ПОСІБНИК З ІНТЕРНЕТ-ГРАМОТНОСТІ

“ Підтримка користувачів в онлайн-світі

www.coe.int/children

Будуємо Європу
для дітей та разом з дітьми

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

ПОСІБНИК З ІНТЕРНЕТ-ГРАМОТНОСТІ

Підтримка користувачів в онлайн-світі

Рада Європи

КИЇВ 2021

Авторський колектив:
Дженіс Річардсон, Елізабет Міловідов, Мартін Шмальцрід

Посібник з Інтернет грамотності / Дженіс Річардсон, Елізабет Міловідов, Мартін Шмальцрід. – Київ: ТОВ «Агентство «Україна», 2021. – 148 с.

ISBN 978-966-137-144-5

Посібник з Інтернет-грамотності це збірник інформаційних матеріалів, що упорядковані у шість тематичних розділів, що дозволяє користувачам легше завантажувати та роздруковувати розділи один за одним або окремо, залежно від своїх потреб. У кожному розділі подано огляд його змісту у вигляді контрольного списку. Всі розділи розглядають основні аспекти Інтернету, починаючи від необхідної інформації про те, як він працює і де зберігаються наші дані, до пошуку якісної інформації та зв'язку з людьми та знаннями, отримання допомоги та погляду в майбутнє, до якого нас можуть привести онлайн-технології.

Посібник пропонує інструментарій, спрямований на те, щоб допомогти користувачам орієнтуватися в мережі можливостей, що пропонуються Інтернетом. Даний посібник призначений для широкої громадськості, включаючи батьків, працівників освіти та творців політики. В посібнику надано детальну інформацію та ресурси для тих, хто захоче заглибитися в тематику Інтернет грамотності. Водночас він може бути ти корисним для підлітків та молодих людей віком до 30 років, які належать до найактивніших користувачів інформаційних технологій, а також формують нові тенденції.

ISBN 978-966-137-144-5

© Д. Річардсон, Е. Міловідов, 2021
© М. Шмальцрід, 2021

Зміст

Подяки

Дженіс Річардсон працює консультанткою з питань захисту прав дітей в Інтернеті уже кілька десятиріч і очолювала редакційну групу цього посібника. До 2014 року Дженіс була координаторкою створеної Європейською Комісією мережі Insafe, яка включає 30 країн, а останнім часом вона координує роботу мережі протидії цькуванню ENABLE; Дженіс також працює в Консультативній раді з питань безпеки при компанії Facebook.

Докторка права Елізабет Міловідов є консультанткою з питань безпеки в електронному середовищі з більш ніж 20-річним досвідом роботи адвокаткою, професоркою права та захисницею прав дітей. Вона вважає своїм завданням розширення прав і можливостей батьків і дітей у сфері Інтернету, інформаційних технологій і соціальних мереж, а також є засновницею вебсайту DigitalParentingCoach.com.

Мартін Шмальцрід є старшим співробітником із питань політики в COFACE (Конфедерації сімейних організацій в ЄС) і спеціалізується на створенні більш безпечного Інтернету та нових технологіях. Він є головою ради проєкту SIP BENCH III (огляд інструментів батьківського контролю) та взяв участь у численних проєктах та ініціативах ЄС, пов'язаних із цією сферою.

Передмова

Наскільки важливо бути Інтернет-грамотним? Коротка відповідь на це запитання цілком ясна: Дуже важливо. Кількість користувачів Інтернету швидко наближається до 3,5 мільярдів, близько 20% з яких перебувають у європейському регіоні. І хоча Інтернет пропонує потік інформації, яку ми можемо сприймати й ділитися нею, безпечна поведінка у складному онлайн-світі може бути складним завданням. Для цього потрібен базовий набір знань.

Цей посібник пропонує такий набір знань, викладених просто та легко для засвоєння. Це не абсолютно нове видання, а набір корисних порад щодо того, як дати собі раду зі щораз потужнішим потоком інформації, причому цей набір постійно розвивається. Зміст посібника однаково чітко викладено і в Інтернеті, у тому числі завдяки передовій графіці, відтак окремі розділи можуть бути представлені під час групових занять у навчальних класах чи громадських центрах. Таким чином, його можна використовувати як інструмент для навчальних цілей і для всіх вікових груп.

Прояснюючи незліченну кількість складних моментів, цей посібник пропонує проникливе розуміння етичних міркувань та ризиків, пов'язаних із обміном інформацією: якщо ми хочемо використовувати Інтернет, щоб втамувати спрагу до знань та поділитися своїми думками та поглядами, то ми повинні робити це відповідально. Принципи прав людини стосуються цифрового світу не менше, ніж офлайн-простору. Вони використовуються, наприклад, стосовно поваги до свободи вираження поглядів і приватності інших людей в онлайн-просторі, а також стосовно поваги до нашої свободи вираження поглядів та приватності з боку інших. Як гарантувати безпеку наших персональних даних? Що робити, якщо ми стикаємось із незаконним контентом або стаємо об'єктом цькувань чи мови ненависті? Ці теми та багато інших представлені таким чином, щоб надати практичні поради для зацікавленої громадськості, а також запросити читачів критично думати про те, що вони бачать і читають в Інтернеті, й робити зважений і безпечний вибір.

Якщо ми перебуваємо онлайн, щоб ділитися думками, ми одночасно формуємо знання та розуміння; ми можемо кидати виклик загальноприйнятій мудрості і творити мережі для позитивних змін. Це особливо очевидно для молоді, для якої Інтернет пропонує безмежні можливості досліджувати, вчитися, спілкуватися та творити, що, у свою чергу, безпосередньо сприяє її особистому розвитку. Він став для молодих людей основним джерелом свободи та інформації під час дорослішання та дає їм можливість здійснювати свої права та свободи онлайн. Хоча Інтернет таїть у собі потенційні підводні камені, можна вживати заходів безпеки та надавати допомогу в розумних межах. Щоб не відлякувати користувачів, особливо молодих, не слід представляти Інтернет як похмуру місцевість, обставлену попереджувальними знаками. Цей посібник є унікальним і цінним інструментом саме тому, що він має на меті надати підтримку у використанні Інтернету зі знанням справи, творчим підходом, за умов безпеки та свободи від страху. Якщо завдяки цьому посібнику діти зможуть скористатися безліччю можливостей, які пропонує Інтернет, одночасно із зміцненням своєї цифрової стійкості та усвідомленням власного потенціалу та обов'язків, ми вважатимемо, що посібник виконав свою місію.

