсом Барнсом (в роботі «Класи та збори у норвезькому острівному приході») [3]. До того багато вчених, які займалися вивченням суспільства, висловлювали думку про важливість розгляду суспільства як складного переплетення взаємин.

Найбільшим феноменом всесвітньої павутини є утворення мережевих спільнот та соціальних мереж. Термін «Virtual Community» (віртуальне, або мережене суспільство) розробив Г. Рейнгольд і дав йому наступне визначення: «Віртуальні співтовариства є соціальними об'єднаннями, які виростають з Мережі, коли група людей підтримує відкрите обговорення достатньо довго і людяно, для того щоб сформувати мережу особистих відносин у кіберпросторі» [3].

Соціальними мережами користуються 82% від всіх інтернет-користувачів у світі − це 1,2 млрд. чоловік. Високий рівень їх проникнення відображає один з головних трендів глобальної мережі – як тільки люди підключаються до Інтернету, вони негайно починають спілкуватися з іншими людьми. Ще більш красномовна статистика часу проведеного користувачами в мережі – за останні кілька років кількість годин, яку люди провели в соціальних мережах, збільшилася втричі. У жовтні 2011 року використання соціальних мереж стало найпопулярнішим заняттям серед інтернет-аудиторії. З 5 хвилин в Інтернеті одна проводиться в який-небудь соціальної мережі. У

березні 2007 року соціальні мережі займали у користувачів лише 6% часу. Сьогодні відсоток тих, хто використовують соціальні мережі у світі коливається від 53% у Китаї до 98% в США. У 41 країні із 43 досліджених цей рівень вище 85%. Час, що проводиться в соціальних мережах, збільшився за останній рік принаймні на 35% у кожному з розглянутих регіонів [5].

1.1.1 Призначення соціальних мереж

Початок сучасної теорії соціальних мереж поклали в 1951 році Рей Соломонофф і Анатолій Рапопорт. У 1959−1968 рр.. угорські математики Пол Ердос і Альфред Рен'ї написали вісім статей, що описують принципи формування соціальних мереж [4].

Теорія соціальних мереж припускає, що соціальна поведінка та комунікація відчувають вплив моделей взаємовідносин людей. Відповідно до одного з її положень, чим міцніше соціальні зв'язки між людьми, тим активніше вони спілкуються один з одним, використовуючи всі доступні медіа. Як і інші нововведення комунікаційної технології, Інтернет продовжує процес з'єднання людей в соціальні мережі, а також людей і організацій, розкиданих географічно, але пов'язаних спільними інтересами. Теорія соціальних мереж стверджує, що соціальна комунікація по Інтернету доповнює і розширює традиційне соціальну поведінку, тому чим активніше люди поводяться в співтоваристві, тим більше вони спілкуються в міжособистісній формі, і чим тісніше їх контакти, тим частіше вони користуються електронною поштою та іншими медіа для спілкування [6].

Форма соціальної мережі допомагає визначити ступінь своєї корисності для її учасників. Менші мережі можуть бути менш корисними для своїх учасників, ніж мережі з багатьма слабкими зв'язками з особами ззовні від основної мережі. Мережі, з багатьма слабкими зв'язками та соціальними взаєминами, вірогідніше будуть пропонувати нові ідеї та можливості для своїх учасників, аніж мережі з багатьма надлишковими зв'язками. Іншими словами,

група знайомих друзів, які спілкуються лише один з одним вже володіють спільними знаннями та можливостями. Група осіб, із зв'язками з іншими соціальними спільнотами, вірогідно, отримуватимуть доступ до ширшого діапазону інформації. Для досягнення успіху, індивідам краще мати зв'язки з декількома мережами, аніж багато зв'язків в межах однієї мережі. Аналогічно, індивіди можуть впливати, або діяти в ролі передавача інформації в середині своїх соціальних мереж з'єднуючи дві мережі, в яких відсутні безпосередні зв'язки. Схему зв'язків в соціальних мережах наведено на рис. 1.1.

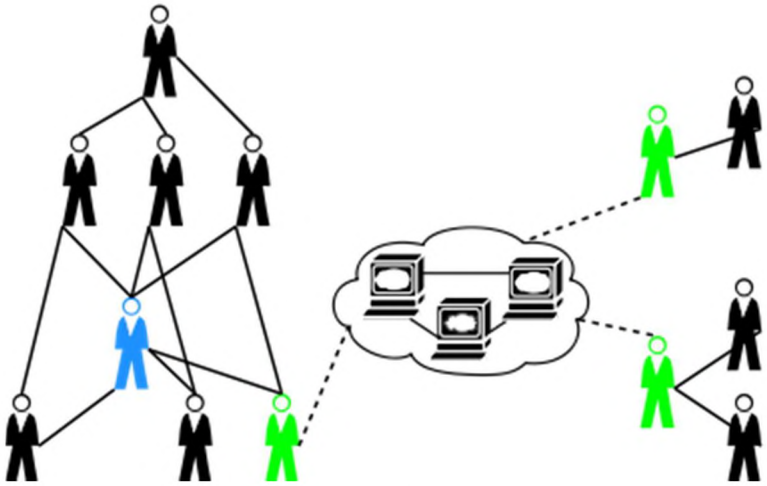

Рисунок 1.1 - Приклад відображення схеми зв'язків в соціальних мережах

На рис. 1.1 в соціальній мережі зліва, індивід, позначений блакитним кольором, має найбільше зв'язків в середині своєї соціальної мережі. В ідеальній ситуації, він мав би бути лідером або керівником групи або організації. Індивіди, позначені зеленою фарбою мають зв'язки із іншими соціальними групами, і можуть виступати в ролі передавачів інформації між мережами.

Сила теорії соціальних мереж у її відмінності від традиційних соціологічних наук, згідно з якими вважається, що саме атрибути окремих користувачів— дружність або недружність, рівень інтелекту, тощо — відіграють основну роль. У теорії соціальних мереж використовується інший погляд, коли атрибути окремих користувачів менш важливі, аніж стосунки та зв'язки з іншими користувачами в мережі. Цей підхід виявився корисним при

поясненні багатьох реальних явищ, але залишає менше простору для індивідуальних дій, можливостей індивідів впливати на свій успіх, так як багато залежить від структури їхньої мережі. [2]

1.1.2 Класифікація соціальних мереж

В сучасних глобальних мережах існує багато різних соцмереж. Для упорядкування можна навести декілька класифікацій соціальних мереж за різними показниками [8]:

За типом:

- особисте спілкування (classmates.com);
- ділове спілкування (linkedin);
- розваги (myspace);
- відео (youtube);
- аудіо (last.fm);
- фото (flickr);
- геолокація (foursquare);
- покупки (groupon);
- блогінг (tumblr);
- новини (reddit);
- питання-відповідь (answers.com);
- закладки (delicious);
- тематичні (slashdot);

за доступністю:

- відкриті (facebook);
- закриті (playboyu);
- змішані;

по регіону:

- світ (hi5);

– країна (qzone);
– територіальна одиниця;
– без регіону (international).

Найбільш інформативною можна вважати класифікацію соціальних мереж за типом, в ній представлено багато різних проєктів з різним типом контенту і для різних цілей, кожен з яких зайняв свою нішу. Якщо проаналізувати дану класифікацію, можна прийти до висновку, що зараз соціалізовані вже всі основні тематики в мережі. Остання група в класифікації «тематичних» мереж приховує в собі величезну кількість спільнот, кожне з яких ґрунтується на тематичному контенті та спілкуванні. Так, наприклад, Last.Fm - музична соціальна мережа - будує зв'язки між користувачами за принципом музичних уподобань, використовуючи при цьому оригінальні засоби - віджети для блогів, утиліту для прослуховування музики, а також будує чарти з прослуханої вами музики.

Наступний тип класифікації показує, наскільки мережі доступні. Зараз більшість мереж повністю відкриті для зовнішнього світу, за що їх активно критикують користувачі. Деякі проєкти не націлені на публічність через свої бізнес-моделі, тому вони спочатку створювалися закритими.

Остання градація - по географічного регіону - найпростіша й очевидна: спочатку з'явилися світові гіганти, які стирали фізичні кордони, трохи пізніше почали розвиватися мережі в окремих регіонах, часто копіюючи повністю або частково світових гігантів, але з ухилом на свій регіон. З розвитком інтернету поступово стали з'являтися мережі навіть по окремих містах. Також варто згадати мережі, які прив'язуються не до регіону, а до організації, наприклад, соціальні мережі корпорацій чи політичних партій [8].

1.1.3 Функціонал соціальних мереж

У глобальній мережі існує своя структура веб-сайтів, у якій своє місце посідають соціальні мережі (таблиця 1.1).

Таблиця 1.1 - Структура Інтернету за видами сайтів

Структура Інтернету за видами сайтів		
Інтернет-представництва	Інформаційні ресурси	Веб-сервіси
– Сайти-візитки – Корпоративні сайти – Інтернет-вітрини – Промо-сайти	– Тематичні сайти – Інтернет-портали – Блоги – Каталоги сайтів	– Пошукові системи – Поштові системи – Інтернет-форуми – Фото-, відео-, аудіо-хостинги – Дошки оголошень – Соціальні інтернет-мережі

З усіх вищеперерахованих видів сайтів більше всього спільних аспектів соціальні мережі мають з блогами, тематичними сайтами, пошуковими системами та інтернет-хостингами. Можна розглянути деякі з перелічених сайти більш детально.

Блоги – це тип сайтів, на яких власник блогу пише тексти зі своїми коментарями, міркуваннями, ідеями та іншою постійно змінюваною інформацією. З блогами соцмережі схожі в тому, що, як і у блогах, в соцмережах користувач може висловлювати думку стосовно певних подій свого життя, показувати свою творчість та формулювати ідеї стосовно певних суспільних подій.

Тематичні сайти – це сайти, призначені для збереження інформації за певною чітко визначеною тематикою. З тематичними сайтами схожість проявляється в тому, що є соціальні мережі як загальнотематичного спрямування, так і за певним типом інтересів.

Пошукові системи – це сайти для пошуку інформації в Інтернеті за певними критеріями. Пошукові сайти мають схожість у фундаментальній ознаці соціальних мереж, а саме у пошуку соціальних контактів. В соціальних

мережах нового типу можна шукати не тільки людей, а й мультимедійну інформацію (фото, відео, музику).

Інтернет-хостинги – на сайтах такого типу існує можливість зберігання файлів для подальшого їх використання. З сайтами-хостингами соцмережі сходяться у такій якості, як збереження файлів, оскільки в мережах соціального типу існує можливість зберігання інформації, зокрема мультимедіа.

Таким чином, можна виділити основні функції, що виконуюсь соціальні мережі як сучасний різновид класичних соціальних мереж:

1) комунікативна функція – можливість спілкування в реальному часі внаслідок створення людиною власного віртуального образу в текстовій формі, а останнім часом це спілкування може здійснюватися у цих мережах за допомогою відео- та аудіозв'язку;

2) інформаційна функція – чи не найважливіша функція, яка дає можливість якісного і достатньо швидкого обміну інформацією між користувачами. Також в соцмережах існує система оцінювання інформації;

3) функція збереження соціальних зв'язків – такого типу мережі надають можливість відновити соціальні зв'язки людей, які через певні причини обірвались, наприклад, через просторовий чинник;

4) нормотворча функція – у соціальних Інтернет-мережах існують певні, хоча й не формалізовані норми, які поширюються серед користувачів. Ці норми проявляються, як у стилях спілкування всередині цих мереж, так і у певній поведінці у цій площині;

5) функція самопрезентації та самовираження – будь-який користувач може за допомогою ресурсів Інтернету створити в таких мережах своєрідний образ власного «Я». В соціальних мережах є можливість вести дискусії стосовно певних питань, створити власний віртуальний образ, поділитись

власною творчістю навіть тим особистостям, які мають певні психологічні чи соціальні комплекси в повсякденному житті;

6) розважальна функція – у деяких людей існує потреба використати свій вільний час для розваг. Розваги у віртуальній реальності і соцмережах надають можливість релаксації завдяки сучасним інформаційним можливостям. Також це дає людям, які мають певні соціально-психологічні комплекси, можливість замінити розваги у соціальній реальності розвагами у віртуальній реальності [9].

1.2 Дослідження використання соціальних мереж громадянами України шкільного віку

Вченими Девідом Уайтом та ЕлісонЛеКорню з Оксфордського університету було висунуто розділення користувачів на "відвідувач" і "житель". У цій моделі "відвідувачі" використовують інтернет у функціональному плані: як інструмент, тоді як "жителі" використовують інтернет як соціальний простір, тобто як місце для комунікації проведення часу [11]. За браком досвіду, більшість школярів не розглядають соціальні мережі, як інструмент, а лише вивчають його зсередини, віртуально живучи в соцмережах.

За даними дослідження «Вплив ЗМІ на підростаюче покоління та формування комп'ютерної залежності у підлітків» [12], інформацію з Інтернету отримують 92,6% учнів, із телебачення - 56,6%. Про те, що найчастіше інформацію шукають у газетах, сказали 3,5% підлітків, з радіопрограм - 3,2%. 26,1% віддають перевагу книгам, а 9% - журналам. Не обрали жодного із зазначених джерел 0,1% респондентів (рис. 1.2).

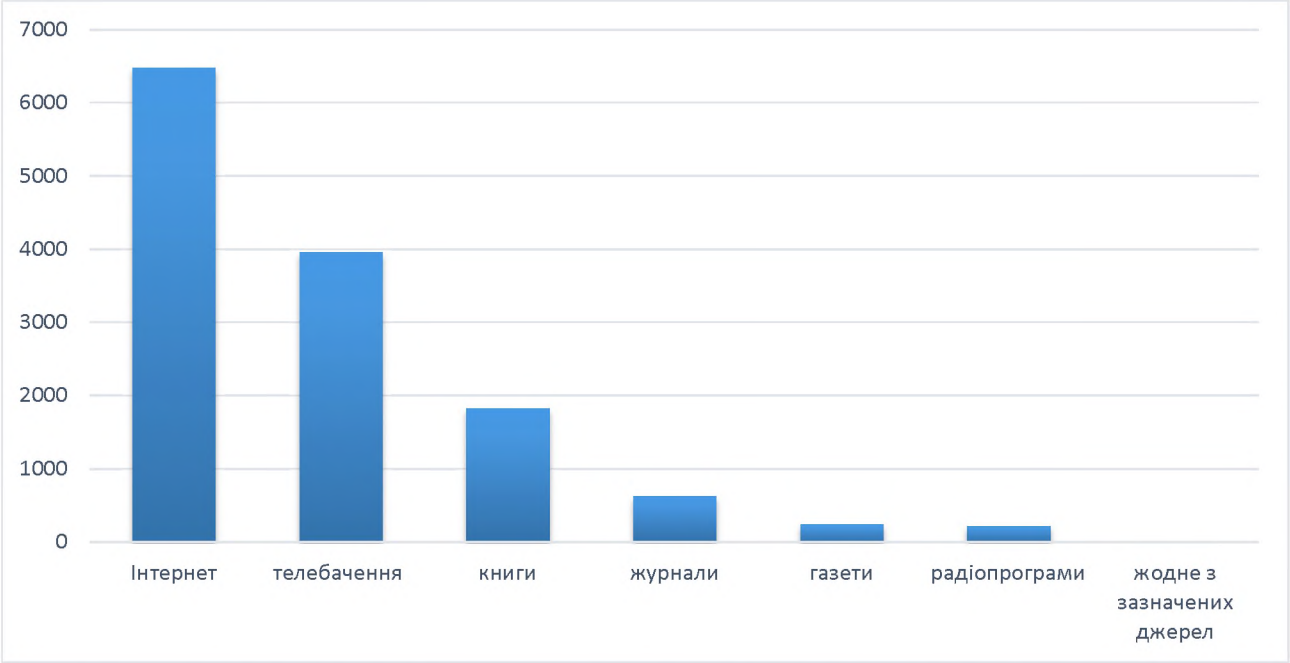

Рисунок 1.2 – Рейтинг популярності джерел інформації серед школярів

Як видно з рис 1.2, значна більшість школярів надає перевагу пошуку інформації в Інтернеті та на телебаченні, аніж друкованим джерелам інформації чи радіопрограмам. Це свідчить про уподобання школярів до усього візуального.