Рада Європи пишається тим, що стежила за розвитком посібника, і вдячна багатьом особам, залученим протягом років до його первинного запуску й пізнішого перегляду та редагування. Зараз цей інструмент є ще багатшим джерелом якісної інформації для дітей, батьків, вчителів та творців політики 47 держав-членів організації, що дозволить їм максимально використовувати можливості Інтернету та підготувати майбутні покоління до його безпечного та впевненого використання.

Снежана Самарджич-Марковіч

Генеральна директорка
з питань демократії

Хрістос Гіакомопулос

Генеральний директор з питань прав людини та верховенства права

Вступ

> Грамотність – це місток від безталання до надії. Це бастіон боротьби проти бідності та будівельний матеріал розвитку,... платформа для демократизації та засіб просування культурної та національної ідентичності. ...Врешті, грамотність є шляхом до людського прогресу та засобом, завдяки якому кожен чоловік, жінка та дитина може повністю реалізувати свій потенціал.
>
> *Кофі Аннан, колишній Генеральний секретар ООН (січень 1997 – грудень 2006)*

Це друге видання Посібника з інтернет-грамотності, уперше опублікованого у 2003 році. Перше видання переглядалося раз на три роки, у 2006 та 2009 роках, щоб не відставати від швидких темпів розвитку в секторі онлайн-технологій. Хоча в цьому виданні використовується подібна структура, його зміст повністю оновлено та додано нові інформаційні матеріали, в яких особливу увагу звернено також і на технології завтрашнього дня.

Посібник призначений для широкої громадськості, включаючи сім'ї, працівників освіти та творців політики; однак у ньому також надано посилання на більш детальну інформацію та ресурси для тих, хто захоче заглибитися в ці теми. Водночас він має бути корисним для підлітків та молодих людей віком до 30 років, які належать до найактивніших користувачів інформаційних технологій, а також формують і творять нові тенденції.

Метою Посібника з інтернет-грамотності є передусім надати інформацію та сприяти роздумам про деякі складні етичні, соціологічні та культурні проблеми, які невід'ємно пов'язані з діяльністю у сфері цифрових технологій та медіа, що відіграє велику роль у житті більшості людей у багатьох частинах світу. Рада Європи, яка видає цей посібник, працює з 1949 року над тим, щоб просувати, захищати та розвивати права людини, демократію та верховенство права у своїх 47 державах-членах.

Оскільки за останні півстоліття інформаційні технології швидко увійшли в більшість сфер життя більшості людей, вони також мали вплив на права, обов'язки та свободи людини, і в той же час значно розширили наше уявлення про грамотність, яка лежить в основі цих прав, обов'язків і свобод. Посібник з інтернет-грамотності є одним із елементів великого набору інструментів Ради Європи, спрямованого на подолання багатьох проблем та використання багатьох можливостей, що з'явилися завдяки поширенню Інтернету. Ми згадуємо в посібнику деякі з цих інструментів.

Грамотність передбачає оволодіння сучасними інструментами спілкування як засобами вираження та розуміння думок, які раніше визначалися англійською як 3R (reading, (w)riting та (a) rithmetic, тобто читання, письмо та арифметика). Але коли ми використовуємо цифрові інструменти та платформи, щоб висловити свої думки, уже сама потужність цих інструментів і платформ та притаманна їм швидкість і миттєвість розповсюдження перетворюють грамотність на багатошарове поняття, з яким багато хто з нас досі не зовсім розібрався. Фотографії, відео, повідомлення з обмеженою кількістю знаків, смайлики та подкасти стали окремими мовами завдяки таким інструментам, як Instagram, Snapchat, Vine та Periscope, а взаємодія та реальне спілкування занадто часто є безликим процесом, що опосередковується електронними технологіями. Особливо це стосується молодих людей, котрі пишуть текстові повідомлення чи твіти, грають в електронні ігри та обмінюються зображеннями вдень та вночі в онлайн-світі, який вплетений і розмито інтегрований у те, що дорослі все ще називають «реальним світом».

Соціальні та культурні умовності перевертаються з ніг на голову, оскільки користувачі соціальних мереж «зафренджують» або «розфренджують» людей із протилежного краю світу, з якими вони навряд чи коли-небудь зустрінуться. Відносини дедалі частіше встановлюються онлайн, а ділові партнери також зустрічаються та створюють компанії через Інтернет, і все частіше він стає місцем, де люди вперше зустрічаються з супутником (супутницею) свого життя. Ці глибокі зміни перенесли відповідальність та підзвітність в основу базового набору навичок грамотності, вимагаючи ґрунтовного розуміння наших власних основних прав людини та поваги до прав інших, якщо ми хочемо уникнути підводних каменів і зробити позитивний внесок у розвиток сучасного суспільства.

Посібник з інтернет-грамотності подано як збірник інформаційних матеріалів у форматі, подібному до першого видання. Однак інформаційні матеріали тепер упорядковані у шість тематичних розділів, що дозволяє користувачам легше завантажувати та роздруковувати розділи один за одним або окремо, залежно від своїх бажань. У кожному розділі подано огляд його змісту у вигляді контрольного списку. Такий список є більш всеохопним, ніж простий покажчик, і полегшує ознайомлення з інформаційними матеріалами, пропонуючи короткий провідник із найбільш важливих питань, розглянутих у них. Узяті разом, ці розділи розглядають основні аспекти Інтернету, починаючи від необхідної інформації про те, як він працює і де зберігаються наші дані, до пошуку якісної інформації та зв'язку з людьми та знаннями, отримання допомоги та погляду в майбутнє, до якого нас можуть привести онлайн-технології. Ці розділи складають інструментарій, спрямований на те, щоб допомогти користувачам орієнтуватися в мережі можливостей, що пропонуються Інтернетом, а паралельно з цим освоїти способи, якими вони можуть сприяти формуванню онлайн-світу, а не формуватися ним.

Відповідно до характеру електронного носія, в якому вони представлені, ми прагнули зробити інформаційні матеріали досить короткими, зручними для читання та придатними для швидкого пошуку ідей, сигналів і корисних порад та посилань. Кожен такий матеріал починається з огляду сучасного стану розглянутої теми, за яким іде трохи повніше і точніше дослідження того, як цей інструмент, платформа або сервіс можуть бути використані в освітніх цілях для створення доданої вартості та нових можливостей. Потім ми звертаємо увагу користувачів на деякі етичні аспекти, які заслуговують на додаткове осмислення, але, як зазначалося вище, інформаційні технології постійно розвиваються, а отже, постійно з'являються нові етичні міркування. Розділ «Як це робити» у більшості інформаційних матеріалів є практичним посібником, який має на меті надати покрокову інформацію про те, як певні явища функціонують, або про те, як їх можна змусити функціонувати, щоб користувачі могли отримати максимум від інформаційних технологій.