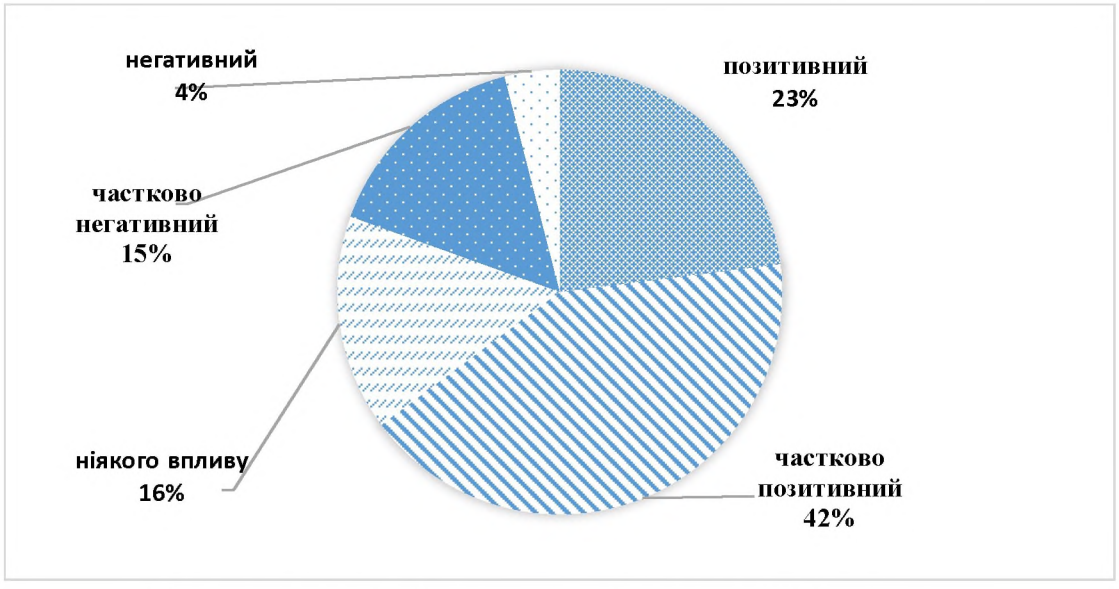

Рисунок 1.3 – Оцінка школярів впливу ЗМІ на них

Позитивний вплив від ЗМІ відчувають 23% опитаних підлітків, частково позитивний - 41,8%. Про частково негативний та негативний вплив ЗМІ сказали відповідно 15,5% та 4%. Не відчувають взагалі ніякого впливу ще 15,7% (рис 1.3).

Як видно з діаграми, майже дві третини учнів вважають вплив ЗМІ (Інтернету та телебачення перш за все) позитивним або частково позитивним, що також свідчить про симпатію школярів до віртуальних джерел інформації.

Більшість учнів також вважають, що інформації у ЗМІ слід довіряти частково - 89,5%. Повністю довіряють інформації у ЗМІ 2,5% опитаних, а 8% не довіряють. Тобто, школярі розуміють ненадійність обраних джерел інформації, проте продовжують ними користуватися.

За даними опитування, 65% столичних школярів щодня проводять свій час в Інтернеті. При цьому 33,4% заявили, що постійно прагнуть перевіряти свої сторінки у соціальних мережах та електронну пошту. 14,7% не уявляють, чим себе зайняти, коли немає доступу до комп'ютера. А 6% вважають, що спілкування в Інтернеті краще, ніж особисте спілкування (рис. 1.4).

Рисунок 1.4 – Прояви Інтернет-залежності школярів

На рис. 1.4 видно, що значна кількість школярів страждають на залежність від Інтернету та соціальних мереж в різних формах та поступово здійснюють перехід від реального спілкування до віртуального.

На запитання, для чого найчастіше учні використовують мережу, 64,8% відповіли, що для спілкування у соціальних мережах, чатах, на форумах. Для підготовки до уроків Інтернет використовують 46,5%, 40,3% - для перегляду фільмів, 30,7% - для прослуховування музики. Для доступу до комп'ютерних ігор Інтернет використовують 18%, для перегляду розважальної інформації - 11,5%, для перегляду сайтів для дорослих - 2,4%. Для чогось іншого

Інтернетом користуються ще 2,6%. 0,4% не визначили, для чого користуються мережею [12]. Найбільшою прихильністю серед опитуваних користувалося спілкування в соцмережах. Проте варто зазначити, що усі інші пункти опитування, обрані школярами, можуть також торкатися соцмереж, адже більшість активних

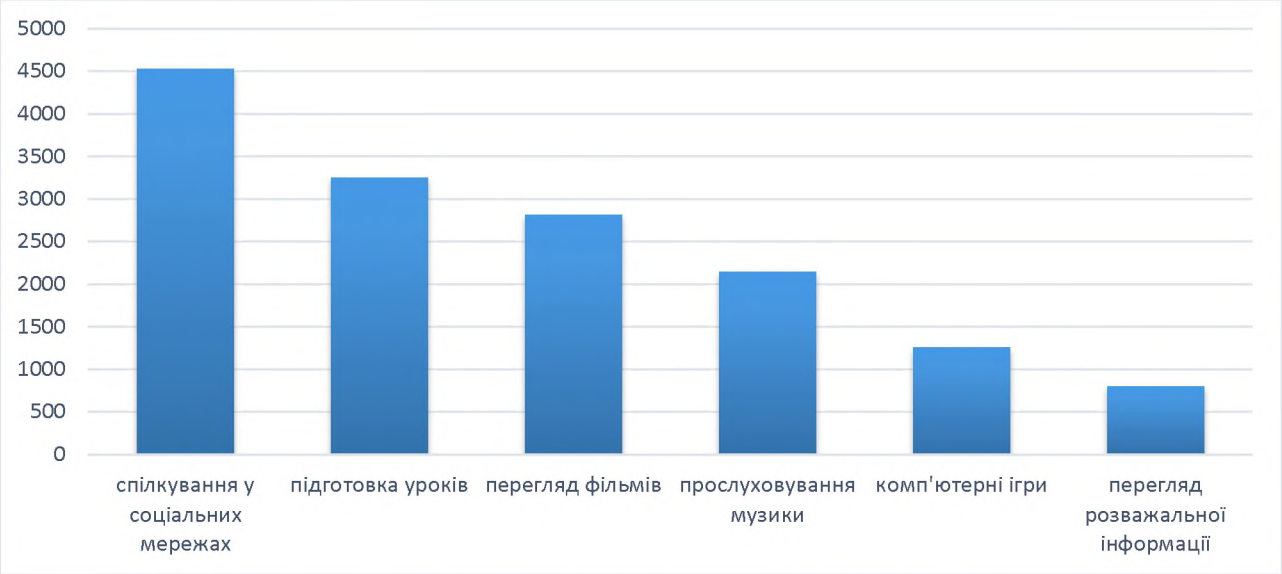

Рисунок 1.5 – Активність школярів в Інтернеті

користувачів соцмереж переглядають фільми слухають музику, грають в ігри тощо, не покидаючи сторінки соціальної мережі.

1.2.1 Дослідження щодо використання соціальних мереж в системі загальної середньої освіти

З метою визначення рівня використання соціальних сервісів та соціальних мереж у навчальному процесі було проведено опитування [12], в якому взяли участь як педагогічні працівники, так і учні загальноосвітніх навчальних закладів. За оцінками респондентів-вчителів значна кількість учнів (до 70%) мають вдома доступ до ПК та мережі Інтернет, якими активно користуються у позанавчальний час. Особливо популярними, на думку вчителів, серед учнів є соціальні мережі, сервіси з обміну миттєвими повідомленнями, голосовий та відеозв'язок, а також сервіси, призначені для збереження та надання доступу до фото- та відеофайлів. Респонденти-учні підтвердили вказане припущення педагогічних працівників. Отримані дані

дозволяють стверджувати, що близько 80% учнів у віці від 13 років мають облікові записи у різноманітних соціальних мережах, а близько 70% даної категорії учасників опитування використовують їх щодня.

Вказані ресурси мають значний потенціал з точки зору організації навчання, який використовується дуже обмежено. Результати проведеного опитування [10] свідчать, що незначна частина педагогічних працівників (до 12% респондентів) має певний досвід використання вказаних інтернет-ресурсів з навчальною метою. Зазвичай це досвід розміщення завдань для учнівських колективів (груп) на особистій сторінці викладача або спеціально створеній групі користувачів (6% респондентів), розміщення планів, програм, конспектів лекцій на особистих сторінках та блогах (12%), зберігання створених документів та надання відповідних з них учням для подальшого ознайомлення та виконання завдань offline (8%) тощо. Вчителі, що належать до першої групи, більш обізнані з можливостями соціальних сервісів, ширше практикують їх використання. Значна частина респондентів використовує інформаційно-комунікаційні технології безпосередньо на уроці, при цьому робить це систематично. Це презентації (учительські та учнівські), відеофрагменти, комп'ютерне тестування, сучасні програмовані педагогічні засоби. Частка таких педагогічних працівників серед учасників опитування склала близько 70%, що свідчить про поступове впровадження сучасних інформаційно-комунікаційних технологіях (ІКТ) в практичну діяльність вчителя.

Проведене опитування та порівняльний аналіз можливостей вказаних вище соціальних сервісів та соціальних мереж дає підстави для наступних висновків:

– доступні безкоштовні соціальні сервіси здатні задовольнити потреби учасників навчального процесу у збереженні, передачі та спільному використанні різних типів документів;

– переважна більшість учасників навчального процесу (як вчителів, так і учнів) мають досвід використання соціальних сервісів та/або соціальних

мереж у повсякденному житті, при цьому педагогічні працівники частіше використовують соціальні сервіси, а учні – соціальні мережі;

– одним із основних чинників, що стримує впровадження використання вказаних ресурсів, залишається рівень готовності системи загальної середньої освіти до використання сучасних засобів навчання (відсутність науково обґрунтованих методичних рекомендацій; норм витрати часу та оплати праці педагогічних працівників).

1.2.2 Дослідження активності громадян України шкільного віку в соціальних мережах

Під час виконання цієї кваліфікаційної роботи було проведено дослідження активності громадян України шкільного віку в соціальних мережах «Facebook» та «TikTok». Досліджувалась активність користувачів соцмереж двох вікових категорій: 6-14 (ряд 1) та 15-17 (ряд 2). Результати дослідження представлені на рис. 1.6 та рис. 1.7.

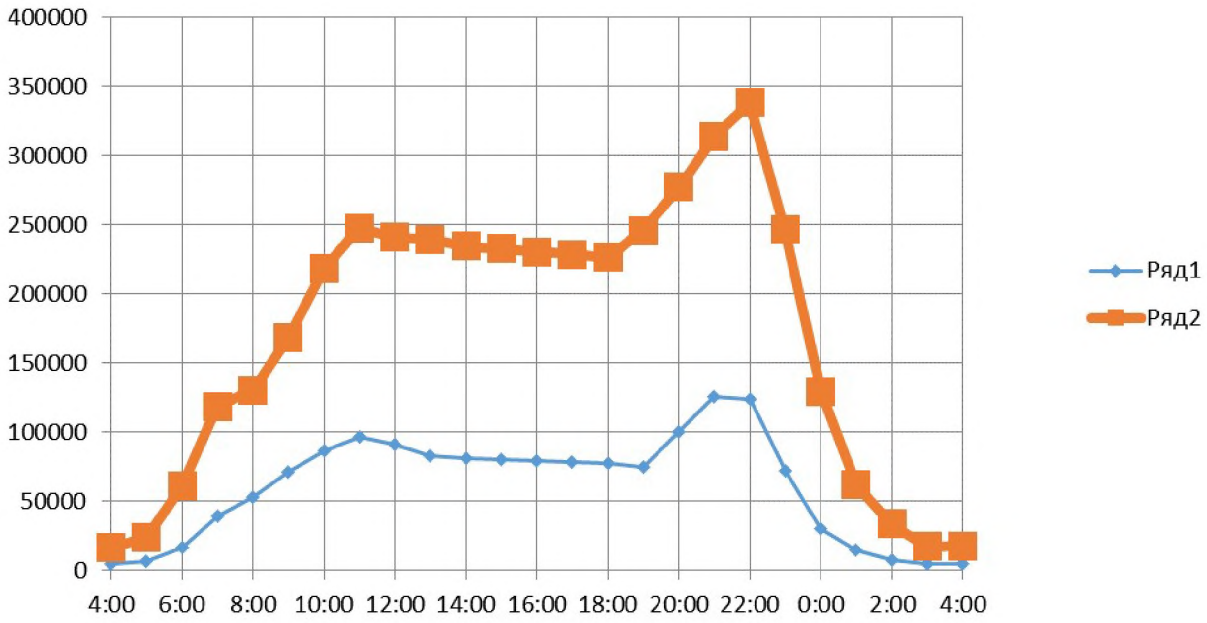

Рисунок 1.6 – Графік погодинної активності громадян України шкільного віку в соціальній мережі TikTok

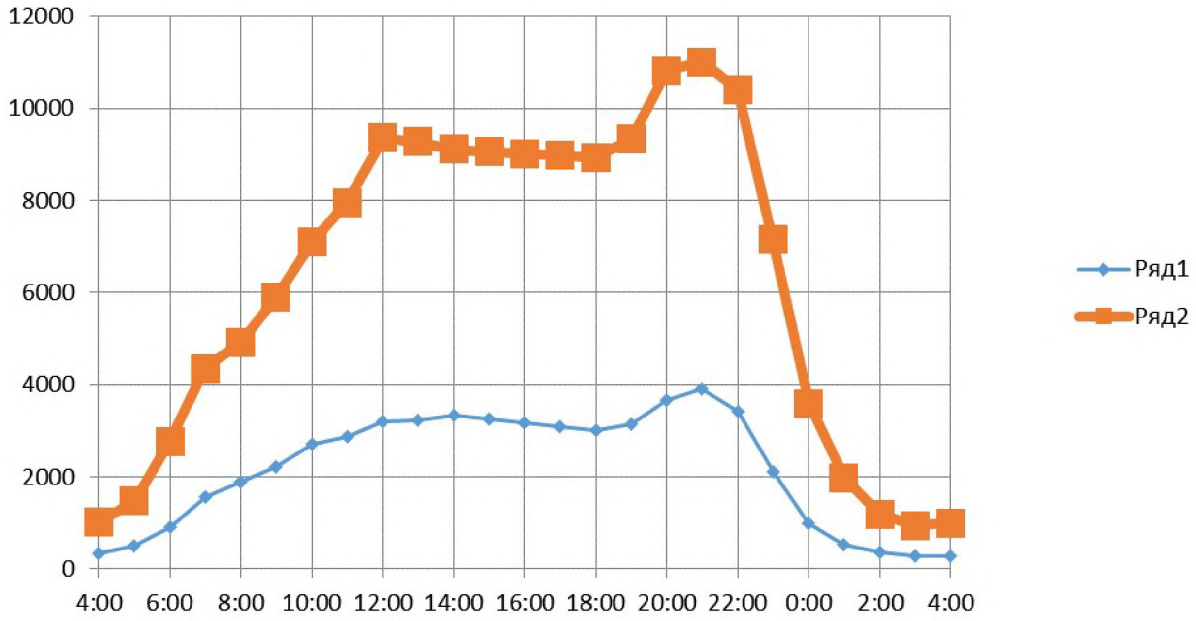

Рисунок 1.6 – Графік погодинної активності громадян України шкільного віку в соціальній мережі Facebook

Варто зазначити, що заняття учнів молодшого шкільного віку закінчуються приблизно о 12-13 годині, а в учнів середнього та старшого шкільного віку – о 14-15 годині, чим зумовлена висока активність користувачів соцмереж у другій половині дня. Проте їхня активність в першій половині дня свідчить про те, що учні активно користуються соцмережами навіть під час шкільних занять.

Як видно з графіку (рис. 1.6), починаючи з 5 години ранку, кількість українських користувачів шкільного віку стрімко зростає та здобуває свого денного максимуму об 11 годині. Потім активність користувачів дещо спадає. О 6 годині вечора у старшої категорії досліджуваних та о 7 годині вечора у молодшої категорії досліджуваних активність знову починає зростати та здобуває свого вечірнього та загальнодобового максимуму о 9-10 годині вечора. Після цього активність школярів спадає до свого загальнодобового мінімуму о 3-4 годині ночі.

Соціальна мережа Facebook має меншу популярність серед школярів, аніж TikTok, проте загальний графік активності користувачів України

шкільного віку дуже схожий. Тенденції розвитку добової активності користувачів TikTok ідентичні активності користувачів Facebook.

Особливу увагу необхідно звернути на те, що навіть у нічний час велика кількість школярів (більше 20 тисяч) не припиняє користування соцмережами. Це свідчить про вже розвинену залежність від соціальних мереж у певних школярів. Також нічна активність користувачів шкільного віку має поганий вплив на здоров'я школярів та якість їх навчання.

1.3 Загрози ІБ при використанні соціальних мереж

Аналізуючи процес виникнення і розвитку соціальних мереж та ті функції, які вони виконують у сучасному світі, можна дійти висновку, що поширення і використання соціальних Інтернет-мереж має певні наслідки, що, безумовно, має як позитивний, так і негативний характер. Розглянемо детальніше, які загрози приховують в собі віртуальні соціальні мережі.

1.3.1 Загрози інформаційній безпеці держави від користувачів соціальних мереж

Соціальні мережі єднають людей. Анонімність у мережі надає хоробрості багатьом і спонукає до дії. Спільнота активних користувачів того чи іншого сегмента глобальної мережі об'єднана не тільки віртуальними, а й реальними соціокультурними обставинами певної географічної території, кордонами держави тощо. З розвитком можливостей Інтернету для висловлення своїх думок і об'єднання у віртуальні групи посилились можливості для масових акцій у мережі, протестів або, навпаки, закликів до дії.

Одним із показових українських прикладів сили інтернет-користувачів став випадок із закриттям файлообмінного ресурсу EX.ua, який, за версією міжнародної організації захисту інтелектуальної власності, був у списку 25 найбільших у світі порушників авторських прав [13].

Український Інтернет уперше настільки явно виявив цілісність і організованість користувачів. Через кілька годин після закриття група хакерів

здійснили Ddos-атаки на сайт МВД, що зробило його неактивним. Увечері того самого дня виникли перші проблеми з web-представництвами СБУ та Президента України. Одночасно в соціальних мережах та в коментарях до матеріалів найбільш популярних інтернет-ЗМІ, таких як “Українська правда” та ForUm, з’явились інструкції, як допомогти атакувати сайти державних установ. Упродовж наступного дня сайт Президента був неактивним, а до атакованих додались сайти Верховної Ради, Кабінету Міністрів, НБУ, Конституційного суду України та ще декількох організацій [14]. Цей протест продемонстрував громадянську позицію великої кількості населення України: в атаках на сайти держустанов взяли участь близько 300 тис. звичайних користувачів, які відповідно до наведених інструкцій Ddos-атак виявили своє ставлення до позиції влади таким онлайн-протестом [15].

Отже, через велику швидкість розповсюдження інформації в соцмережах, подібна Ddos-атака згідно детальних інструкцій стає реальною загрозою для інформаційного простору держави в Інтернеті (сайти Верховної Ради, Кабінету Міністрів, НБУ тощо). Звернемо увагу на те, що у підлітковому віці діти більш схильні до ризикових вчинків (фахівцями доведено, що діти, які проводять за комп'ютерами більше 2-3 годин день, на 50% більш схильні до небезпечних вчинків [16]), до вивчення чогось незвичайного (інструкції Ddos-атак дуже цікаві сучасним школярам), довіряти незнайомцям, з якими вони нібито згодні, аніж дорослі громадяни.

Група компаній "1+1 Медіа" звернулася до керівників офісів соціальних мереж Facebook, Twitter тощо, а також до секретаря РНБО стосовно фактів постійного поширення в соцмережах закликів до порушення територіальної цілісності України, сепаратизму і тероризму на території самопроголошених всупереч Конституції України так званих Донецької та Луганської народних республік, які створюють істотні загрози національній безпеці України.

Таким чином, питання виховання розсудливих та відповідальних користувачів соцмереж стає актуальним для держави з точки зору її безпеки.

1.3.2 Загрози користувачам з боку соціальних мереж

1.3.2.1 Доступ до небажаного контенту

Під небажаним контентом розуміємо нелегальні та шкідливі матеріали, що не відповідають віковим особливостям дітей і негативно впливають на стан їх фізичного та психічного здоров'я.

Контентні загрози у соціальних мережах – це матеріали (тексти, зображення, аудіо, відеофайли, посилання на сторонні ресурси), які містять насильство, агресію, еротику і порнографію, нецензурну лексику, інформацію, що розпалює расову ненависть, пропаганду анорексії і булімії, суїциду, азартних ігор, наркотичних речовин і т.д.

Беззаперечно, соціальні мережі є інструментом для задоволення таких потреб дітей як допитливість, бажання навчитися новим речам, пізнати незвідані грані знань. Діти, проводячи свій час у соцмережах, набувають нового статусу – статусу громадян цифрового онлайнового світу, котрий, в той же час, немає жодних обмежень, цензури, табу чи застережень. Недосконаліть законодавства, яке б регулювало діяльність електронних ЗМІ, зумовлює те, що кожного разу, користуючись послугами соціальних мереж, діти опиняються в ніким неконтрольованому просторі з величезною кількістю інформації, у тому числі і шкідливою, що, безперечно, має негативний вплив на розвиток їх внутрішнього світу та сприйняття навколишнього середовища. Згідно з статистичними даними [21] в п'ятірку найбільш популярних у дитячому середовищі пошукових запитів входить слово «порно», а цього у соціальних мережах достатньо. І провина у цьому навіть не адміністраторів соціальних мереж, котрі докладають максимум зусиль, щоб відфільтровувати подібні тематичні групи, а користувачів, які безперервно створюють ресурси такого змісту, переміщують їх із групи в групу, випереджаючи дії служби безпеки. Більше того, гарантовано, і це є серйозним приводом для хвилювання,

що дитина, блукаючи тенетами соціальних мереж, зіткнеться із небажаним контентом, навіть якщо вона цього і на прагнула.

1.3.2.2 Залежність від соціальних мереж

Розвиток телекомунікаційних та комп'ютерних технологій сприяє поширенню явища, яке сучасна соціальна психологія визначила як «самотність в натовпі». Соціальні мережі через їх здатність створювати специфічний ефект присутності за рахунок високого рівня «іммерсивності» (занурення в середовище) призводять до виникнення проблеми залежності (адикції). Вона більш небезпечна ніж, приміром, залежність від комп'ютерних ігор. Якщо доступ до Інтернету зникає, залежний від соцмереж користувач відчуває сильне занепокоєння. З'являються психологічні проблеми такі, як депресія, поганий сон, виникають конфлікти в реальному житті. Якщо дитина перебуває в соціальних мережах більше 4 годин на добу, то вона удвічі частіше страждає від депресії і втричі частіше – від порушення сну, ніж та, яка проводить в соціальних мережах менше часу [32].

Більшість дослідників проблеми Інтернет-адикції погоджуються [33], що основними факторами, які приваблюють і, як наслідок, провокують виникнення залежності від соціальних мереж, є такі:

– анонімність соціальних взаємовідносин між учасниками;

– можливість приховати/розкрити фобії, комплекси і таємні потяги;

– можливість зміни ідентифікації (імені, статі, віку, національності, зовнішності);

– подолання власної внутрішнього душевного болю;

– реалізація уявлень, фантазій;

– «психологічний ексгібіціонізм»;

– компенсація психологічних комплексів завдяки участі в неформальних об'єднаннях;

– проведення часу в середовищі подібних до себе;

– «інформаційний вампіризм».

Загалом фактори виникнення та умови формування мережевої залежності можна поділити на дві групи:

– кібернетичні – об'єктні умови і фактори, пов'язані із властивостями кіберсередовища;

– індивідуально-психологічні – суб'єктні фактори, пов'язані з особистісними властивостями кіберкористувачів.

Соціальні мережі змінюють спосіб спілкування дітей з ровесниками, спосіб доступу до інформації, спосіб висловлення думки, спосіб розміщення і спільного використання творчого контенту. У дітей, які виросли в соціальних мережах, втрачаються навички міжособистісного спілкування; розвивається синдром гіперактивності; відзначається підйом психотичних проявів, таких як марення, неспокій, сплутаність свідомості, тривога, підвищена вразливість; формується відчуття безкарності; відсутні знання про добро і зло, про моральні закони соціуму, про межі поведінки і т.д. Потенційна небезпека надто активної поведінки у соціальних мережах має у педіатрії свою назву – «Facebook-депресія». У соцмережах реальне спілкування має тенденцію переміщатися в віртуальне. І віртуальним світом замінює реальний доволі значний відсоток дітей.. Слід визнати, спілкування у форматі подібних комунікаційних ресурсів навряд чи може претендувати на статус повноцінного, це, скоріше – квазіспілкування. До речі, китайськими лікарями Інтернет-залежність офіційно визнано хворобою, яку відповідно лікують в клініках.

Цікавими є також результати дослідження, проведеного групою вчених під керівництвом Пауля Кіршнера (PaulKirschner) в одному з американських університетів, які довели факт зниження академічної успішності на 20% у студентів, що активно користуються соціальними мережами. Крім того, ними виявлено: ті студенти, які не захоплюються соцмережами, приділяють навчанню в середньому на 88% більше часу (йдеться про час самостійної підготовки до занять).

Інший діяч, член редакційної ради енциклопедії «Британіка» Ніколас Карр (Nicholas Carr) у своїй резонансній книзі «The Shallows», стверджує: Інтернет привів до «побіжного читання, поспіху, відволікання думки і поверхневого засвоєння знань».

1.3.2.3 Підміна особистості

Основна проблема соціальних мереж - це довіра до тих, хто внесений до списку «друзів». Бездумна пропозиція «дружби» від невідомих або маловідомих людей може призвести до драматичних наслідків. Очевидно, що рівень довіри до тих, хто знаходиться в списку «друзів», за визначенням завжди буде вище, ніж до випадкових людей. З одного боку, це добре, оскільки формує лояльну аудиторію навколо компанії, бренду або людини. Але з іншого боку, це відкриває двері для зловмисників. «Дружній» стиль спілкування, поширений в соцмережах, оманливий - він може створити хибне відчуття, що навколо тільки друзі та доброзичливці, з якими можна ділитися будь-якою інформацією.

Достеменно невідомо, хто саме приховує свої дії під ім'ям друзів або прикривається фотографіями знайомих в профілі соціальної мережі. Це призводить до виникнення наступних видів загроз.

1.3.2.4 Розкриття дитиною шкільного віку конфіденційної інформації про себе і свою сім'ю

Відкритість соціальних мереж дає змогу зловмисникам легко реалізувати метод атаки «маскарад» – користувачі самі надають багато особистих даних. Вони сприймають соціальні мережі як електронні щоденники, забуваючи про те, що на відміну від їх паперових аналогів соціальні мережі загальнодоступні. Інформація, яка розміщена на сайтах соцмереж, доволі часто нагадує досьє на користувача і тому, природно, викликає інтерес у сторонніх людей. Існує навіть таке поняття, як «викрадення особистості». Сучасні соціальні мережі пропонують користувачу вказати про себе майже все: фото, відео, зв'язки, хобі, освіту, інформацію про місце навчання, праці, громадські місця, в яких буває, особисті думки і т.д. Такі

«вимоги» діти сприймають як необхідність, і заносять особисту інформацію в усі графи. Згідно з результатами досліджень ЮНІСЕФ «Покоління UaNet», багато дітей, активно спілкуючись в соцмережах, вказує номер мобільного телефону (46%), домашню адресу (36%), тощо. Складається враження, що для збору приватної інформації не обов'язково вдаватися до «зовнішнього спостереження» чи прослуховування засобів зв'язку – достатньо лише зайти в мережу Інтернет. Тим більше, що не завжди у користувача, який в свій час розмістив інформацію, є можливість її вилучити. Бо навіть у випадку вилучення даних, вони можуть залишитися у кеші пошукових серверів (наприклад, збережені Яндексом сторінки), а якщо інформація проіснувала достатньо довго - то попасти в webarchive.org.

Джерело ukrDay попереджає: Facebook, Twitter, Instagram, TikTok та їм подібні – потенційні інформатори. Безкарна, здавалося б, публічність у цих сервісах – питання часу. У базі даних зібраний гігантський компромат на всіх користувачів, який готовий, як переконаний ukrDay, опинитися в руках спецслужб. Підтвердження цьому – описане в Інтернет-ресурсах відкриття, зроблене на підставі тестувань австралійським технологом Ніком Цубріловічем (Nik Cubrilovic) – Facebook впровадив алгоритм, що дає змогу стежити за відвідуваннями його користувачами інших сайтів навіть у випадку, коли ті вийшли із сторінки соцмережі [24]. Коли користувач натиснув на кнопку «Вихід», Facebook замість того, щоб видалити cookie, просто підмінює їх, створюючи видимість виходу і водночас зберігаючи інформацію про акаунт користувача та інші унікальні дані, на основі яких може ідентифікувати його. Зараз Facebook порівнюють з паноптикумом – ідеальною, за проєктом англійського філософа Джеремі Бентама (Jeremy Bentham), будівлею для в'язниці, наглядач якої має можливість спостерігати за всіма ув'язненими, проте ув'язнені ніколи не знають, у який саме момент за ними стежать.

Нещодавно арсенал кіберзлочинців та Інтернет-маркетологів поповнився новим засобом крадіжки особистих даних – соціальними ботами. Соціальні боти (англ. socialbot) – це програми, створені для імітації поведінки

людей в соціальних мережах. Основним їх завданням є продукування несправжніх профілів, здатних ефективно викрадати персональні дані користувачів соціальних спільнот, а також штучно викликати, вводячи в оману, їх інтерес до тих чи інших веб-ресурсів. За інформацією канадських вчених з University of British Columbia Vancouver зараз придбати подібний набір скриптів можна в Інтернеті всього за 29$. Тобто подібні технології не просто існують, а й доступні для кожного охочого. Використовування таких програм можливе і для інших цілей: для розповсюдження спаму, шкідливого програмного забезпечення, проведення прихованих рекламних кампаній і т.д.

1.3.2.5 Перехід від віртуальних стосунків до реальних

Надамо статистичні дані тайських дослідників: 24% дітей віком 7–11 років зустрічалися з друзями, з якими познайомилися через соціальні мережі. Ще 24% дуже б хотіли це зробити. Більшість дітей ішли на зустріч зі своїми друзями, а 25% були самі без супроводу (незважаючи на свій вік). У 58% випадків зустріч з «другом» була неприємним сюрпризом, тому що діти зрозуміли, що їхній віртуальний «друг» брехав про себе. Підлітки були здивовані при зустрічі з тими, з ким мали зв'язки в Інтернеті в 48 % і шоковані у 28 % [20].

1.3.2.6 Кібербулінг

Кібербулінг (англ. cyberbullying від bully – хуліган, забіяка, грубіян, ґвалтівник) – переслідування повідомленнями, що містять образи, агресію, залякування; хуліганство; соціальне бойкотування за допомогою використання сучасних електронних технологій, у тому числі різних сервісів соціальної мережі.

Волонтерами Київського психологічного центру «Територія психотерапії та тренінгу «Психолог» проведене незалежне опитування київських школярів віком від 10 до 16 років. В опитуванні прийняли участь 346 охочих учнів. 62 % опитаних визнали застосування по відношенню до себе електронних технологій, які можна розцінювати проявом кібертероризму. Частіше всього це була нецензурна лайка (49%); пропозиції відвідати

порносайт, переглянути відео із сценами насильства (26%). Майже щочетвертого користувача мережі ображали, над ним насміхались. 26% респондентів засвідчували випадки шантажу та погроз на свою адресу. 54% молодих людей це дратувало, 40% відчували сором, у 14% опитаних це викликало страх. Майже 4% жертв кібербулінгу звертались за психологічною допомогою.

Згідно з дослідженнями компанії Harris Interactive більшість підлітків стверджують, що їхні однолітки займаються кібербулінгом, бо вважають це кумедним заняттям (81%); хочуть помститися комусь (64%); сприймають свою жертву хронічною невдахою (45%). Підлітки також переконані: кібербулери тому такі активні, бо не бояться відплати.

Методи кібербулінгу, використовувані у соціальних мережах для залякування і цькування своїх «потенційних жертв», вирізняються різноманітністю:

- злам сторінки для отримання особистої інформації про її власника з метою подальшого використання цієї інформації для шантажувань;
- блокування профілю жертви;
- розсилання масових скарг і претензій на власника профілю;
- створення профілю від імені жертви (англ. impersonation – удавання кого-небудь) та використання його для дискредитації цієї особи;
- переслідування (англ. harassment – приставання, домагання) – довготривале регулярне надсилання своїй «потенційній жертві» повідомлень, шантажування якимись фактами з її життя;
- троллінг (англ. trolling – «ловля риби на блешню») – розміщення в соціальних мережах провокаційних повідомлень з метою викликати флейм («суперечку заради суперечки») і тим самим спровокувати конфлікти між учасниками, взаємні образи шляхом порушення правил етичного кодексу Інтернет-взаємодії, тощо;

– флеймінг (англ. flaming – розпалювати) – це обмін, як правило, короткими емоційними репліками між двома користувачами соцмережі – агресором (іноді, їх може бути декілька) і «потенційною жертвою». Мета агресора – принизити «жертву» і отримати від цього моральне задоволення. Деколи така дискусія перетворюється на затяжний конфлікт – холівар (англ. holiwar – священна війна);

– онлайн-відчуження (остракізм, ізоляція, соціальне бойкотування). Будь-якій людині, а тим більше дитині, притаманне бажання бути прийнятим у суспільстві. Кіберостракізм у соцмережах проявляється у вигляді відсутності відповіді на миттєві повідомлення, а також через виключення із списку друзів чи групи. Відчуження у віртуальному просторі сприймається як соціальна смерть і може призвести до повного емоційного руйнування дитини;

– хеппіслепінг (англ. happyslapping – щасливе ляскання) – так називають відеоролики, в яких зняті сцени насильства над «потенційною жертвою». Найчастіше подібні ролики розміщуються, зрозуміло, без згоди жертви на таких ресурсах, де їх може переглядати велика кількість людей. Під цей критерій ідеально підпадають соціальні мережі.