Останні розділи кожного інформаційного матеріалу містять ідеї щодо їх використання під час класних занять, приклади належної практики та додаткову інформацію, яка широко варіюється від посилань на статті та каталоги до подальших застосувань цього конкретного інструменту чи сервісу. Ці сторінки можна розглядати як сховище «передових досягнень», відібраних кількома спеціалістами спеціально для користувачів цього посібника з досвіду установ, організацій та осіб, що працюють у всьому світі в соціальній, освітній, культурній сферах та у сфері захисту прав дітей. Ми доклали всіх зусиль для того, щоб усі надані рекомендації були актуальними, відповідними ситуації та надійними для використання у всіх вікових групах, якщо не зазначено інше. Утім, користувачі, безумовно, усвідомлюють, що в сучасному швидкозмінному світі щодня створюються і видаляються тисячі URL-адрес (Uniform Resource Locators, інакше їх називають «посиланнями» або «вебпосиланнями»). Відтак для жодного посібника, що стосується технологій в Інтернеті, не можна гарантувати, що вся інформація залишатиметься достовірною і що всі вміщені в ньому URL-адреси існуватимуть і надалі.

Відтак Посібник з інтернет-грамотності слід радше розглядати як миттєвий знімок певного часового моменту. На нього треба буде накладати нову інформацію, ідеї та поради, якщо ми хочемо зберегти його повну актуальність для цільової аудиторії. Ми запрошуємо читачів узяти участь у цьому еволюційному процесі, надсилаючи свої ідеї, ресурси та приклади належної практики до відділу Ради Європи в справах дітей за адресою: children@coe.int.

1. Інтернет: будь-коли, будь-де

> «Ми всі зараз під'єднані до Інтернету, як нейрони в гігантському мозку».
>
> *Стівен Гокінг, фізик-теоретик*

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 1 – ЯК ПІДКЛЮЧИТИСЯ

Чи переконалися ви, що ваше з'єднання з Інтернетом захищено шляхом налаштування антивіруса, брандмауера та встановлення пароля для вашого Wi-Fi-роутера?
Чи встановили ви політику прийнятного користування (яку іноді називають політикою відповідального користування) для тих, хто користується Інтернетом або отримує до нього доступ через вашу мережу та пристрої?
Чи створили ви «гостьові» облікові записи на пристроях, якими користуються ваші діти?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 2 – ПРИСУТНІСТЬ У ОНЛАЙН-ПРОСТОРІ ТА ХМАРНІ ТЕХНОЛОГІЇ

Чи помістили ви контактні дані на своєму вебсайті або в блозі? Чи вжили ви заходів щодо захисту вашої приватності онлайн?
Чи перевірили ви контент, який використовуєте для свого вебсайту/блогу, на відповідність законодавству про авторські права?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 3 – WEB 2.0, WEB 3.0 ТА ІНШІ

Систематично просіть дозволу на використання їхніх зображень у людей, зображених на фотографіях і відео, які ви розміщуєте онлайн. Рекомендації користувачів на сайтах подорожей і товарів можуть бути корисними, але чи впевнені ви, що вони справжні?
Згенерований користувачами контент сприяє творчості та свободі вираження поглядів, але також покладає на вас обов'язок попіклуватися про те, щоб перетворити Інтернет на краще місце.

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 4 – БЛОГИ ТА ВЛОГИ

Захистіть свою конфіденційність, використовуючи псевдонім та приховуючи певні персональні дані.
Захистіть свій блог або влог від хакерів, встановивши відповідні заходи безпеки та регулярно зберігаючи контент.
Розміщуйте контент у блозі з урахуванням його цілі та аудиторії.

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 5 – ІНТЕРНЕТ НА ХОДУ

З якого віку діти можуть безпечно починати користуватися мобільними пристроями, і які з них найбільше підходять для зовсім маленьких дітей?
Чи розумієте ви технології геолокації та Bluetooth достатньо, щоб комфортно та безпечно користуватися мобільними пристроями?
Мобільне навчання та мобільні гаманці – це сфери, в яких використання мобільних пристроїв змінює способи нашого навчання, роботи та покупок. Що ви знаєте про ці нещодавні зміни?

Інформаційний матеріал 1

Як підключитися

Інтернет – це всесвітня мережа комп'ютерів, пов'язаних між собою через сервери, які функціонують як вузли зв'язку[1]. У червні 2016 року в світі налічувалося 3,5 мільярда користувачів Інтернету, з яких 614 мільйонів жили в Європі[2].

Як працює Інтернет і чому важливо знати про цей процес? Ви, швидше за все, вже користуєтесь Інтернетом щодня, навіть частіше, ніж велосипедом чи машиною. Хоча вам не потрібно знати всіх технічних деталей про те, як працює Інтернет, ви повинні принаймні мати базове уявлення про те, як це працює, подібно до того, як люди знають, як змінити шину свого велосипеда або перевірити рівень мастила у автомобілі.

Вдома ви, швидше за все, підключені до Інтернету за допомогою роутера, цієї таємничої коробки, яка підключається або до телефонної лінії, або до телевізійного кабелю. Всі ваші пристрої, будь то смартфон чи комп'ютери, підключені до цього роутера або через кабель Ethernet або через Wi-Fi.

1. http://en.wikipedia.org/wiki/Node_%28networking%29
2. www.Internetworldstats.com/stats.htm

А тепер уявіть, що ваш роутер був підключений кабелем до роутера ваших сусідів, а роутер вашого сусіда – до сусіднього будинку тощо. Саме таким є Інтернет у менших масштабах. Інтернет – це просто величезна кількість роутерів, підключених один до одного, які дозволяють пересилати та передавати інформацію (дані, що містять електронні листи, зображення, відео тощо) з однієї точки (наприклад, домашнього комп'ютера) в іншу (смартфон вашого друга, який перебуває у відпустці в іншому кінці світу).

Хоч як дивно це звучить, існують величезні підводні кабелі, які тягнуться під океаном між усіма континентами безпосередньо до пунктів виходу кабелів на берег, у яких вони підключаються до наземної інфраструктури (як правило, телефонних ліній).