1.3.2.7 Кібергрумінг

Кібергрумінг (англ. cybergrooming). Спеціальний термін «грумінг» означає встановлення дорослими людьми дружніх відносин з дитиною з метою вступу в сексуальний контакт. Знайомство в соціальній мережі здійснюється ними найчастіше від імені однолітка дитини. Он-лайн-хижаки добре знаються на особливостях дитячої психіки. Вони в курсі останніх музичних новинок і їм все відомо про хобі, якими найчастіше цікавляться діти. Вони уважно вислуховують дітей і «співчувають» їхнім проблемам. Спілкуючись особисто («в приваті»), кіберзлочинці входять у довіру до неї, намагаються дізнатися особисту інформацію і домовитися про зустріч. І вже під час зустрічі діти з'ясовують, що їх віртуальний друг зовсім не той, за кого себе видавав в Інтернеті: це доросла людина з корисливими і навіть нездоровими планами щодо їх стосунків. До речі, за статистикою

onGuardOnline [29], 22% молодих осіб у віці від 16 до 24 років взагалі не знають людей, з якими вони «дружать» віртуально. Найбільш вразливими до кібергрумінгу є молоді люди, яким притаманні такі риси:

- вони початківці в онлайні й незнайомі з «мережевим етикетом»;
- хочуть спробувати у житті щось нове, авантюрне;
- активно шукають уваги та дружби;
- бунтівні;
- ізольовані або самотні;
- їх приваблюють субкультури, що існують за межами їхнього власного, контрольованого батьками, світу.

1.3.2.8 Секстінг

Секстінг (англ. sexting – sex і texting, тобто «секс» і «обмін повідомленнями») – це своєрідний аналог ексгібіціонізму, пересилання особистих фотографій, повідомлень інтимного змісту за допомогою сучасних засобів зв'язку, в тому числі, засобами соціальних мереж.

Американські медики опублікували у журналі Archives of Pediatricsand Adolescent Medicine результати соціологічного дослідження, що стосується звичок сучасних підлітків. Середній вік опитаних – 15,8 років. 28% опитаних підлітків зізналися, що фотографували себе без одягу та пересилали ці пікантні зображення своїм знайомим, 57% заявили, що отримували повідомлення з проханням надіслати подібні світлини.

1.3.2.9 Споживацькі загрози

Зловмисники під різними приводами змушують дітей у соціальних мережах підключатися до платних послуг. На жаль, діти не завжди помічають підступ і не звертаються за допомогою до дорослих. Як приклад, можна навести послугу передплати на «преміальні» номери. Дитина прийнявши рішення «закачати» яку-небудь «безкоштовну» програму, останнє, що вона буде читати і то недбало (у чому не має сумніву), це умови угоди під час

завантаження дистрибутиву. А вони, як правило, містять пункт про обов'язкову передплату на пропоновані сервіси. Таким чином, і з'явиться заборгованість перед сайтом, котру необхідно буде погасити.

Ще один приклад. Сьогодні майже всі азартні комп'ютерні ігри з'явилися в додатки соціальних мереж. Для оплати використовується внутрішня валюта соціальної мережі. Відомі випадки, коли діти для підняття свого рейтингу витрачали реальні гроші батьків (шляхом надсилання SMS) за "золоті монети", що використовуються у грі.

1.3.2.10 Віруси

Користувач соцмереж має велику імовірність заразити комп'ютер вірусами. Соціальні сайти, пропонуючи широкий набір сервісів, як ігрових, так і для завантаження інформації різноманітної форми та змісту – фотографій, музики, відео, неявно піддають загрозі комп'ютер їх користувачів, оскільки останні можуть, під виглядом додатку скачати вірус чи троянську програму. Зацікавившись змістом листа від, так званого, друга, дитина, не задумуючись, вибере посилання, яке може перевести її на сайт, що завантажує на комп'ютер всілякі шкідливі програми. Серед таких програм, зокрема, можуть бути:

– програми клавіатурних шпигунів (англ. keylogger) – це програми, які відслідковують усі дії користувача на комп'ютері та інформацію, що на ньому вводиться, з метою її викрадення. Якщо користувач здійснює покупки або користується онлайн-банкінгом на цьому ж комп'ютері, то такі програми, зрозуміло, можуть викрасти паролі та логіни для Інтернет-банкінгу, дані про платіжну карточку, включаючи її номер, PIN-код та ім'я власника;

– вінлокери (англ. winlocker) – програми, які перекривають зображенням весь екран, пропонуючи при цьому користувачу заплатити певну, як правило, немалу суму, щоб розблокувати комп'ютер. Дуже часто вінлокери використовують світлини порнографічного змісту, супроводжуючи її погрозою заявити про користувача комп'ютера, як про любителя забороненого, у правоохоронні органи;

– потрапляння в бази розсилки спаму. Якщо електронна адреса користувача з'явиться у відкритому доступі, то вона з легкістю може потрапити до кіберзлочинця, який буде атакувати її незліченою кількістю спаму [20].

1.3.2.11 Злом, крадіжка паролів і фішинг

Оскільки для ідентифікації соціальні мережі використовують паролі, то досить дізнатися цю послідовність символів - і можна від чужого імені розсилати рекламу і здійснювати інші, в тому числі і заборонені, дії. Крім того, деякі компанії використовують соціальні мережі для просування власної продукції, а крадіжка пароля адміністратора групи дозволяє, по суті, вкрасти і саму групу. А для отримання конфіденційної інформації традиційно використовують фішинг, підставні сайти, соціальну інженерію і багато іншого. Декілька років тому в галереї німецького міста Кассель відкрилася незвичайна виставка. Замість творів мистецтва відвідувачам пропонувалося подивитися на 4,7 млн. роздрукованих паролів учасників соціальної мережі LinkedIn.

Зловмисники можуть використовувати вкрадені облікові записи з метою вразити якомога більше людей, які знаходяться у вас в друзях: попросити у них грошей або інфікувати їх комп'ютерним вірусом.

Цей тип шахрайства заснований на довірі до сім'ї і друзів, що дозволяє зловмисникам виманювати гроші. Якщо користувач пройде по посиланню нібито від члена родини або друга, то завантажить на свій комп'ютер вірус, який буде шукати важливу інформацію. Приманкою слугувало повідомлення на стіні від друга, який нібито хотів поділитися з даним користувачем чимось цікавим. І натиснувши на це посилання, користувач розсилав вірус всім своїм друзям.

Шляхом злому зловмисник може проникнути в соціальну мережу (у тому числі від імені того, хто представляє в ній компанію, організацію або бренд), розіслати за її списком друзів фішингових повідомлень і отримати

гроші або мотивувати одержувачів до яких-небудь негативних дій - зокрема, пройти по вказаному посиланню і запустити шкідливий код.

1.3.2.12 Витік персональних даних

Найбільша загроза соціальних мереж полягає в тому, що доступ до всієї особистої інформації є у великої групи людей, і вони можуть в будь-який момент її переглядати, навіть, якщо людина видалила щось з мережі. По-перше, це співробітники самої соціальної мережі: у них є доступ до баз даних, в яких міститься вся інформація, а також спеціальні інструменти входу в профайли користувачів, як, наприклад, спеціальний майстер-пароль в facebook, який дозволяє увійти в будь-який профайл.

Відомий викривач Джуліан Ассандж, засновник WikiLeaks, заявив, що Facebook має спеціальний інтерфейс, який використовує розвідка США. Все це цілком логічно: співробітники соціальних мереж не можуть не мати доступ, в цьому полягає їхня робота, а співробітники правоохоронних органів ловлять в мережах злочинців, однак це не рятує від небезпеки передачі даних третім особам, причому часто такими даними можуть бути цілі психологічні портрети або конфіденційна інформація [8].

Крім цього, адміністрація сайтів соціальних мереж часто «забуває» видаляти інформацію, видалену користувачами з їх персональних сторінок. У ході експерименту, проведеного вченими кембриджського університету, з'ясувалося, що багато популярних соціальних сервісів продовжують зберігати зображення, видалені користувачами. Експериментатори завантажили фотографії в користувальницькі профілі на сайтах, зберегли прямий URL кожного знімка, а потім видалили їх. У семи випадках фотографії, як і раніше були доступні за прямими посиланнями навіть через 30 днів з моменту вилучення. Зберігати видалені фото вже стало традицією соціальних мереж: видалити особисті фотографії, власноруч розміщені в соціальних мережах, може виявитися непосильним завданням для користувача. Навіть після деякого часу «видалені» користувачем фотографії продовжують залишатися у доступі, як у господаря профілю, так і у його гостей. Подібним чином,

адміністрація сайтів «забуває» видаляти й іншу інформацію, видалену користувачем з персональної сторінки в соціальних мережах [19].

Використання персональних даних різноманітно: від нав'язливої реклами до оформлення кредитів. Також популярність соціальних мереж може бути вигідна спецслужбам. Фахівці відзначають, що на популярних сайтах все частіше можна зустріти позначення військових частин і секретних підрозділів. А за допомогою даних про місце проживання користувачів сервісу обчислити локацію цих стратегічно важливих точок не так вже й складно. Інтерес спецслужб до соціальних мереж цілком зрозумілий. Кожен подібний сервіс увазі потужну систематизацію даних по містах, навчальних центрах, підприємствах і навіть військових частинах - із зазначенням дат служби та особистих анкет з набором фотографій. Зібравши ці дані і завдавши їх на карту, можна отримати повну картину дислокації військових частин з прив'язкою до часу.

Користувачі соціальних мереж повинні розуміти, що конфіденційність розміщеної у соціальній мережі інформації піддається сумніву. Так, навіть якщо вона не буде використана спецслужбами, її цілком можна викрасти. Витік особистих даних користувачів з вини мережі вже неодноразово спостерігалася. Однією з найбільших за розмірами можна вважати витік особистих даних 77 млн. Користувачів ігрової мережі playstationnetwork. Проблем з безпекою завжди багато і цілком імовірно, що більшість подібних витоків просто приховується від громадськості[8].

Усі перелічені загрози з боку соціальних мереж є актуальними і можуть бути реалізовані по відношенню до школярів.

1.4 Висновок. Постановка задачі

У даному розділі наведені загальні відомості про соціальні мережи, їх функціонал та особливості використання. Представлені результати досліджень особливостей використання соцмереж громадянами України

шкільного віку. Сформовано перелік загроз ІБ користувачів соцмереж та описані можливі загрози ІБ держави від користувачів соцмереж.

Враховуючи результати досліджень та аналізу загроз інформаційній безпеці школярів в соціальних мережах, в даній кваліфікаційній роботі необхідно вирішити наступні задачі:

– проаналізувати існуючі організаційні методи захисту громадян України шкільного віку від загроз ІБ в соцмережах;

– визначити особливості різних вікових груп школярів;

– запропонувати комплекс організаційних методів та заходів щодо підвищення рівня ІБ школярів України в соцмережах;

– розрахувати витрати на реалізацію системи інформаційної безпеки у приватній школі.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз існуючих методів захисту громадян України шкільного віку від загроз інформаційної безпеки в соціальних мережах

2.1.1 Застосування спеціальних соціальних мереж для школярів

Наразі в Україні з'являються освітні мережі, які дозволяють організувати навчально-виховний процес у школі, забезпечують соціальні функції спілкування, водночас дбаючи про інформаційну безпеку учнів.

Наприклад, всеукраїнська освітня мережа Щоденник.ua. У цій мережі нових користувачів додають тільки адміністратори шкіл, тому гарантується відсутність сторонніх: учні, вчителі й батьки реєструються на сайті після отримання в школі кодів запрошень. Усі коди зберігаються в адміністрації школи й не підлягають розголошенню. Для завершення реєстрації користувачі не тільки вводять код запрошення, але й підтверджують свої персональні дані.

Окрім того, адміністратори шкіл мають можливість контролювати всі дії користувачів всередині шкільної мережі і так захистити учнів від небажаної інформації.

Цей метод, разом із вказаними перевагами, має також й ряд недоліків:

1) такі соцмережі не мають популярності серед школярів. На це є декілька причин. По-перше, такі мережі менш яскраві, аніж популярні Instagram чи Facebook. По-друге, в них значно менше цікавої для учнів інформації, адже в популярних мережах школярі здобувають інформацію зі сторінок на цікаву школяреві тему, які створюють, адмініструють та наповнюють дорослі. Звісно, функцію наповнення безпечної соцмережі цікавою інформацією можна покласти на батьків та учителів, проте не так багато з них матимуть на це вільний час, бажання, необхідні уміння та смак. По-третє, думка про те, що усі дії в соцмережі контролюються адміністратором, відвертає школярів від бажання застосовувати таку соцмережу;

2) рівень захисту учнів залежить від рівню знань та умінь системного адміністратору школи. Більшості шкіл складно знайти відповідального фахівця з необхідним рівнем знань та умінь через значну обмеженість у фінансуванні, тому здатність системного адміністратору виконувати таку перевірку підлягає сумнівам;

3) усі коди зберігаються в адміністрації школи й не підлягають розголошенню. Проте через низький рівень фінансування, в школах рідко можна забезпечити ретельний захист таких кодів. Зазвичай інформація, що не підлягає розголошенню, в школах знаходиться у приймальні директора та через необхідність легкого доступу до неї необхідністю ретельного захисту нехтують, а теки, у яких зберігається така інформація, помічені надписами «Особові справи учнів 5-А класу», «Адреси і телефони працівників школи» тощо. Таким чином, за бажання поцупити подібну інформацію, у злочинця майже не буде перешкод;

4) залишається необхідність пояснення правил безпеки користування соцмережею, так як кіберзлочинцями чи шахраями (які будуть використовувати здобуту в цій мережі інформацію в інших місцях) можуть виявитися школярі, їхні батьки чи навіть вчителі.

Така соцмережа може слугувати організаційним методом протидії усім переліченим видам загроз, проте лише за умови усунення перелічених недоліків (що потребує значних коштів з боку кожної школи принаймні на ще одного системного адміністратора, який буде виконувати тільки адміністрування такої мережі) але лише в межі одного сайту.

Така нібито безпечна веб-сторінка може слугувати для школярів молодшого віку наочним прикладом соцмережі. На ній можна вивчати особливості поведінки в соцмережі, розглядати правила безпечної реєстрації в соцмережах тощо. В такому разі є необхідність наповнення мережі цікавою та корисною для учнів молодших класів інформацією, що сприятиме їхньому вихованню та створенню певного світогляду. При вступі до 6 класу таку

сторінку необхідно видалити задля забезпечення інформаційної безпеки (ІБ) учнів молодшого шкільного віку.

2.1.2 Використання програм батьківського контролю

Батьківський контроль – комплекс правил і заходів щодо запобігання негативного впливу Інтернету і комп'ютера на опікувану людину (зазвичай дитину). Для забезпечення «батьківського контролю» зазвичай використовується програмне забезпечення, додаткове або вбудоване (наприклад, в Windows 10).

Обмеження при такому контролі може здійснюватися як за часом (певні години протягом доби, або певні дні), так і по певних інтернет-ресурсах небажаної спрямованості.

Батьківський контроль буває активний і пасивний. До пасивних видів батьківського контролю відносяться такі методи як:

– обмеження на час використання комп'ютера (наприклад в робочі дні з 16:00 до 17:30, у вихідні з 10:00 до 18:00);

– обмеження на запуск програмних продуктів (можна вказати тільки ті програми, якими Ваша дитина може користуватися);

– обмеження на час використання тієї чи іншої програми (наприклад «гра» до 2-х годин на день);

– обмеження на відвідування інтернет ресурсів: відвідування тільки певних сайтів (зазначених у списку), заборона на відвідування сайтів певних тематик, блокування певних сайтів для відвідування.

До активних методів батьківського контролю належать:

– відстеження контенту сайтів відвідуваних дитиною;

– контроль листування по електронній пошті;

– контроль розміщуваних коментарів;

– контроль інформації, що розміщується в соціальних мережах;

– контроль листування в соціальних мережах;

– контроль програм, картинок, фільмів, що завантажуються.

Програми батьківського контролю призначені, в першу чергу, для створення обмежень дитині, вони покликані забезпечити її безпеку, захистити від того, що, можливо, їй ще рано знати і бачити.