Тож просто уявіть, що щоразу, коли ви надсилаєте фотографію з комп'ютера другові, трапляється ось що: ваша картинка розбивається на крихітні шматочки даних, які називаються пакетами, які позначені більш-менш як конверт на пошті (пункт призначення, місце походження та інформація про те, як знову зібрати цей масив даних, щоб скомпонувати ваше зображення). Замість такої інформації, як назва вулиці та номер будинку, пакети даних містять IP-адресу[3] того місця, куди їх було надіслано, та IP-адресу, на яку вони повинні надійти. Потім вони проходять через телефонну лінію до об'єктів вашого Інтернет-провайдера, які підключені до магістральної мережі Інтернет (це величезна кількість взаємопов'язаних роутерів, про які ми вже писали). Роутери переспрямовують ці пакети кілька разів, поки вони не досягнуть місця призначення (це називається числом стрибків). Але що насправді є місцем призначення вашого знімка? Наприклад, якщо ви надсилаєте зображення електронною поштою, місцем призначення є не комп'ютер вашого друга, а центри обробки даних поштового клієнта, яким користується ваш друг.

Центри обробки даних – це величезні склади, заповнені роутерами та жорсткими дисками. Ваше зображення зберігатиметься на декількох жорстких дисках (для захисту даних у разі несправності якогось із них). Наприклад, якщо ваш друг використовує Gmail, то зображення, яке ви надіслали йому, може фізично зберігатися в одному з центрів обробки даних Google, розташованих у США, Ірландії, Бельгії, Нідерландах та багатьох інших країнах[4]. І ваш друг/подруга, коли він/вона хоче подивитися на зображення, надсилає запит зі свого комп'ютера, який переспрямовується через магістральну мережу Інтернет аж до того центру обробки даних, який потім надсилає дані з вашим зображенням на екран його/її комп'ютера.

УПРАВЛІННЯ

Але як узагалі був створений Інтернет? Хто відповідає за підтримку наявної інфраструктури та створення нової? Хто ухвалює рішення щодо таких стандартів, як IP-адреси?

Хоча ідея гіперпосилань та взаємопов'язаних вебсторінок виникла у Тіма Бернерса-Лі та Роберта Кайо, коли вони працювали у центрі CERN у Швейцарії, перша взаємопов'язана мережа під назвою ARPANET була створена як міжуніверситетська мережа в США[5].

Тому найперший орган, який відповідав за розподіл унікальних «адрес», тобто, по суті, дозволяв комусь під'єднуватися до мережі, було створено в США (IANA – Internet Assigned Numbers Authority, Управління з присвоєння інтернетних номерів).

Мірою зростання Інтернету зростала й потреба у кращій координації роботи з його розвитку, обслуговування, стабільності та безпеки. Міністерство торгівлі США наполягало на реформі IANA, яке в 1998 році перетворилося на ICANN[6] (the Internet Corporation for Assigned Names and Numbers, Інтернет-корпорація з присвоєння імен і номерів). ICANN була офіційно створена як некомерційна корпорація «для благодійних та суспільних цілей» із сильною роллю підходу до управління «знизу вгору», що полягає у координації зусиль тисяч зацікавлених сторін по всьому світу, включаючи зацікавлені сторони приватного сектору, організації громадянського суспільства та уряди. Однак вона стикається з потужною критикою та закликами до реформ з боку різних країн світу через свої зв'язки з урядом США та ризик надмірного представлення інтересів США.

У відповідь ICANN відкрила свою діяльність для широкого кола зацікавлених сторін, включаючи 111 держав і низку спостерігачів, таких як ключові телекомунікаційні організації та Рада Європи.

3. https://en.wikipedia.org/wiki/IP_address
4. http://www.google.com/about/datacenters/inside/locations/index.html
5. https://en.wikipedia.org/wiki/World_Wide_Web
6. https://www.icann.org/

Але ICANN і надалі критикували за відсутність внеску широких мас до її рішень та більш широких консультацій із зацікавленими сторонами, що спонукало Організацію Об'єднаних Націй створити в 2006 році Форум із управління Інтернетом (IGF, ФУІ).

IGF збирається щороку та надає можливість широкому колу зацікавлених сторін, включаючи молодь, поділитися своїми поглядами на майбутнє Інтернету.

КОРИСТЬ ДЛЯ ОСВІТИ

- Інтернет пропонує доступ до безлічі нових ідей, ресурсів, можливостей для навчання, інформації та послуг.
- Інтернет сприяє транскордонному обміну досвідом та спілкуванню між користувачами різними способами: на форумах, електронною поштою, в соціальних мережах, чатах, відеоконференціях тощо. Відтак він надає учням можливість брати участь у проєктах та співпрацювати з іншими учнями без необхідності дорогих подорожей.
- Інтернет робить інструменти дослідження доступними навіть для тих, хто не є постійним відвідувачем якоїсь традиційної бібліотеки.
- За допомогою додаткових пристроїв та програмного забезпечення, Інтернет може відкрити нові можливості для людей із особливими потребами.
- Дізнаючись про те, як управляється Інтернет, усі громадяни отримують змогу брати участь у ключових рішеннях, які визначатимуть його майбутнє.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Майте на увазі, що Інтернет часто створює помилкове відчуття анонімності. З огляду на те, як він працює, ви завжди залишаєте слід, коли заходите в Інтернет (ваша IP-адреса є цим слідом).
- Як і в офлайн-світі, тут існують шахрайство, неправдива інформація та інформація, до якої не повинні мати доступ діти.
- Хоча Інтернет пропонує низку нових можливостей, рішення за допомогою інформаційних технологій не завжди кращі за традиційні. Наприклад, електронна пошта спричинила революцію у спілкуванні, і хоча відеоконференції можуть створити відчуття «майже присутності», вони ніколи не замінять спілкування віч-на-віч.
- Управління Інтернетом може мати величезний вплив на ваш досвід роботи у ньому, оскільки від нього залежить дотримання таких принципів, як анонімність або мережевий нейтралітет. Постійно відбувається боротьба між принципом вільного та відкритого Інтернету та тими, хто бажає контролювати його. Деякі компанії намагаються перенаправити трафік на власні вебсайти, застосунки чи сервіси, надаючи «безкоштовні» тарифні плани мобільного Інтернету, обмежені цими вебсайтами, програмами чи сервісами, та стягуючи плату за відвідування інших[7]. Наприклад, Facebook створив портал «Internet.org», який є домашньою сторінкою за замовчуванням для всіх користувачів, які підключаються до мережі через Інтернет-сервіс Facebook в різних частинах світу, особливо у країнах, що розвиваються[8].

ЯК ЦЕ

- Практично всі пристрої, які люди купують в наш час, здатні підключатися до Інтернету через Wi-Fi або мобільний доступ до Інтернету (наприклад, смартфони та планшети) або через кабель Ethernet (більшість комп'ютерів оснащені портом Ethernet).