До недоліків програм батьківського контролю можна віднести наступні:

1 Найважливіше в таких програмах – правильно налаштувати фільтри, регулярно їх оновлювати, аналізуючи сайти та їх наповнення, що відвідує школяр. По-перше, це займає багато часу. Можна, звісно, створити так званий «білий список», тобто перелік дозволених сайтів і на цьому припинити моніторинг. Проте це може звузити кругозір дитини відносно мережі Інтернет та сформує певні психічні комплекси та образи, що негативно вплине на подальше життя школяра. По-друге, налаштування таких програм потребує від користувача відносно високого рівня володіння комп'ютером, що є проблемою для багатьох сучасних батьків;

2 Школяр – юний дослідник. Тому, якщо існує можливість уникнути такої системи захисту – він її, скоріш за все, знайде;

3 Програми батьківського контролю захищають лише комп'ютер чи комп'ютерну мережу, у якій вони встановлені. Таким чином, цей метод підходить лише для захисту школяра в певному середовищі (вдома, у школі) і не дає ніякого захисту за межами цього середовища (комп'ютерні клуби, домашні комп'ютери знайомих тощо). Тому залишається необхідність пояснення школяреві правил поведінки у соціальних мережах та мережі Інтернет взагалі.

Такий метод може захистити від небажаного контенту, вірусів, попередити залежність від соціальних мереж. При регулярному моніторингу повідомлень, якими обмінюються школярі, можна відстежити реалізацію таких загроз як розкриття дитиною конфіденційної інформації про себе і свою сім'ю, перехід від віртуальних стосунків до реальних, кібербулінг, кібергрумінг, секстінг та споживацькі загрози. Проте будь-яка спроба батьків захистити свою дитину може сприйнятися як зрада у разі, якщо дитина не знала, що увесь її обмін повідомленнями відстежувався батьками.

2.1.3 Обмеження доступу

В разі можливості вдалої реалізації часткового обмеження доступу неповнолітніх до небажаної інформації, можна протидіяти таким загрозам як доступ до небажаного контенту та віруси. Проте від інших видів загроз може захистити лише повне обмеження доступу школярів у соцмережі. Реалізація повного обмеження доступу можлива в теорії. Деякі країни, наприклад, Китай, ввели обмеження по віку на доступ до певних сайтів шляхом перевірки документів перед виходом в Інтернет, проте через особливості українського менталітету реалізація такого обмеження не принесе бажаних результатів. Можна додавати на сайтах спливаюче вікно, що пропонує підтвердити наявність 18 років, проте це також ненадійний метод обмеження доступу.

2.2 Розробка організаційних методів виховання громадян з високим рівнем грамотності в питаннях інформаційної безпеки в соціальних мережах

2.2.1 Організаційні методи протидії з боку школи загрозам інформаційної безпеки громадян України шкільного віку в соціальних мережах

Найпоширеніший шлях виховання певної моделі поведінки та точки зору у школярів є вплив школи на учнів. За радянських часів через надмірну зайнятість більшості батьків, виховання підростаючого покоління було покладено на школи та позашкільні гуртки (музикальні та художні школи, спортивні секції тощо). В наш час ця тенденція дещо зберіглася, адже більшу частину свого життя (за винятком сну та вихідних) школяр проводить у школі. У школі він росте, розвивається, здобуває важливий для подальшого життя досвід. Отже, правила сучасного соціуму краще за все прививати майбутньому дорослому ще у школі або у дитячому садку. Тобто в установах, де людина зазвичай здобуває свій перший досвід спілкування у соціумі. Тому перед школою можна поставити мету щодо виховання громадянина, грамотного у питаннях особистої інформаційної безпеки.

Також великий вплив на школярів мають їхні батьки. І задля того, щоб батьки допомагали створенню правильного відношення учнів до питань ІБ в соцмережах, необхідно пояснити їхнім батькам найпростіші методи для підвищення особистої безпеки учнів в соціальних мережах. Таку задачу як ознайомлення батьків із методами протидії загрозам ІБ школярів також можна поставити перед школою.

Задля поліпшення комплексу заходів щодо підвищення обізнаності учнів в питаннях ІБ в соцмережах, необхідно регулярно аналізувати рівень знань учнів з приводу інформаційної безпеки. Анонімні опитування учнів з цього приводу делегуються шкільним психологам. Психолога також необхідно залучити для корекції запропонованих спеціалістами тематичних ігор (ігри мають бути різними задля того, аби діти не грали в одну гру двічі, бо це матиме негативні наслідки) відповідно до кожного окремого класу з урахуванням психологічних особливостей учнів класу та опитувань школярів і їх батьків.

Усі вчителі та психологи, залучені до програми підвищення рівня знань у сфері ІБ в соцмережах мають пройти спеціальне навчання, згідно якого вони не тільки отримають знання з ІБ, але й дізнаються про методи, якими варто чи не варто ці знання школярам та їх батькам передавати. Наголосимо на тому, що матеріали, необхідні вчителям та шкільним психологам для тематичної роботи зі школярами мають бути розроблені спеціалістами з питань ІБ з залученням шкільних психологів та вчителів, а не тільки шкільними вчителями, що дасть змогу підвищити рівень і якість інформування.

Матеріали та підходи пропонується розбивати згідно трьох (або більше) вікових груп. Сучасна школа передбачає розбиття учнів на молодшу (1-4 класи), середню (5-9 класи) та старшу школу (10-11 класи). Проте варто зазначити, що такий поділ школярів за віком не дає змогу розробляти дієві загальні методи впливу на учнів певної вікової категорії та матеріали для реалізації таких методів. Під час проходження науково-педагогічної практики у школі було проаналізовано інтереси школярів різного віку та особливості їх

поведінки та підходу до навчання, і було виявлено ряд деяких особливостей перехідних класів між прийнятими віковими поділами школярів. Учням 5 класу важче сприймати велику кількість текстового матеріалу і вони мають потребу у чомусь яскравому та легкому до сприйняття, так само як і учні, наприклад, 2 класу. А учні 9 класу вважають себе вже дорослими, і підходи, що спрацьовують у 6 чи 7 класі, їм здаються дитячими і нудними. Тому, враховуючи особливості сприймання навчального матеріалу в тій чи іншій формі, а також особливості інтересів та уподобань, школярів пропонується поділити на наступні вікові категорії:

- учні молодшого шкільного віку (1-5 клас);
- учні середнього шкільного віку (6-8 клас);
- учні старшого шкільного віку (9-11 клас).

2.2.1.1 Особливості молодшої вікової категорії та методи протидії загрозам ІБ шляхом підвищення обізнаності школярів

Учні 1-5 класу тільки набувають навичок навчання, тому матеріал для цієї вікової категорії повинен бути дуже легким для сприйняття. Також їм важко довго концентрувати увагу на чомусь одному, тому заняття має бути різноманітним (застосування друкованих матеріалів, робота в зошиті, перегляд мультфільму чи яскравої комп'ютерної презентації тощо).

Варто звернути увагу, що будь-який вчитель має великий вплив (як позитивний, так і негативний) на школярів молодшого шкільного віку, а класний керівник приділяє багато уваги вихованню своїх учнів. Також в початковій школі батьки більше уваги приділяють своїм дітям та частіше обговорюють з класним керівником питання виховання учня. Тому в цій віковій категорії головну роль з боку школи грає саме класний керівник. Адже саме від нього залежить, наскільки важливим для школярів та їхніх батьків стане те чи інше питання.

Для впливу на цю вікову категорію можна використовувати наступні методи виховання та навчання:

1) ознайомлення школярів із особливостями використання соціальних мереж та правилами спілкування в них;

2) створення (для наочності) разом із учнями сторінки в соцмережі для вигаданого хлопчика/дівчинки та заповнення разом із учнями необхідних при створенні сторінки даних, у формі гри наголосити на тому, які дані можна вносити в мережу, а які – ні;

3) внесення деяких змін в існуючу шкільну програму з метою підвищення рівня обізнаності школярів в питаннях ІБ в соцмережах;

4) використання яскравих та цікавих комп'ютерних презентацій та коротких мультфільмів для підвищення інтересу учнів до питання ІБ в соцмережах та кращого засвоєння матеріалу, що вивчається;

5) надання тематичного матеріалу у вигляді казок чи повчальних історій;

6) проведення шкільним психологом спеціальних тематичних ігор;

7) залучення батьків школярів до співпраці;

8) наголошення на важливості питання ІБ в соцмережах під час батьківських зборів, розповсюдження брошур із тематичними матеріалами та рекомендаціями.

Задля реалізації запропонованих методів необхідно забезпечити володіння необхідними знаннями (з питань ІБ у соцмережах та щодо методів розповсюдження цих знань серед батьків та учнів) та матеріалами (брошурами, мультфільмами, яскравими презентаціями тощо) класних керівників 1-5 класів, вчителів інформатики та шкільного психолога.

Для молодшого шкільного віку можна рекомендувати казки про ІБ для позакласного читання. Як і інші тематичні матеріали, казки повинні розроблятись фахівцями.

Також рекомендовано розробити та включити у вже існуючу програму «Сходинки до інформатики» тематичні ігри для учнів 2-5 класу задля можливості використання їх на уроках інформатики.

2.2.1.2 Особливості середньої вікової категорії учнів школи та методи протидії загрозам ІБ

Як і школярі молодшого шкільного віку, учні середнього шкільного віку полюбляють ігри та все яскраве, тому матеріали, що будуть демонструватися школярам, мають привертати увагу та бути цікавими. Проте, на відміну від учнів 1-5 класу, представники цієї вікової категорії вже більш свідомо сприймають навчальний матеріал. Вони аналізують усі знання, що отримали, через свій особистий світогляд, що вже почав формуватися. Тому необхідно додати завдання для осмислення тематичного матеріалу.

Для учнів середньої школи думка вчителів та батьків стає вже менш важливою, в той час як свої особисті погляди та точка зору однолітків та друзів із віком зростає. Тому виникає необхідність залучати учнів до висловлювання особистої думки, та поступово й непомітно її формувати.

Класні керівники 6-8 класів, зазвичай менше уваги приділяють вихованню своїх підопічних і більше переймаються рівнем успішності навчання та все частіше виникаючими конфліктами (часто з приводу розбіжностей точок зору). Таким чином, стає необхідність знизити відповідальність класного керівника за формування свідомості учнів та делегувати її вчителю інформатики та шкільному психологу.

Для підвищення рівня обізнаності учнів цієї вікової категорії можна застосовувати наступні методи:

1) внесення деяких змін в існуючу шкільну програму для підняття рівня знань школярів з питань ІБ в соцмережах та привернення їхньої уваги до можливих загроз;

2) проведення додаткових уроків про вибір надійних паролів та інших способів підвищення ІБ школярів;

3) використання спеціальних матеріалів (комп'ютерних презентацій, тематичного відео тощо) для проведення уроків та інших заходів;

4) обговорення зі школярами нагальності проблеми ІБ в соцмережах, проведення дебатів та семінарів на цю тематику;

5) задавання цікавих та оригінальних домашніх завдань для підвищення зацікавленості та обізнаності школярів в питаннях ІБ;

6) проведення психологами тематичних ігор для закріплення вивченого матеріалу та наочності загроз ІБ в соцмережах;

7) співпраця з батьками з метою всебічного впливу на школяра;

8) формування в школяреві відповідальної особистості з високим рівнем обізнаності в питаннях ІБ в соцмережах.

2.2.1.3 Особливості старшої вікової категорії школярів та методи протидії загрозам ІБ цієї вікової групи

Представники старшого шкільного віку більше спираються у формуванні своєї моделі поведінки на особисту думку та погляди однолітків та друзів. Зазвичай, вони вважають себе достатньо дорослими і бажають бути рівними старшім. Тому серед вчителів авторитет мають, в основному, ті, хто це розуміють та ставляться до учнів відповідно. Строгість вчителів в цьому віці у школярів може породжувати страх чи повагу, але точка зору суворих вчителів часто викликає бажання зробити все навпаки. Тому пояснення та обговорення особливо важливого матеріалу має проходити у вигляді напівдружніх бесід, де кожен бажаючий зможе висловити свою особисту думку та відкрито задавати будь-які питання по темі.

Так як школярі вважають себе дорослими, варто їм давати більш дорослі завдання: створити презентацію чи відзняти відео не тему ІБ в соцмережах, розробити власні методи протидії. Необхідно давати завдання, в яких учень зможе проявити себе, висловити особисту думку та бути почутим. Найкращі ідеї можна рекомендувати до включення у тому числі до національної програми підвищення рівня обізнаності у сфері ІБ громадян України.

Для поглиблення, оновлення та систематизації знань з ІБ в соцмережах в старшій віковій категорії школярів можна застосовувати наступні методи:

1) проведення лекцій-бесід та лекцій «від противного» для обговорення загроз ІБ в соцмережах та можливих шляхів їх уникнення;

2) завдання створення тематичних рекламних плакатів, комп'ютерних презентацій та інших проявів творчості школярів на тему ІБ в соцмережах та застереження для користувачів соціальних мереж;

3) залучення старшокласників до розробки лекцій на тему ІБ в соцмережах для учнів 1-8 класів;

4) залучення психологом школярів старшої вікової групи до проведення ігор з учнями початкової школи, оскільки, навчаючи інших, краще засвоюєш матеріал сам. Найкращі запропоновані ідеї також можна рекомендувати до включення у програму підвищення рівня обізнаності у сфері ІБ;

5) проведення психологічних ігор на тему ІБ в соцмережах;

6) проведення дебатів та семінарів на тему ІБ в соцмережах;

7) залучення старшокласників до суддівства на конкурсах з ІБ для учнів 1-8 класів;

8) обговорення реальних історій реалізацій загроз.

2.2.1.4 Залучення до проведення спеціальних уроків фахівців з питань ІБ

З особливою увагою школярі відносяться до лекцій-бесід, що проводять вузькі фахівці. Тому для підвищення рівня грамотності школярів в питаннях ІБ в соцмережах рекомендовано залучити фахівців з питань ІБ з підприємств, що займаються питаннями ІБ або з відділів безпеки банків чи заводів. Також залучення спеціалістів з ІБ до участі у батьківських зборах для підвищення рівня ефективності впливу на батьків.

2.2.1.5 Проведення тематичних конкурсів

Конкурси користуються особливою популярністю серед школярів. В творчих конкурсах для учнів школярі мають можливість проявити себе, розкрити той чи інший свій талант. Під час участі у конкурсах школярі охоче самостійно вивчають необхідний матеріал, швидко його опрацьовують за запам'ятовують. Самою масштабною реалізацією такого методу в Україні можна вважати загальнодержавний конкурс соціальної реклами з питань ІБ в соцмережах. Необхідно запропонувати учням у вигляді відео, плакату, презентації, вірша тощо представити свої ідеї щодо інформування населення про загрози ІБ в соцмережах. Найкращі ідеї надалі використовувати при створенні реальних соціальних реклам для показу по телебаченню та на білбордах. Для проведення такого конкурсу необхідне залучення спонсорів.

2.2.1.6 Підвищення рівня обізнаності батьків учнів в питаннях інформаційної безпеки в соціальних мережах

Батьки мають вплив на своїх дітей. І задля того, щоб батьки приймали участь у підвищенні рівня грамотності школярів з питань ІБ при використанні соцмереж, необхідно підвищення рівня обізнаності з цих питань їхніх батьків. Для цього необхідно розробити спеціальні брошури (наприклад, покрокову інструкцію для встановлення та використання програм батьківського контролю), проводити спеціальні навчальні лекції на батьківських зборах тощо.

2.2.1.7 Проведення семінарів і дебатів

Проведення класних, шкільних та міжшкільних семінарів та дебатів для учнів з метою обговорення проблем загроз ІБ соцмереж та можливих шляхів вирішення таких проблем. Для участі в таких заходах необхідно добре підготуватися, щоб мати змогу приводити аргументи на підтвердження своєї точки зору. Такий метод підвищення рівня знань з питань ІБ в соцмережах рекомендований для впливу на учнів, які знають та вміють більше за інших, мають великий потенціал, цілеспрямованих учнів та учнів з високою самооцінкою, тобто для тих учнів, які мають свою особисту думку та полюбляють її висказувати.

2.2.1.8 Проведення гри «Брейн-ринг»

Так само, як дебати та семінари, «Брейн-ринг» можна проводити на рівні класу, школи, району, міста тощо. Суть гри полягає в тому, що перед двома командами ставляться питання і першою відповідає та команда, що першою підняла прапорець (натиснула на кнопку). Такі ігри полюбляють товариські учні, учні, що користуються авторитетом у однолітків, а також учні, які полюбляють змагатися та перемагати. Зазвичай, до думки таких активних учнів прислуховуються однолітки та друзі, а тому формування їхнього відношення до питань ІБ соцмереж є необхідним.

2.2.2 Вплив за допомогою телебачення

2.2.2.1 Соціальна реклама

В наш час реклама – це найпопулярніший метод впливу на свідомість населення. Підприємці розміщують на телебаченні, у друкованих періодичних випусках та на біл-бордах рекламу товарів та послуг, які вони хочуть продати, політичні діячі проводять свої агітації за допомогою реклами. Тому відносної популярності зазнала і соціальна реклама.