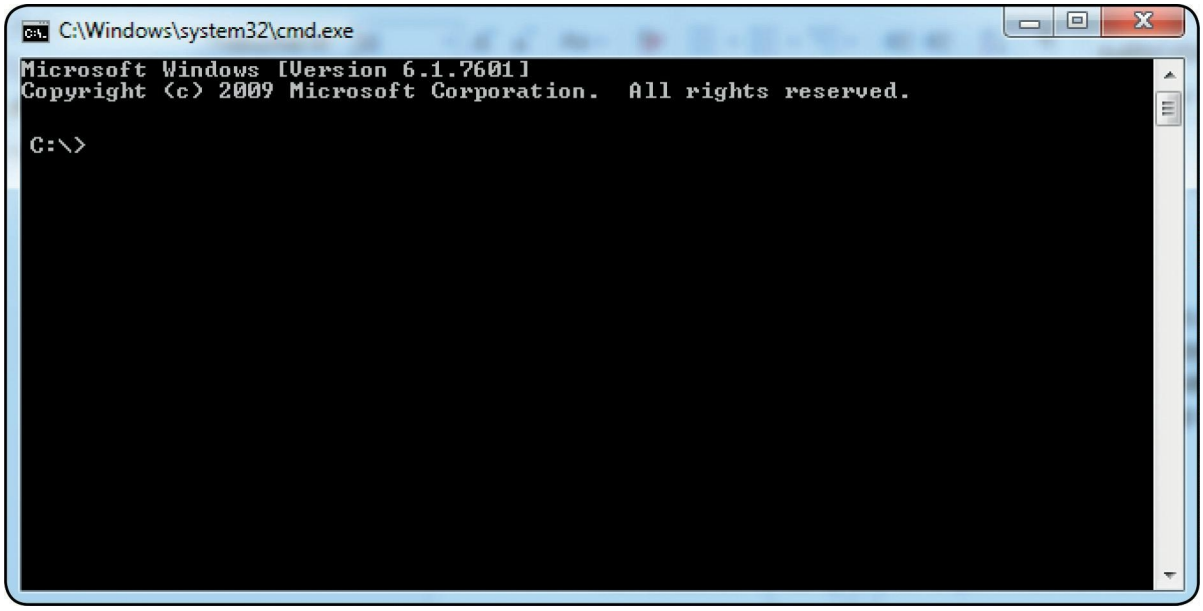
7. https://en.wikipedia.org/wiki/Zero-rating
8. https://en.wikipedia.org/wiki/Internet.org

- Є два основні варіанти для підключення до Інтернету:
  - Зверніться до інтернет-провайдера (як правило, це телефонна або кабельна компанія), який надасть вам ім'я користувача та пароль, а іноді ще й модем/роутер для підключення до Інтернету за допомогою вашої телефонної лінії або телевізійного кабелю.
  - Отримайте тарифний план «мобільний Інтернет» від свого оператора мобільного зв'язку. Майте на увазі, що обмеження на обсяг даних, які ви можете завантажити/вивантажити, все ще досить значні для мобільного Інтернету, хоча вони будуть поступово зменшуватися, оскільки все більше операторів впроваджують стандарти мобільного зв'язку 4G або 5G (зі значним збільшенням швидкості).
- Також з'являється дедалі більше «відкритих» точок доступу Wi-Fi, якими ви можете користуватися для безкоштовного підключення до Інтернету. Їх можна знайти в різних громадських місцях, таких як публічні бібліотеки, а також у барах, ресторанах та торгових центрах. У більшості випадків перед тим, як підключитися, вам буде запропоновано виконати одну або декілька з наступних дій: прийняти умови використання, створити обліковий запис, використовуючи свою електронну адресу (пам'ятайте, що ваша електронна пошта може потім використовуватися для надсилання вам реклами, тому обов'язково створіть окрему адресу електронної пошти спеціально для цих ситуацій) або ввести пароль для підключення до Інтернету. Наприклад, у барах, ресторанах або готелях «відкритий» Wi-Fi часто доступний лише для клієнтів, тому вам доведеться попросити співробітника надати вам пароль. Ніколи не діліться конфіденційними даними та не виконуйте конфіденційні операції, такі як мобільний банкінг, через загальнодоступні точки доступу Wi-Fi.
- Більшість інтернет-провайдерів нададуть вам заздалегідь налаштований роутер, який вам просто потрібно буде під'єднати до своєї телефонної/кабельної лінії, щоб підключитися. Іноді роутер буде потрібно купити та налаштувати самому. Обов'язково уточніть у свого інтернет-провайдера, чи сумісний роутер, який у вас є, або який ви маєте намір придбати, із вимогами вашої угоди про доступ до Інтернету!

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

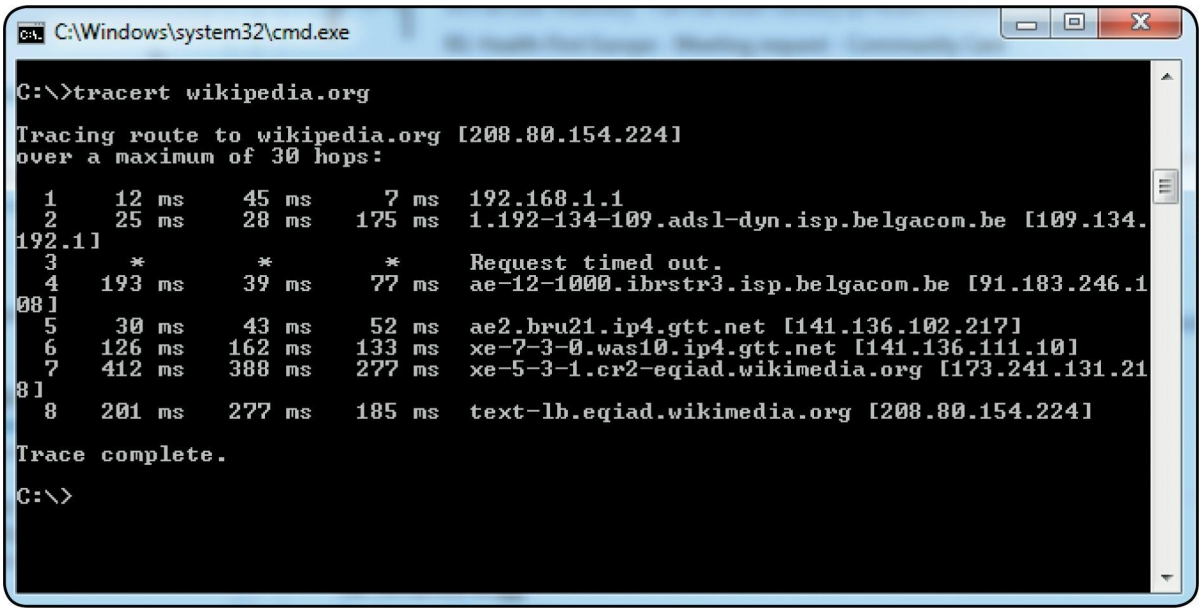
З використанням ОС Windows 7 або пізнішої версії

1. Натисніть кнопку «**Пуск**» у Windows.
2. Введіть «**cmd**» у рядку «пошук» та натисніть на піктограму програми, яка з'явиться в меню «Пуск».