Соціальна реклама — інформація будь-якого виду, розповсюджена в будь-якій формі, яка спрямована на досягнення суспільно корисних цілей, популяризацію загальнолюдських цінностей і розповсюдження якої не має на меті отримання матеріального прибутку. Соціальна реклама спрямована на зміну моделей суспільної поведінки і залучення уваги до проблем соціуму.

Соціальна реклама є одночасно видом мистецтва, компонентом соціальної політики та механізмом впливу на формування громадської думки. Найвідомішими прикладами такої реклами є кампанії по боротьбі з наркотиками, дотриманню правил дорожнього руху, пропаганда здорового способу життя, охорона навколишнього середовища та інші.

Враховуючи довірливість школярів телебаченню, як джерелу інформації, соціальна реклама на телебаченні може розглядатися як метод виховання громадян з високим рівнем грамотності в питаннях ІБ у соцмережах. Соціальна реклама має бути незвичайною, щоб привертати увагу. Вона має бути приємною на вигляд, аби її хотілося переглядати. Така реклама може мати жартівливий або ліричний характер. Для відбору найкращих ідей можна залучити спеціалістів з реклами або провести конкурс серед школярів чи серед студентів творчих та технічних професій. Головним недоліком такого методу є вартість трансляцій реклами по телебаченню. Прикладом можуть служити ціни (в гривнях) на одну трансляцію 30-секундної рекламу на телеканалі «СТБ» (табл 2.1).

Таблиця 2.1 – Вартість реклами на телеканалі СТБ

Час	06:00 - 09:00	09:00 - 11:00	11:00 - 18:00	18:00 - 00:00	00:00 - 02:00
Будні	29124,00	24314,00		34065,00	24314,00
Вихідні дні	24314,00	34065,00	29124,00	34065,00	24314,00

Як видно з таблиці 2.1, реалізація такого методу потребує залучення значних коштів. Проте, так як найчастіше замовниками такої реклами виступають державні органи або некомерційні організації, а рекламні агенції і розповсюджувачі реклами у ряді випадків виготовляють і розміщують її на безвідплатній основі або за зниженими цінами. Таким чином, можна спробувати домовитися з керівництвом телеканалу про безоплатну трансляцію соціальної реклами чи шукати та залучати спонсорів.

2.2.2.2 Мультфільми та мультсеріали

За статистикою, кожен третій прихильник мультсеріалу «Боб Губко – квадратні штани» - це доросла людина, а, отже, можна зробити висновок, що не лише діти, але й дорослі полюбляють дивитися мультфільми. На відміну від шкільних уроків, які значна частина школярів вважають нудним примусом, мультфільми розцінюються, як веселий відпочинок. Як школярі молодшого та середнього, так і старшого віку досить легко піддаються впливу популярних мультсеріалів. Вони щодня обговорюють події нових серій, співчувають улюбленим героям, хочуть бути схожими на них, намагаються в реальному житті повторювати чи відтворювати їхні вчинки. А тому мультфільми і, особливо, мультсеріали стають дуже привабливим методом виховання досвідченого в питаннях інформаційної безпеки покоління.

Задля того, щоб отримати якісний результат, важливо звернути увагу на наступні вимоги до створення мультфільму чи мультсеріалу (або циклу коротких мультфільмів на тему ІБ та правил користування комп'ютерами та іншими гаджетами), як методу протидії загрозам ІБ:

1) популярність. Навіть найцікавіший і найбільш інформаційний мультсеріал втрачає свою масову силу, як метод, якщо його ніхто не буде дивитись. Отже, необхідно розробити яскраву, заохочувальну рекламу та намагатись популяризувати цей мультсеріал (мультфільм) іншими методами (рекомендувати його батькам для перегляду дітьми, розповсюдити в соціальних мережах тощо);

2) яскравість. Діти, зазвичай, звертають увагу на усе яскраве. Тому дуже важливо, щоб мультсеріал був яскравим, з приємною графікою та симпатичними персонажами. Тьмяні мультсеріали, зазвичай, не викликають інтересу у дітей і вони можуть просто переключити канал, щоб подивитись більш цікаву, на думку школяра, передачу;

3) час і канал. Цей фактор впливає на популярність. Чим краще обраний час і чим популярніший канал, тим більший вплив матиме мультсеріал на свідомість школяра. Так як краще за все запам'ятовується матеріал, який людина дізнається зранку після сну та ввечері перед сном, короткі серії (5-7 хвилин) можна включини у ранкові програми, а вдень (коли школярі повертаються зі школи та відпочивають за переглядом телевізору) та ввечері транслювати більш тривалі серії (15-20 хвилин). Тривалість серії також має значення. Школярам молодшого віку буде складно сприймати інформацію протягом 15 хвилин в той час як школярам середнього та старшого шкільного віку серії у 5 хвилин буде замало і таких серій необхідно транслювати принаймні три-чотири за випуск;

4) сюжет. Щоб школяреві було легше запам'ятати правило, необхідно в якості звичайної життєвої ситуації сформулювати проблему та наприкінці серії дати чітку рекомендацію щодо дій при виникненні подібної проблеми та порад щодо уникнення таких ситуацій у майбутньому;

5) художність змісту. Зазвичай публіцистичний стиль визиває у школярів нудьгу, а деколи визиває відверту відразу. Те, що складне та нудне,

дуже складно запам'ятовується, бо не привертає увагу. Тому серії мають бути цікавими та легкими до сприйняття;

6) жарти. Веселі програми, фільми та серіали мають значну популярність у школярів будь-якого віку, а також у дорослих. Вдалі почуті жарти переказуються друзям, родичам, публікуються в соціальних мережах, що робить жарти добрим засобом розповсюдження інформації.

До переваг такого методу можна віднести:

- значну зацікавленість школярів мультфільмами та мультсеріалами;
- легкість сприйняття матеріалу;
- високій ступінь впливу;
- створення сучасних популярних тенденцій щодо ІБ в рамках певного віку та подальше їх розповсюдження.

Головним недоліком даного методу можна вважати витрати на реалізацію. Також необхідні кошти на рекламу тощо. Тому реалізація такого методу потребує пошуку та залучення спонсорів.

2.2.2.3 Серіали на шкільну тематику

Цей метод за вимогами та властивостями багато в чому схожий на попередній, але має ряд відмінностей. Серіали на шкільну тематику мають значну популярність у дітей старшого та середнього шкільного віку. Школярі, зазвичай, дуже емоційно сприймають події, що відбуваються з героями серіалу та проєктують їх на себе так, ніби вони переживають ці події разом із героями улюбленого серіалу. А тому такий метод можна вважати дуже ефективним.

Сформуємо вимоги до серіалу як методу підвищення обізнаності школярів в питаннях забезпечення ІБ в соцмережах:

1) популярність;

2) сюжет. Значну увагу при створенні такого серіалу необхідно звернути на сюжет. Він має захоплювати. Наприклад, це може бути історія про групу школярів, які протидіють кіберзлочинцям. В них має бути загальний головний ворог і кожної серії має траплятись якась проблема, яку вони будуть вирішувати. Також має бути загальний розвиток подій в серіалі, аби у

школяра-глядача виникала потреба дивитися кожну серію цього серіалу, не пропускаючи. Важливо, щоб група головних героїв була набором зовсім різних психотипів людей, не схожих один на одного, задля того, щоб школяр у комусь впізнав себе і відчував себе частиною серіалу. В серіалі мають бути бійки та небезпека задля привернення уваги чоловічої частини аудиторії та романтична лінія сюжету – для жіночої;

3) час і канал. Як вказувалося вище, канал має бути популярним. Такі серіали мають найбільшу популярність вдень, коли більшість школярів приходить зі школи та відпочивають. Після відпочинку школярі, зазвичай, йдуть виконувати домашні завдання, тому показ серій ввечері не має сенсу. Щодо тривалості, вона має становити 20-40 хвилин за серію. Короткі серії по 20-30 хвилин не бажано показувати по дві за випуск, тому що в такому разі школяр більше уваги зверне на сюжет, аніж на нову інформацію про ІБ, що він дізнався із серії;

4) відносна складність поданого матеріалу та необхідність аналізувати та логічно мислити. Якщо поданий матеріал буде занадто легким, ним школяр може знехтувати, якщо заскладним – занудьгувати, втратити віру у себе тощо. В будь-якому з перелічених випадків школяр припинить сприймати серіал серйозно. Почута інформація в серіалі має бути в дечому новою (щоб школяр розвивався), в дечому – вже йому відомою (задля повторення та підвищення інтересу за рахунок підвищення самооцінки).

Як і в випадку з мультсеріалами, головним недоліком даного методу можна вважати витрати на реалізацію. Тому реалізація такого методу також потребує пошуку та залучення спонсорів.

2.2.2.4 Розважально-пізнавальні програми

Розважальні програми, зазвичай, менш популярні серед школярів, проте вони можуть виконувати мету закріплення вивченого матеріалу чи для привернення уваги на деякі особливі моменти мульт- чи шкільному серіалі. Також в таких програмах можна викладати принципи та особливості ІБ не ховаючи у сюжет. Крім того, інформацію можна представляти у формі гри чи

завдання, щоб збільшити увагу під час перегляду серії (в такому випадку обов'язкове закріплення матеріалу після перегляду серії).

Сформуємо деякі критерії до такої розважально-пізнавальної програми:

1) програма має бути цікавою і дійсно розважальною задля привернення уваги школярів;

2) час і канал. Канал має бути популярним, а час – залежати від серій, які програма супроводжує. Якщо це коротка мультсерія (5-7 хв.), то краще за все зробити випуск в кілька хвилин перед серією та хвилину після. Якщо це серії мульт- та/або шкільного серіалу, то необхідно вставляти короткі перерви у вигляді програми між серіями та більш тривалий випуск перед та після показу усіх серій. Якщо це окрема програма, то критерії показу такі самі, як і для шкільного серіалу;

3) ведучі. В якості ведучих необхідно взяти дорослого або дітлахів, що завітали до дорослого, адже інакше школярі можуть не сприймати програму серйозно.

Враховуючи велику вартість ефірного часу, реалізація такого методу також потребує залучення спонсорів.

2.2.2.5 Виступ у шоу талантів представника інформаційної безпеки

В березні 2015 року старший лейтенант служби цивільного захисту Троян Віталій Віталійович відкривав кастинг сьомого сезону шоу-програми «Україна має талант». Під час виступу Віталій Віталійович прочитав реп на тему пожежної безпеки. Текст пісні був веселий та легкий для сприйняття, і під кінець виступу Віталію підспівувала значна частина аудиторії слухачів, запам'ятовуючи правила пожежної безпеки. Після цього, Віталія Віталійовича стали запрошувати у школи для проведення тематичних уроків про пожежну безпеку, а рівень знань школярів по цій темі підвищився.

Таким чином, можна звернути увагу до загроз ІБ в соцмережах за рахунок виступу в шоу талантів спеціалісту з ІБ з яскравим виступом на дану

тематику. Витрати на реалізацію такого методу невеликі. Головна складність реалізації – знайти талановитих бажаючих серед спеціалістів з ІБ.

2.2.3 Вплив через Інтернет

Усі методи, описані в підрозділі про телебачення, можливо використовувати в Інтернеті, завдяки чому можна заощадити на вартості телевізійного ефіру. Згідно результатів досліджень «Вплив ЗМІ на підростаюче покоління та формування комп'ютерної залежності у підлітків», описаних в першому розділі цієї кваліфікаційної роботи, Інтернет має найбільшу популярність серед джерел інформації. А тому інформація, що розповсюджується через Інтернет, може мати більший вплив, аніж через телебачення. Проте, варто зазначити, що кількість каналів на телебаченні обмежена, а програма фіксована, тобто, якщо школяр хоче подивитися телевізор, то вірогідність того, що він подивиться тематичний телевізійний матеріал, призначений для шкільного віку, значно збільшується, в той час як в Інтернеті користувач сам обирає, що, де і коли йому дивитися. З одного боку, зменшується настирливість пропагованої матеріалу, з іншого – зростає необхідність зацікавити школяра, щоб він передивися чи прочитав запропоновану інформацію.

2.2.3.1 Розміщення відео на YouTube

YouTube (укр. «Ютюб») — популярний відеохостинг, що надає послуги розміщення відеоматеріалів. Входить до трійки найбільш відвідуваних сайтів Інтернету. Користувачі можуть додавати, продивлятись і коментувати ті чи інші відеозаписи. Завдяки простоті та зручності використання, YouTube став одним із найпопулярніших місць для розміщення відеофайлів. Служба містить як професійні кліпи, так і аматорські відеозаписи, включаючи відеоблоги.

Кількість переглядів відеоматеріалів на сайті YouTube зросла до 2 млрд. на день, що майже вдвічі перевищує щоденну аудиторію трьох найпопулярніших американських телеканалів разом узятих. Таким чином, розміщене на сайті youtube.com відео має досить великі шанси до перегляду, а

при розміщенні відео, що підвищить обізнаність населення, на популярному серед молоді каналі, вірогідність перегляду такого відео школярами значно зростає.

Створення популярного каналу з регулярним додаванням нових унікальних відео не тільки підвищить ймовірність перегляду цих відео школярами України та їх батьками, а й дасть можливість заробити володарям каналу на розміщенні відео (за рахунок того, що володарям популярних каналів керівництво сайту youtube.com оплачує винагородження, розмір якого залежить від кількості переходів глядачів на розміщені на сайті реклами), що підвищує економічну ефективність цього методу.

2.2.3.2 Розповсюдження матеріалів через соціальні мережі

Найпопулярнішими шляхами розповсюдження матеріалів в соцмережах можна вважати:

– створення сторінки, на якій розміщувати необхідні тематичні матеріали;

– розміщення матеріалів в якості реклами на вже існуючих популярних сторінках.

Перший варіант потребує значних витрат сил та часу від адміністраторів сторінки для наповнення її цікавим матеріалом, підвищення рівня популярності та зацікавленості у матеріалах, пошуку інших користувачів, які б хотіли так само викладати у мережу цікаву інформацію за темою сторінки. Головною проблемою такого методу розповсюдження інформації є здобуття та підтримання популярності. Якщо взяти дві схожі за змістом сторінки, важко сказати, чому саме одна сторінка має мільйони читачів, а інша – лише кілька сотень. Проте, в разі, коли сторінка має велику популярність серед певної частки користувачів, вона також має дуже великий вплив на них. В багатьох школярів є звичка читати нові публікації улюбленої сторінки перед сном та одразу після. Інформація, що отримується в таких час засвоюється якнайкраще та має великий вплив на свідомість, особливо на ще не сформовану свідомість школяра.

Другий варіант є простішим та швидшим у реалізації, але потребує залучення коштів на рекламу. Суть такого методу полягає в тому, що певна інформація публікується в певний час на популярній сторінці. Зазвичай, для визначення часу публікації проводять дослідження активності на тій чи іншій сторінці певної вікової категорії. Подібне дослідження розглянуто у першому розділі цієї роботи.

Матеріали, опубліковані на таких сторінках, мають відповідати наступним вимогам:

– інформація має бути стислою, адже більшість школярів не витрачають свій час на читання довгих публікацій;

– розміщені матеріали мають викликати яскраві емоції: веселощі, співчування, занепокоєння тощо;

– тематичні матеріали необхідно викладати у вигляді картинки, що містить текст або короткого тексту на декілька рядків.

Після перегляду описаних матеріалів у читачів має формуватися певне уявлення про те, як потрібно поводитися в соціальних мережах, аби уникнути загроз ІБ.

2.2.3.3 Розміщення інформації на популярних сайтах та сайтах новин

Усю перелічену інформацію можна розміщувати на популярних серед школярів сайтах, а також на сайтах новин. Також на сайтах можна розміщувати інформацію про реальні історії реалізації загроз ІБ в соцмережах та рекомендації щодо уникнення таких ситуацій або алгоритми дій у випадку реалізацій таких загроз. Школярі мають досить розвинену уяву і такі історії справляють сильне враження на них. Особливо вони піддаються впливу, якщо уявляють себе на місці героїв історії і переживають прочитане. Тому історії мають бути яскравими, але цілком реалістичними, без прикрас.

2.2.4 Співпраця з керівництвом існуючих соціальних мереж

Так як найбільшою популярністю серед школярів користуються соцмережі інших держав, то законодавство України не може ніяким чином

вплинути на них, окрім як заборонити їх зовсім, що призведе до масових протестів з боку користувачів. Проте можна звернутися до керівництва тієї чи іншої соцмережі та запропонувати заходи, що сприятимуть підвищенню рівня ІБ користувачів.

Зміст застережливого повідомлення наступний: «Шахраї часто видають себе за ваших друзів і просять «нагадати» їм ваш номер телефону чи інші персональні дані. Потім вони використовують їх задля того, щоб викрасти ваші гроші. Зараз ви спілкуєтесь із людиною, з якою не товаришуєте в цій соціальній мережі – будьте обачні!».