3. Введіть «**tracert wikipedia.org**» і натисніть «**enter**».
4. Тоді ви зможете побачити «**стрибки**», які відбуваються між вашим комп'ютером та вебсайтом, до якого ви намагаєтесь дістатись, і скільки часу займає кожен «стрибок». У цьому прикладі

ми бачимо, що для доступу до Вікіпедії ми спочатку проходимо через роутери нашого «місцевого» Інтернет-провайдера (в даному випадку Belgacom з Бельгії), потім ми рухаємося через Атлантику до роутера у Вашингтоні (скорочено «was»), щоб нарешті прибути до місця, де фізично розміщена Вікіпедія. Звичайно, слід заохотити учнів спробувати це щодо інших вебсайтів. Зверніть увагу, скільки часу займав кожен крок у мілісекундах.



З використанням Mac OS X або пізнішої версії

1. Запустіть мережеву утиліту в Mac OS X (це можна зробити, перейшовши в пошуковик Spotlight, набравши «**network utility**» та клікнувши на верхньому результаті).
2. Клікніть на «**Traceroute**».
3. Введіть ім'я домену, для якого ви хочете виконати контроль проходження сигналу, наприклад, «**Wikipedia.org**», і натисніть «**Trace**».
4. Тоді ви зможете побачити «стрибки», які відбуваються між вашим комп'ютером та вебсайтом, до якого ви намагаєтесь дістатись, і скільки часу займає кожен «**стрибок**».

Факультативний матеріал для вчителів

- Щоб отримати докладнішу інформацію, перегляньте відеозапис «How does the Internet work?»[9] («Як працює Інтернет?») із циклу Naked Science Scrapbook.
- Почніть дискусію в класі про те, як онлайн-технології можуть принести користь людям з особливими потребами, і погляньте на план дій Ради Європи, щоб ініціювати появу ідей[10].

НАЛЕЖНА ПРАКТИКА

- Оберіть підключення, яке підходить для вашого рівня використання Інтернету. Якщо ви регулярно користуєтесь сервісами, які вимагають дуже швидкого Інтернету (наприклад, потокове передавання відео високої чіткості), обов'язково отримайте швидше Інтернет-з'єднання (принаймні 20 мегабіт в секунду, що еквівалентно ADSL2+). Конкретніше, шукайте підключення до Інтернету без обмежень щодо кількості завантажених даних. Якщо Інтернет вам потрібен лише для читання новин та надсилання електронних листів, то вам буде достатньо практично будь-якої базової угоди про доступ до Інтернету[11].
- Завжди вимикайте свої пристрої (комп'ютери) або відключайте з'єднання Wi-Fi на смартфоні/планшеті, коли лягаєте спати. Якщо пристрої залишаться підключеними, це може збільшити ризики для безпеки ваших даних, а також становити ризик для вашого здоров'я (див. Інформаційний матеріал 19 про безпеку).

9. https://www.youtube.com/watch?v=oj7A2YDgIWE
10. https://www.coe.int/t/dg4/majorhazards/activites/2013/DIDRR/Action_Plan_CoE_Easy_to_Read_13nov08_EN.pdf
11. www.cnet.com/internet-speed-test

- Переконайтеся, що ви знаєте, як отримати доступ до сторінки конфігурації роутера. У більшості випадків ви можете отримати до неї доступ, якщо введете в браузер одну з цих IP-адрес: 192.168.1.0 або 192.168.1.1. Чому це важливо? Більшість сторінок конфігурації Wi-Fi мають облікові записи адміністратора за замовчуванням із дуже простими іменами користувачів та паролями (наприклад, ім'я користувача «admin» та пароль «admin»). Дуже важливо убезпечити доступ до сторінки конфігурації роутера, оскільки її можна легко використати для зміни налаштувань або отримання доступу до вашої домашньої комп'ютерної мережі.
- За будь-якої можливості сідайте поруч зі своїми дітьми, коли вони займаються інтернет-серфінгом, щоб стимулювати дискусію про їхній досвід перебування онлайн та підвищити рівень довіри; поставте перед собою мету навчатися разом.
- Активно цікавтеся управлінням Інтернетом і працюйте над тим, щоб ваш голос почули в публічних дебатах щодо таких основних принципів, як анонімність, безпека чи мережевий нейтралітет.
- Укладіть політику прийнятного користування (ППК)[12] або політику відповідального користування (ПВК), яка має застосовуватися, якщо інші особи користуватимуться комп'ютером або мережею, за які ви відповідаєте.

ДОДАТКОВА ІНФОРМАЦІЯ

- Цей список є світовим каталогом інтернет-провайдерів: *<http://www.thelist.com>*.
- Освітні вебсайти, як-от: European Schoolnet за адресою *<http://www.eun.org>*, Global SchoolNet за адресою *<http://www.globalschoolnet.org/GSH/>* і Education World за адресою *<http://www.educationworld.com/>*, пропонують доступ до ресурсів та участь у спільних проєктах.
- Поради щодо укладання ППК можна знайти на Інтернет-порталі Education World, призначеному для вчителів та інших освітніх працівників: *<http://www.educationworld.com/a_curr/curr093.shtml>.*
- Портал Insafe пропонує ресурси та поради щодо безпечного підключення та інтернет-серфінгу: *<https://www.betterinternetforkids.eu/>*.
- Офіційний вебсайт Форуму з управління Інтернетом дозволяє обговорювати питання державної політики, пов'язані з Інтернетом: *<http://www.intgovforum.org/cms/>*.
- Різноманітна інформація про мережевий нейтралітет міститься на цій сторінці Вікіпедії: *<https://en.wikipedia.org/wiki/Net_neutrality>*.
- Інформацію про ICANN можна знайти на її офіційному вебсайті: *<https://www.icann.org/>*.