2.2.5 Книги, комікси, журнали

Книги та комікси мають менше прихильників серед більшої кількості школярів, проте мають популярність серед меншості. Так само, як і в випадку з мульт- та шкільними серіалами, читач уявляє себе у ситуаціях, у яких опиняється головний герой та його друзі. Особливо захоплюють школярів детективні історії. Читаючи, кожен намагається пригадати все, що стало відомо з книги/коміксу, аби розкрити злочин раніше за головного героя, через що можна ефективно вкладати інформацію про загрози ІБ в соцмережах і методи протидії таким загрозам.

Такий метод можна запропонувати реалізувати, наприклад, письменникам та комікс-художникам, надати їм всі необхідні консультації та допомогти в пошуку спонсорів за необхідності.

2.2.6 Дитячі пісні та тематичні літні табори

Більшість школярів полюбляють співати пісні. Особливо разом. У формі пісні навіть вірші легше запам’ятовувати, чим часто користуються учні. Тому надання інформації щодо загроз ІБ та методів протидії їм у вигляді дитячих пісень буде сприйматись школярами із задоволенням. Проте для ще більшого засвоєння матеріалу необхідно мати потребу співати такі пісні. Таку можливість можуть надати уроки музики у школі учням молодшого та

середнього віку. Також особливою популярністю користуються пісні у літніх таборах.

Окрім тематичних пісень, в літніх таборах можна проводити конкурси та ігри на тематику ІБ в соцмережах. Відпочиваючи, школярі із задоволенням будуть грати у детективів, розв'язувати логічні завдання тощо. Тому створення такого тематичного літнього табору є незвичайним, проте дієвим методом підвищення рівня обізнаності з питань ІБ у соцмережах та інтересу до них.

2.2.7 Популяризація питань інформаційної безпеки серед населення

Якщо політичні діячі та журналісти почнуть обговорювати питання ІБ школярів в соцмережах і почнуть сприяти розробці та впровадженню, а також самі демонстративно вживати різноманітні заходи протидії загроз ІБ громадянам України шкільного віку задля попередження цих загроз, це питання почне обговорюватися як школярами, так і їх батьками, що сприятиме швидкому підвищенню рівню грамотності населення у сфері ІБ. По-перше, значна більшість населення навіть не задумується щодо небезпеки, що ховається за безпечністю соцмереж. Під час написання роботи було опитано багато громадян України з приводу їхньої думки щодо тих чи інших заходів протидії загрозам ІБ, більшість з яких були учнями середньої та старшої школи, а також батьками школярів. Усі відповідали охоче, лише згодом ставлячи питання щодо можливості небезпеки публікації персональних даних у соцмережах. Більшість після кількох прикладів можливої реалізації загроз діставали свої телефони, заходили на свої сторінки та обмежували доступ до персональних даних або зовсім видаляли їх. Інші казали, що обмежать доступ, тільки-но вийдуть до мережі. З цього довільного опитування легко зробити кілька припущень. По-перше, в більшості своїй населення не знає про загрози ІБ у соцмережах, а деякі навіть ніколи не задумувались про це питання. По-друге, вони хочуть про це дізнатися, але легкими та доступними шляхами.

Отже, просте обговорення (популяризація) теми ІБ в соцмережах можна розглядати як один з найважливіших методів протидії загрозам ІБ. При чому для реалізації цього методу не потрібно виділення значних коштів. Варто лише кілька разів, наприклад, в виступах політичних діячів на телебаченні торкнутися цієї теми або розповісти про неї в новинах, і про неї почнуть говорити народні маси.

2.3 Запропонований комплекс організаційних заходів для протидії загрозам інформаційної безпеки громадян України шкільного віку

Для підвищення обізнаності школярів рекомендується застосування організаційних методів, які передбачають:

– під час кожного інструктажу з техніки безпеки перед тим, як діти йдуть на канікули, класним керівникам необхідно звертати увагу учнів на питання ІБ в соцмережах згідно віку школярів;

– проведення психологом щороку різних тематичних ігор в кожному класі із зверненням уваги на необхідні в певному віці питання;

– проведення психологом опитувань задля подальшого поліпшення програми виховання громадян з високим рівнем грамотності в питаннях ІБ соцмереж;

– проведення загальношкільних батьківських зборів з метою розповсюдження брошури з покроковою інструкцією по встановленню та використанню безкоштовної програми батьківського контролю та загального пояснення необхідності таких заходів;

– для навчання учнів користуванню соцмережею та пояснення особливостей поведінки в соцмережах використовувати безпечну соцмережу для школярів, описану в даному розділі з урахуванням запропонованих змін з метою вилучення недоліків.

Комплекс заходів для молодшої вікової групи:

1) 1 клас.

Відповідальний - класний керівник:

– на перших батьківських зборах роздати батькам брошуру з правилами безпечного використання Інтернету школярами молодшого шкільного віку «Безпека дітей в Інтернеті»;

– провести виховну годину про важливість обережного розповсюдження персональних даних учнів та їх сімей, використовуючи спеціальну презентацію у вигляді казки;

Відповідальний - шкільний психолог: прийняти участь у батьківських зборах з метою пояснювання методів, якими можна чи не можна користуватись при проведенні бесіди на тему ІБ школярам.

2) 2 клас

Відповідальний - класний керівник:

– на батьківських зборах розповсюдити брошуру з інструкцією безпечного створення власної сторінки в соціальній мережі «Як створити безпечну сторінку в соціальній мережі» на випадок, якщо школярі забажають створити власну сторінку в соціальній мережі та усно прокоментувати її, звертаючи увагу на важливі питання;

– провести виховну годину про небезпеку спілкування з незнайомцями, в тому числі у соцмережах, використовуючи комп'ютерну презентацію або мультфільм;

– проведення конкурсу творчості створення соціальної реклами про ІБ в соцмережах;

– під час інструктажу з техніки безпеки перед тим, як діти ідуть на канікули, згадувати про важливість конфіденційності персональних даних та небезпеку спілкування з незнайомцями.

Відповідальний - шкільний психолог: прийняти участь у батьківських зборах з метою нагадування методів, якими можна чи не можна користуватись при проведенні бесіди на тему ІБ школярам.

3) 3 клас

Відповідальний - вчитель інформатики:

– розгляд безпечної поведінки в соцмережах в контексті уроку «Безпека в Інтернеті» в розділі «Пошук даних в Інтернеті», використовуючи комп'ютерну презентацію;

– створення сторінки для віртуального учня разом із школярами для наочності правил вірного з точки зору ІБ заповнення запропонованої при створенні анкети та поведінки у разі реалізації тієї чи іншої загрози;

– обговорення теми безпечної поведінки в Інтернеті під час інструктажу техніки безпеки на початку та наприкінці семестру;

– встановити зв'язок з батьками учнів через класного керівника задля закріплення матеріалу (попросити батьків розпитати своїх дітей про те, що вони знають про безпеку в Інтернеті).

Відповідальний - класний керівник: допомогти своєчасному встановленню зв'язку вчителя інформатики з батьками учнів.

4) 4 клас (за наявності)

Відповідальний - вчитель інформатики:

– повторення вивченого в 3 класі матеріалу, в тому числі питання безпеки користування Інтернетом;

– включити до уроків з розділу «Безпека дітей в Інтернеті» доповнення стосовно користування соцмережами на прикладі сторінки, створеної в 3 класі для віртуального учня та з використанням комп'ютерних презентацій, а саме:

1) на уроці «Безпечний Інтернет» розповісти про те, як безпечно здійснювати вхід в соціальні мережі;

2) на уроці «Веб-сторінка для дітей» розповісти про важливість особистих даних та приховання їх від сторонніх осіб;

3) на уроці «Електронна скринька та електронне спілкування» звернути увагу на такі питання безпеки як створення надійного паролю, заборону передачі логіну та паролю стороннім особам, розповісти про небезпеку спілкування з незнайомцями;

4) на уроці «Електронне листування» більш детально звернути увагу на вибір людей в мережі для спілкування;

5) на уроці «Етикет електронного спілкування» звернути увагу учнів на те, яку інформацію можна розповідати в соцмережі, а яку – ні;

– обговорення теми безпечного спілкування в соцмережах під час інструктажу техніки безпеки на початку та наприкінці семестру.

5) 5 клас

Відповідальний - вчитель інформатики:

– повторення вивченого в 3/4 класі матеріалу, в тому числі питання безпеки користування Інтернетом та спілкування в соцмережах;

– створити/підібрати картинки для створення презентації-фотоальбому на тему «Безпечна сторінка в соцмережі» для виконання учнями практичної роботи «Створення презентації-фотоальбому»;

– обговорення теми безпечного спілкування в соцмережах під час інструктажу техніки безпеки на початку та наприкінці семестру.

Відповідальний - класний керівник.

– на перших батьківських зборах роздати батькам брошуру з правилами безпечного використання Інтернету школярами молодшого шкільного віку «Безпека в Інтернеті»;

– провести виховну годину про важливість обережного розповсюдження персональних даних учнів та їх сімей з використанням тематичного мультфільму.

Відповідальний - шкільний психолог: прийняти участь у батьківських зборах з метою нагадування методів, якими можна чи не можна користуватись при проведенні бесіди на тему ІБ школярам.

Комплекс заходів для середньої вікової групи:

1) щосеместрове проведення тематичних дебатів чи семінарів для учнів 6-8 класів;

2) 6 клас

Відповідальний - вчитель інформатики:

– обговорення теми інформаційної безпеки під час інструктажу техніки безпеки;

– під час повторення вивченого матеріалу торкнутися теми безпеки створення сторінки в соцмережі та використанні Інтернета взагалі;

– в контексті уроку «Поняття про мультимедіа» розглянути особливості (з точки зору інформаційної безпеки) розміщення мультимедіа в соціальних мережах;

– провести додатковий урок на тему розповсюдження логіну та вибору якісного паролю, використовуючи тематичне відео.

3) 7 клас

Відповідальний - вчитель інформатики:

– обговорення теми інформаційної безпеки під час інструктажу техніки безпеки;

– під час повторення вивченого матеріалу торкнутися теми вибору безпечного паролю, особливостей безпечної поведінки в соціальних мережах;

– включити до уроків з розділу «Електронне листування» доповнення стосовно користування соцмережами з залученням комп'ютерних презентацій, а саме:

1) на уроці «Поштова служба Інтернету. Електронна скринька та електронне листування» провести аналогію з листуванням у соцмережах, обговорити особливості безпечного листування у соцмережах;

2) на уроці «Вкладання файлів. Перенаправлення повідомлень. Правила електронного листування» звернути увагу учнів на ретельність відбору інформації, що знаходиться у повідомленнях, що відправляються та вкладених файлах;

3) на уроці «Використання адресної книги. Операції над папками та листами» обговорити з учнями небезпеку додавання до списку друзів незнайомців;

– Задати особливе домашнє задання «Створюємо сторінку разом», згідно якого учень повинен розповісти батькам або іншим родичам про те, які дані можна публікувати, які – ні, допомогти створити власну сторінку у разі потреби.

4) 8 клас

Відповідальний – вчитель інформатики:

– обговорення теми інформаційної безпеки під час інструктажу техніки безпеки;

– під час повторення вивченого матеріалу пригадати особливості безпечної поведінки в соціальних мережах;

– в розділі «Комп'ютерні мережі» дати завдання підготовити доповідь на тему «Загрози соціальних мереж», організувати семінарське заняття на однойменну тему з метою її обговорення.

Комплекс заходів для старшої вікової групи:

1) проведення дебатів та семінарів на тему ІБ в соцмережах для учнів 9-11 класів;

2) залучення представників старшої вікової групи до суддівства на конкурсах та дебатах, що проводяться для учнів 6-8 класів;

3) 9 клас

Відповідальний - вчитель інформатики:

– обговорення теми інформаційної безпеки під час інструктажу техніки безпеки;

– під час повторення вивченого матеріалу пригадати особливості безпечної поведінки в соціальних мережах;

– провести додатковий урок-жарт «Подаруй шахраям зброю», в якому спростовуються усі заходи протидії загрозам і ситуація жартівливо доводиться до абсурду;

– в якості практичної роботи «Створення растрових зображень» - створення плакату, що закликає до безпечної поведінки в соціальних мережах.

6) 10 клас

Відповідальний - вчитель інформатики:

– обговорення теми інформаційної безпеки під час інструктажу техніки безпеки;

– під час повторення вивченого матеріалу пригадати особливості безпечної поведінки в соціальних мережах;

– провести додатковий урок-бесіду «Реальні випадки реалізації загроз інформаційної безпеки в соцмережах», в якому кожен учень зможе поділитися власним досвідом або досвідом своїх знайомих щодо цього питання.

7) 11 клас

Відповідальний - вчитель інформатики:

– обговорення теми інформаційної безпеки під час інструктажу техніки безпеки;

– під час повторення вивченого матеріалу пригадати особливості безпечної поведінки в соціальних мережах;

– провести додатковий урок на тему «Заробіток в соцмережах», в якому буде розглянуто не лише можливості заробітку учнів, але й приклади, як на них можуть заробляти кіберзлочинці;

– створення презентації на тему «Розумне використання соцмереж».

Перелічені заходи рекомендовано внести в календарні плани, для внесення змін у вже існуючі уроки за програмою необхідно розробити нові плани уроків з урахуванням змін, для додаткових уроків необхідно розробити нові плани уроків. До розробки нових планів уроків залучити авторів підручників з інформатики. Додаткові уроки проводити за рахунок годин резерву. Необхідні для проведення перелічених заходів тематичні матеріали розробити та надіслати усім школам.

2.4 Висновок

У даному розділі було проаналізовано основні методи протидії загрозам ІБ українських школярів у соцмережах, які застосовуються на сьогоднішній день. Були запропоновані методи, спрямовані на виховання громадян з високим рівнем обізнаності в питаннях ІБ в соцмережах за рахунок впливу на

них школи, батьків, ЗМІ та соціуму, вказані недоліки цих методів та шляхи реалізації.

Також у розділі запропоновано комплекс організаційних методів протидії загрозам ІБ громадян України різного шкільного віку в соцмережах шляхом виховання громадян з високим рівнем грамотності в питаннях ІБ, підвищення рівня знань з цих питань батьків школярів, вдосконалення існуючої безпечної соцмережі для школярів. Розрахунок витрат на впровадження запропонованого комплексу наведений в економічному розділі.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Метою виконання економічного розділу є визначення того, чи буде використання запропонованих засобів та заходів інформаційної безпеки вигідним. Впровадження заходів ІБ та їх обґрунтування, а також розрахунок проведено для приватної школи «Європейська гімназія» м. Дніпра.

3.1 Необхідність обґрунтування витрат на реалізацію політики безпеки.

Для цього визначено економічну ефективність використання основних результатів, що отримані в результаті виконання роботи.

Економічна доцільність визначається розрахунками:

- капітальних витрат, що потребує розроблена політика безпеки;
- експлуатаційних витрат;
- річного економічного ефекту від впровадження інформаційної політики безпеки.

Запропонована політика інформаційної безпеки передбачає необхідність витрат на її реалізацію. Заходами, що потребують витрат, є:

- оновлення ліцензій програмного забезпечення;
- навчання персоналу в питаннях інформаційної безпеки.

3.2 Визначення трудомісткості розробки політики безпеки інформації

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ год.} \quad (3.2)$$

Де $t_{тз}$ = 4 год. - тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ = 3 год. - тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ = 3 год. – тривалість процесу аналізу ризиків;

$t_{вз}$ = 4 год. – тривалість визначення вимог до заходів, методів та засобів захисту;

tозб = 3 год. – тривалість вибору основних рішень з забезпечення безпеки інформації;

tовр = 2 год. – тривалість організації виконання відновлювальних робіт забезпечення неперервного функціонування організації;

tд = 4 год.– тривалість документального оформлення політики безпеки.

t = 4 год + 3 год + 3 год + 4 год + 3 год + 2 год + 4 год = 23 год.

3.3 Розрахунок витрат на створення політики безпеки

$$Крп = Ззп + Змч, \quad (3.3)$$

де Крп – витрати на створення політики безпеки;

Ззп – заробітна плата спеціаліста з інформаційної безпеки;

Змч – вартість витрат машинного часу, що необхідні для створення політики безпеки.

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) та визначається за формулою:

$$Ззп = t * Зіб = 23 * 150 = 3450 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, год;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки становить 150 грн/год.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$Змч = t * Смч, \text{грн.}$$

де t – трудомісткість розробки політики безпеки інформації на ПК, год.;

Смч – вартість 1 години машинного часу ПК, грн/год.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = Р * tнал * Се + \frac{Фзал * На}{Fр} + \frac{Клпз * Напз}{Fр} =$$

$$= 0{,}3 * 2 * 1{,}68 + \frac{(6000 * 0{,}2)}{1920} + \frac{3000 * 0{,}2}{1920} =$$

$$= 1{,}01 + 0{,}63 + 0{,}31 = 1{,}95 \text{ грн/год.}$$

Де Р- встановлена потужність апаратури інформаційної безпеки, 0.3 кВт - середня потужність одного комп'ютера;

tнал – кількість машин на яких розроблюється політика безпеки;

Се – тариф на електричну енергію, 1,68 грн/кВт·год;

Фзал – залишкова вартість ПК на поточний рік, 6000 грн.;

На – річна норма амортизації на ПК, 0.2 частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, 0,2 частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення, 3000 грн.;

Fр – річний фонд робочого часу (за 40-годинного робочого тижня Fр = 1920 год.)

$$Змч = t * Смч = 23 * 1{,}95 = 44{,}85 \text{ грн.}$$
$$Крп = Ззп + Змч = 3450 + 44{,}85 = 3494{,}85 \text{ грн.}$$

3.4 Розрахунок (фіксованих) капітальних витрат.