12. http://en.wikipedia.org/wiki/Acceptable_use_policy

Інформаційний матеріал 2

Присутність у онлайн-просторі та хмарні технології

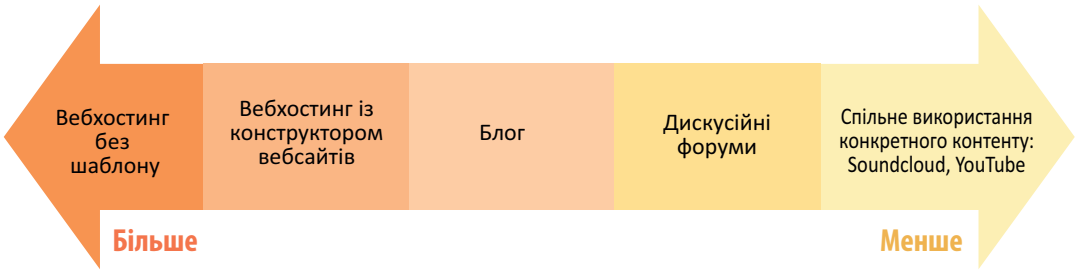
Чи є у вас щось, чим ви хочете поділитися зі світом, і вам потрібне місце, щоб поділитися цим онлайн?

Хоча вебсайти були одним із перших способів обміну інформацією онлайн, протягом останнього десятиліття з'являлося все більше альтернатив вебсайтам. На початку існування Інтернету створити вебсайт було нелегко: це було досить дорого і вимагало певних навичок кодування. Однак сьогодні вам навіть не потрібно бути IT-спеціалістом, щоб створити та сконструювати власний вебсайт. Але перш ніж це зробити, завжди виділяйте час, щоб обміркувати всі варіанти своїх дій.

Ви повинні розуміти, чим та як ви хочете поділитися.

Ви хочете поділитися конкретним контентом (зображеннями, відео, текстами тощо) чи різноманітним контентом? Ви хочете мати повний контроль над усім процесом творчості чи віддаєте перевагу роботі за попередньо встановленим шаблоном, який ви, однак, можете до певної міри змінювати? Із якою метою ви ділитиметеся контентом, і навіщо це вам потрібно? Якою є передбачувана аудиторія – світ, ваш округ, ваша мала батьківщина чи просто учні та батьки? Скільки ви готові заплатити за можливість ділитися контентом онлайн?

Подана нижче діаграма ілюструє неповний перелік способів, за допомогою яких ви можете ділитися контентом, організованих як континуум від повного контролю/налаштування під свої потреби до меншого.



Якщо ви хочете бути абсолютно вільним щодо як контенту, так і щодо дизайну, то вам слід вибрати вебхостинг без шаблону. Але пам'ятайте, що це вимагає певних витрат, і в більшості випадків вам доведеться придбати доменне ім'я (наприклад, <www.mywebsite.com>). Якщо ви не хочете навчитися кодувати, але хочете ділитися різноманітним контентом та мати вебсайт із гнучкою конструкцією, ви можете обрати вебхостинг у розробника вебсайтів або блог (який іноді матиме ще меншу гнучкість конструкції). Дискусійні форуми уже самі по собі є досить конкретними платформами: наприклад, ви можете створити дискусійні форуми або дошки оголошень для своєї школи. І нарешті, якщо ви просто хочете поділитися фотографіями, відео чи музикою, ви можете створити обліковий запис у сервісі, який спеціалізується на розміщенні такого типу контенту. Зрештою, ваш контент, яким би він не був, опиниться десь на сервері хостингового сервісу, який ви оберете: він перебуватиме в «хмарному сховищі».

Також майте на увазі, що, хоча багато з цих сервісів є безкоштовними, це часто означає, що ваші глядачі можуть стати цілями більш-менш нав'язливої реклами (тобто реклами, яка значно перешкоджає нормальному користуванню, наприклад, численні вікна, що спливають, накладання вебсайтів один на одного, надмірна кількість банерів тощо).

ОСВІТНЯ ЦІННІСТЬ, ЧОМУ ЦЕ АКТУАЛЬНО Й ВАЖЛИВО?

Формування онлайн-присутності та поширення контенту онлайн має велике освітнє значення й допомагає розвинути низку навичок.

- **Управління контентом/організація контенту:** незалежно від того, вирішили ви розробити вебсайт чи створити фотогалерею, ваш контент повинен бути організований просто, щоб користувачі могли знайти те, що вони шукають.
- **Дизайн:** ваша ідентичність в Інтернеті часто буде пов'язана з логотипом, зображенням, вибором кольорів, макетом вашого вебсайту, а все це є частиною роботи над дизайном.
- Цифрові навички: цілком очевидно, що формування онлайн-присутності посилить певні цифрові навички, такі як кодування (наприклад, HTML, PHP, HTML5, Javascript), якщо ви вирішите створити вебсайт. Але навіть якщо ви оберете інші варіанти, вам доведеться дізнатися про пошукові системи та рівень видимості вашого контенту, формати файлів тощо.
- Навички спілкування/письма: якщо ви не плануєте ділитися контентом без коментарів, вам доведеться освіжити свої навички спілкування/письма, щоб привернути увагу та інтерес користувачів.
- **Навички маркетингу:** враховуючи, наскільки багато людей вже є онлайн, там легко залишитися непоміченим. Формування репутації та підвищення онлайн-видимості пов'язані зі знанням, як продати себе та рекламувати те, що ви створили чи чим поділилися.
- **Командна робота:** крім того, якщо ваша онлайн-присутність буде спільним проєктом за участі ваших друзів/однокласників/учнів, то це також поліпшить ваші навички командної роботи. Управляти вебсайтом нелегко, і цю роботу часто потрібно організовувати та розподіляти між кількома людьми: адміністратором, дизайнером, автором контенту тощо.
- **Вторинні переваги:** створюючи вебсайт на певну тему, наприклад, вебсайт із математики для шкільного проєкту, ви неминуче також поглиблюєте своє розуміння цієї теми та знання з неї.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

Якщо ви захочете поділитися особистим контентом або створити персональний вебсайт, ви нестимете повну відповідальність за те, що ви розміщуєте. Ви (і ваші батьки, якщо ви є неповнолітнім) можуть опинитися в скрутній ситуації з низки причин.