Оновлення ліцензії системного, прикладного і спеціалізованого ПЗ: Avast Antivirus Pro Plus - 525 грн. (вартість ліцензії для одного ПК на рік), Windows 11 Pro — 1150 грн. на рік, MS Office 2019 – 2210 грн. на рік, Бухгалтерія А5 – 1000 грн. на рік. Необхідно оновлення ПЗ для 4 комп'ютерів.

Загальна вартість закупівель ліцензійного ПЗ:

$$Кзпз = 4 * 4885 \text{ грн} = 19540 \text{ грн.} \qquad (3.4)$$

Таким чином, капітальні (фіксовані) витрати на впровадження системи інформаційної безпеки складають:

$$К = Кпр + Кзпз + Крп + Каз + Кнавч + Кн$$

де Кпр – вартість розробки проєкту інформаційної безпеки та залучення для цього зовнішніх консультантів, 12000 грн.;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 19540 грн.;

Каз – вартість закупівель апаратного забезпечення та допоміжних матеріалів відсутня, оскільки за розробленими політики безпеки закупівля апаратного забезпечення не є необхідною.

Кнавч - витрати на навчання адміністратора безпеки, становлять 5000 грн.

Крп – вартість розробки політики безпеки інформації, 3494,85 грн.;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки відсутні, оскільки не закуповується апаратне забезпечення.

$$К = Кпр + Кзпз + Крп + Каз + Кнавч + Кн =$$
$$= 12000 + 19540 + 3494{,}85 + 5000 = 40034{,}85 \text{ грн.}$$

3.5 Розрахунок поточних (експлуатаційних) витрат.

- навчання персоналу в питаннях інформаційної безпеки;
- витрати на керування системою інформаційної безпеки.

1. Витрати на навчання персоналу в питаннях інформаційної безпеки включають в себе послуги сторонніх організацій, що створюють політику безпеки інформації та відповідно до неї розробляють інструкції для персоналу, що є користувачами системи. Вартість навчання адміністративного персоналу й кінцевих користувачів розглянутої системи:

Со = 3500 грн. – витрати на навчання персоналу.

2. Обов'язки з керування системою інформаційної безпеки виконує керівник та адміністратор безпеки (за відсутності керівника), тому річний фонд заробітної плати складає додаткову заробітну плату директора та системного адміністратора за рік:

$$Сз = Зк + Заб = 2000 + 1500 = 3500 \text{ грн. (за 1 місяць)} \quad (3.5)$$

$$Сз = 3500 * 12 = 42000 \text{ грн. (за 1 рік)}$$

де Зк – додаткова заробітна плата керівника, 24000 грн. на рік.

Заб – додаткова заробітна плата адміністратора безпеки, 18000 грн. на рік.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Се), визначається за формулою:

$$Се = Р * Fp * Це$$

де Р – встановлена потужність апаратури інформаційної безпеки (0,3 кВт*4 комп'ютерів = 1,2 кВт)

Fp = 12 міс * 20 робочих діб/міс * 8 робочих годин * 4 комп'ютерів = 7680 год – річний фонд робочого часу системи інформаційної безпеки;

Це = 1,68 грн за 1 кВт/год – тариф на електроенергію на 01.01.2023 року.

$$Се = 1,2 * 7680 * 1,68 = 15482,88 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Стос) визначаються у відсотках від вартості капітальних витрат (2%).

$$Стос = К * 0,02 = 40034,85 * 0,02 = 800,7 \text{ грн.}$$

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = Со + Сз + Се + Стос =$$

$$= 3500 + 42000 + 15482,88 + 800,7 = 61783,58 \text{ грн.}$$

Розрахунок оцінки величини збитку:

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки (Пп).

Таблиця 3.1 Заробітні плати працівників за місяць

Посада	Розмір зар. плати	Кількість співробітників	Витрати на зар. плату на міс., грн.
Директор	25000	1	25000
Адміністратор	15000	1	15000
Заступник директора	20000	1	20000
Системний адміністратор	20000	1	20000
Бухгалтер	15000	1	15000
Менеджер з продажів	15000	1	15000
Викладач	15000	10	150000
Прибиральниця	10000	2	20000
Охоронник	10000	2	20000
Завідувач господарчим відділом	12000	1	12000
		Сума	312000

Місячний фонд робочого часу складає 160 годин. Річний – 1920 годин. Час простою внаслідок атаки tп = 4 год.

$$Пп = (Зс/Fр) * tв = (312000/160) * 4 = 7800 \text{ грн.}$$

Витрати на відновлення працездатності системи включають кілька складових:

Пви – витрати на повторне введення інформації, грн.;

Ппв – витрати на відновлення системи, грн.;

Пзч – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви = 8 год.:

$$Пви = (312000/160) * 8 = 15600 \text{ грн.}$$

Витрати на відновлення системи визначаються часом відновлення після атаки tв = 4 год і розміром середньогодинної заробітної плати адміністратора безпеки:

$$Ппв = (20000/160) * 4 = 500$$

Витрати на відновлення працездатності системи:

$$Пв = Пви + Ппв + Пзч = 15600 + 500 + 4000 = 20100 \text{ грн.}$$

Пзч = 4000 грн. - вартість для витрат на заміну частин;

О = 3000000 грн. - обсяг чистого прибутку за рік.

Втрати від зниження працездатності атакованої системи:

$$V = \frac{О}{Fр} * (tп + tв + tви) = \frac{3000000}{1920} * (3 + 4 + 8) = 23437{,}5 \text{ грн.}$$

Fr – це річний фонд часу роботи відділення, 1920 годин;

tп – 4 годин простою після атаки;

tв – 4 годин відновлення після атаки;

tви – 8 годин повторного введення загубленої інформації під час атаки;

Таким чином, загальний збиток від атаки на ІКС відділення при реалізації загрози складе:

$$U = Пп + Пв + V = 7800 + 20100 + 23437{,}5 = 51337{,}5 \text{ грн.}$$

Таким чином, загальний збиток від атак на вузол або сегмент корпоративної мережі складе:

$$В = \sum_i \sum_n * U = 3 * 4 * 51337{,}5 \ = 616050 \text{ грн.}$$

де: і- число атакованих вузлів, 3 комп'ютери;

n – середнє число атак на рік, 4 рази.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням В – загального збитку від атаки; R – очікуваної ймовірності атаки на систему; С – щорічних витрат на експлуатацію системи інформаційної безпеки.

Ймовірність R (0…1). Якщо реалізація загроз найімовірніша 1 раз на 3 місяці, тобто 4 рази на рік, то R=0,25.

Загальний ефект від впровадження політики безпеки:

$$E = B * R - C = 616050 * 0{,}25 - 61783{,}58 = 92228{,}92 \text{ грн.}$$

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки:

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

- коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій To.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі.

Коефіцієнт ROSI розраховують за допомогою показників:

E – загальний ефект від впровадження системи інформаційної безпеки, грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

$$\text{ROSI} = \frac{E}{K} = \frac{92228{,}92}{40034{,}85} = 2{,}3$$

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження ПБ.

$$To = K/E = 1/\text{ROSI} = 1 / 2{,}3 = 0{,}43 \text{ років} = 5{,}16 \text{ місяців.}$$

3.6 Висновки до розділу

Розробка і впровадження політики інформаційної безпеки для приватної школи «Європейська гімназія» можна назвати економічно доцільними, так як витрати на її створення значно менші за суму збитків, завдяки невеликій вартості комплектуючих, необхідних для відновлення системи та її інформаційних ресурсів у разі успішних атак порушників.

Тому в результаті:

- капітальні витрати на впровадження інформаційної політики безпеки становлять 40034,85 грн.;
- експлуатаційні витрати на впровадження інформаційної політики безпеки становлять 61783,58 грн.;
- загальний збиток від атаки на вузол складає 616050 грн.;
- ефект від впровадження системи інформаційної безпеки становить 92228,92 грн.;
- термін окупності капітальних інвестицій складатиме 5,16 місяців.

Отже, економічна доцільність обґрунтована і впровадження інформаційної політики безпеки може бути ефективним та успішним.

ВИСНОВКИ

В ході дослідження питань, пов'язаних із станом захищеності громадян України шкільного віку в соціальних мережах, було наведено характеристику, функціонал та класифікацію соціальних мереж, представлено результати досліджень активності використання соціальних мереж громадянами України шкільного віку та проведений аналіз загроз ІБ з боку соцмереж, в тому числі школярів.

Враховуючи результати досліджень та аналізу загроз ІБ школярів в соціальних мережах, в даній кваліфікаційній роботі було поставлено та вирішено наступні задачі:

– проведено аналіз існуючих організаційних методів захисту учнів українських шкіл від загроз ІБ в соцмережах;

– проведено розбиття школярів на три вікові групи згідно особливостей сприйняття ними інформації, активності користування соцмережами та вподобань;

– запропонований комплекс організаційних методів та заходів щодо підвищення рівня ІБ школярів України в соцмережах.

В економічному розділі було розраховано витрати на розробку і впровадження політики інформаційної безпеки для приватної школи. Ефективність запропонованих заходів доведена.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1) Що таке соціальні мережі? (Електрон. ресурс) / Спосіб доступу: URL: http://h.ua/story/93865/ – Назва з екрана.

2) Соціальна мережа (Електрон. ресурс) / Спосіб доступу: URL: http://uk.wikipedia.org/wiki/Соціальна_мережа – Назва з екрана.

3) Ю.А. Данько соціальні мережі як форма сучасної комунікації: плюси і мінуси (Електрон. ресурс) / Спосіб доступу: URL: http://irbis-nbuv.gov.ua/ cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/cuc_.pdf – Назва з екрана.

4) Галіч Т. О. Соціальні інтернет-мережі та віртуалізація суспільного життя (Електрон. ресурс) / Спосіб доступу: URL: http://www.sociology.kharkov.ua/docs/ magazin/soc_fut/16.pdf – Назва з екрана.

5) Івашньова С.В. Використання соціальних сервісів та соціальних мереж в освіті (Електрон. ресурс) / Спосіб доступу: URL: http://irbis-nbuv.gov.ua/ cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Nzspp_5.pdf – Назва з екрана.

6) Як студенти використовують соцмережі (Електрон. ресурс) / Спосіб доступу: URL:http://www.osvita.org.ua/news/70779.html – Назва з екрана.

7) Київські школярі використовують Інтернет здебільшого для спілкування в соцмережах (Електрон. ресурс) / Спосіб доступу: URL: http://www.telekritika.ua/news/76743 – Назва з екрана.

8) І.М. Артамонова Інтеграція соціальних мереж та інтернет-змк: вплив на соціалізацію споживачів сучасних медіа (Електрон. ресурс) / Спосіб доступу: URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21

DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/drsk.pdf – Назва з екрана.

9) Хронологія подій закриття Ex.ua. (Електрон. ресурс) / Спосіб доступу: URL: http://tsn.ua/video/video-novini/hronologiyapodiy-zakrittya-ex-ua.html/ – Назва з екрана.

10) Найєм М. Хакери вийшли на зв'язок [Електронний ресурс] / М. Найєм. (Електрон. ресурс) / Спосіб доступу: URL:http://www.pravda.com.ua/articles/6948363/ – Назва з екрана.

11) "1+1 Медіа" просить керівників соцмереж заблокувати групи, які становлять загрозу нацбезпеці (Електрон. ресурс) / Спосіб доступу: URL: http://tsn.ua/politika/1-1-media-prosit-kerivnikiv-socmerezh-zablokuvati-grupi-yaki-stanovlyat-zagrozu-nacbezpeci-350992.html – Назва з екрана.

12) Наталія Кухарська, Віталій Кухарський. Загрози безпеці дітей у соціальних мережах (Електрон. ресурс) / Спосіб доступу: URL:http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/bezin_.pdf – Назва з екрана.

13) Брачевський С. Категорії загроз для дітей в Інтернеті (Електрон. ресурс) / Спосіб доступу: URL:http://krosha.net/article10022013kategorii-zagroz-ditej-internet.html – Назва з екрана.

14) Logging out of Facebook is not enough [Electronic recourse]. – Access mode: http://www.nikcub.com/posts/logging-out-offacebook-is-not-enough – Назва з екрана.

15) Socialbots used by researchers to «steal» Facebook data (Електрон. ресурс) / Спосіб доступу: URL:http://www.bbc.co.uk/news/technology-15553192 – Назва з екрана.

16) Безпечне користування сучасними інформаційно-комунікативними технологіями: методичні рекомендації (Електрон. ресурс) /

Спосіб доступу: URL:http://lib.selyam.net/tw_files2/urls_102/116/d-115783/7zdocs/1.pdf – Назва з екрана.

17) Тичковський Є. Що таке кібербулінг? Чи потрібно з ним боротись (Електрон. ресурс) / Спосіб доступу: URL:http://psiholog.com.ua/node/11?q=node /673 – Назва з екрана.

18) Moessner Chris Cyberbullying (Електрон. ресурс) / Спосіб доступу: URL:http://www.ncpc.org/resources/files/pdf/bullying/Cyberbullying%20Trends%20-%20Tudes.pdf – Назва з екрана.

19) Temple Jeff R. Teen Sexting and Its Association With Sexual Behaviors (Електрон. ресурс) / Спосіб доступу: URL: http://archpedi.jamanetwork.com/article.aspx?articleid=1212181 – Назва з екрана.

20) Доведено негативний вплив соціальних мереж на успішність (Електрон. ресурс) / Спосіб доступу: URL:http://aratta-ukraine.com/news_ua.php?id=11408 – Назва з екрана.

21) Гущина Н.І. Проблема захисту учнів від негативних впливів у соціальних мережах (Електрон. ресурс) / Спосіб доступу: URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/komp.pdf – Назва з екрана.

22) Волкова Н.П. Педагогіка (Електрон. ресурс).

23) Сучасні тренди кібербезпекової політики: висновки для України (Електрон. ресурс) / Спосіб доступу: URL: http://www.niss.gov.ua/articles/294/ – Назва з екрана.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1	30	
6	А4	Розділ 2	31	
7	А4	Розділ 3	9	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація_Дрожев.ppt

2 Кваліфікаційна робота_Дрожев.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22з-1 Дрожева А.В.

на тему: «Обґрунтування методів протидії загрозам інформаційної безпеки школярів в соціальних мережах»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 87 сторінках.

Тема кваліфікаційної роботи є актуальною, так як соціальні мережі набули широкої популярності, в тому числі у школярів, і від загроз інформаційної безпеки, що містять в собі соцмережі, необхідно захищати майбутнє України.

У першому розділі кваліфікаційної роботи наведена характеристика, функціонал та класифікація соціальних мереж, представлені результати досліджень активності використання соціальних мереж громадянами України шкільного віку та проведений аналіз загроз ІБ з боку соцмереж, в тому числі школярів.

У спеціальній частині проведено аналіз існуючих методів захисту громадян України шкільного віку від загроз ІБ в соціальних мережах та запропонований комплекс організаційних методів протидії загрозам ІБ школярам різних вікових груп при використанні соц.мереж.

Наукова новизна результатів даної кваліфікаційної роботи полягає у розробці комплексу організаційних методів підвищення рівня обізнаності громадян України шкільного віку з питань ІБ в соціальних мережах.

Практичне значення роботи полягає у можливості застосування результатів дослідження та запропонованих організаційних методів для забезпечення необхідного рівня інформаційної безпеки громадян України шкільного віку.

Перевагами кваліфікаційної роботи є проведення практичних досліджень щодо використання соціальних мереж серед школярів України, розбиття школярів на вікові групи з урахуванням особливостей їх інтересів та уподобань, а також сприймання ними навчального матеріалу. Застосування запропонованого комплексу організаційних методів та заходів протидії загрозам ІБ від соцмереж дозволить підвищити рівень ІБ громадян України шкільного віку.

Серед недоліків роботи слід відзначити: незначні відхилення від стандартів при оформленні пояснювальної записки, відставання від календарного плану виконання кваліфікаційної роботи, недостатньо уваги приділено іншим методам впливу, окрім шкіл, та опрацюванню методичних матеріалів з запропонованих методів.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Дрожев А.В. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доц. **Сафаров О.О.**