Юридичні причини

Межі «свободи вираження поглядів»: це право не є абсолютним, й існують певні обмеження щодо його здійснення. Обмеження свободи вираження поглядів мають бути чітко визначені законом, вони повинні бути необхідними в демократичному суспільстві (пропорційними) та мати законні цілі (у п. 2 статті 10 *Європейської конвенції з прав людини* зазначається, що це можна робити «в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду»). Ці обмеження можуть різнитися залежно від держави, але є кілька «широких» міркувань, про які слід пам'ятати:

- наклеп[1];
- мова ненависті[2];
- поширення персональних даних іншої особи[3];
- зберігання даних – якщо ви вирішите використовувати хмарні сервіси, заздалегідь з'ясуйте, де будуть зберігатися ваші дані; це ваше право та обов'язок зберігати контроль за їх використанням та доступністю[4];
- заохочення тероризму:
  - <https://goo.gl/cv9XDR>;
  - <https://goo.gl/Tq3UDp>;
- інтелектуальна власність: чи не ділитесь ви чужим контентом? Якщо так, то обов'язково перевірте, чи є у вас на це дозвіл. Комерційний контент захищено законом про авторські права, і для його використання вам потрібен окремий дозвіл власника авторських прав. Деякі митці чи автори публікують свій контент на умовах спеціальної «ліцензії», яку часто називають «Creative Commons». Залежно від наявності цієї ліцензії, ви можете мати право використовувати контент без згадування про автора, а також використовувати його з комерційною метою. Що стосується захищеного авторським правом матеріалу, якщо ви хочете його використовувати, вам слід отримати відповідний дозвіл організації/особи, що володіє цими правами (звукозаписувальна компанія, кіностудія тощо).

Будь-яка з наведених вище дій може спричинити певну юридичну проблему для вас.

Особисті причини

- Надмірне поширення: майте на увазі, що все, чим ви ділитесь, швидше за все, буде доступним для всіх у всьому світі. Наприклад, якщо ви поділитеся своїми приватними фотографіями про літні канікули із інформацією про місцезнаходження (GPS), це може дати змогу стороннім особам стежити за вами або злодіям точно знати, коли ви перебуваєте на виїзді, щоб вони могли організувати наліт на ваш будинок. Ретельно обирайте, чим ви будете ділитися.
- Онлайн-репутація: хоча у вас може бути ілюзія, що ви можете зберігати анонімність онлайн, існує багато способів, щоб дізнатися про вашу справжню особу. Правоохоронні органи мають необхідні засоби для вистежування користувачів Інтернету за певних умов (у більшості випадків для цього потрібен судовий ордер). Щоразу, коли ви ділитеся чимось онлайн, пам'ятайте, що це вплине на вашу репутацію як онлайн, так і офлайн.

1. https://en.wikipedia.org/wiki/Defamation
2. https://en.wikipedia.org/wiki/Hate_speech.
3. http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf
4. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

- Якщо ви ділитесь образливим або безглуздим контентом онлайн, це може вплинути на ваше нинішнє і майбутнє громадське та професійне життя. Наприклад, якщо ви хочете виплеснути своє розчарування, поговоріть із друзями/членами родини, яким ви довіряєте, кричіть у подушку, але не розсилайте твіт про це на весь світ, оскільки він може повернутися до вас і лишитися з вами назавжди. Загляньте на вебсайт Web We Want5, щоб дізнатись більше про захист своєї онлайн-репутації.

Якщо ви захочете поділитися іншими формами контенту (наприклад, чимось із напрацювань вашої школи) або створити офіційний вебсайт на доручення школи, слід мати на увазі ще кілька моментів:

- Політика школи щодо безпеки в Інтернеті та прийнятного користування повинна бути чітко визначена ще до того, як створювати офіційний вебсайт або дозволяти учням брати участь у конкурсах зі створення вебсайтів.
- Макет і спосіб використання фотографій повинні відображати політику школи щодо безпеки в Інтернеті.
- Через проблеми безпеки та конфіденційності багато шкіл взагалі не надають ПІБ або надають лише імена осіб, присутніх на фотографіях, які вони публікують. Це треба враховувати під час створення вашого вебсайту: яким є ваш протокол безпеки із цього питання?
- Радимо перевірити всі зовнішні гіперпосилання на інші вебсайти, щоб забезпечити цілісність інформації та належне відображення вебсайтами позиції школи щодо безпеки в Інтернеті.
- Якщо ви є учителем, ваша школа повинна буде вирішити, чи буде ваш доступ до Інтернету відфільтрований (якщо це не передбачено законом), чи ви мусите навчити своїх учнів краще орієнтуватися в онлайн-небезпеках. Враховуючи досвід багатьох шкіл, поєднання цих двох підходів є ефективним. Крім того, коли учні створюють вебсайт як навчальне завдання, пам'ятайте, що його можуть відвідувати користувачі з усього світу. Сприймайте ці вебсайти як своєрідний інструмент зв'язків із громадськістю для вашої школи. Тому для вас як учителя було б розумно контролювати роботу учнів і спрямовувати їх під час творчого процесу.
- Учителі, а в деяких випадках і батьки, врешті-решт несуть відповідальність за всю роботу, виконану учнями. Тому вчителі повинні мати право відмовити в розміщенні певних вебсторінок або видалити їх із вебсайту школи чи проєкту. Щоб належним чином контролювати роботу учнів, вчителі повинні завжди мати доступ до паролів[6], вебсайтів[7] тощо.

ЯК ЦЕ РОБИТИ

- Якщо ви не хочете платити за послугу професійного вебхостингу та отримати власне доменне ім'я, розпочати ділитися контентом онлайн не так уже й складно.
- Більшість сервісів, якими ви будете користуватися, будь то конструктори сайтів, блоги чи влоги (див. Інформаційний матеріал 4), мають вбудовані інструкції, які допоможуть вам розпочати роботу.
- Утім, створення вебсайту з нуля все ж вимагатиме набуття певної кількості навичок. На щастя, в наш час є буквально мільйони способів навчитися кодувати, щоб створити вебсайт. До найпопулярніших належать Codeacademy8 і W3schools9. Але в жодному разі не зупиняйтеся на цьому. Завжди приділяйте час пошуку інформації онлайн, щоб знайти інший матеріал, який буде викладено вашою мовою або відповідно до ваших потреб.
- Крім того, подання заявки на професійний вебхостинг вимагає від вас надання додаткової інформації, крім вашої адреси електронної пошти, наприклад, вашого справжнього ПІБ, адреси, номера телефону та особливо деяких платіжних даних, таких як номер кредитної картки. Відтак діти та молодь завжди повинні заздалегідь звертатися за порадами та підтримкою до дорослого (вчителя чи когось із батьків).

5. http://www.webwewant.eu
6. http://en.wikipedia.org/wiki/Password
7. http://en.wikipedia.org/wiki/Website
8. www.codeacademy.com
9. www.w3schools.com/

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

Формуючи онлайн-присутність своєї школи

При правильному використанні вебсайт, блог, влог чи інша подібна платформа школи можуть слугувати потужним інструментом для об'єднання різноманітних елементів спільноти. Вони можуть формувати почуття згуртованості та бути цінним інструментом спілкування, завдяки чому інформація стає легкодоступною для всіх сторін. Ось декілька корисних пропозицій щодо вебконтенту.

- Учителі можуть надати плани уроків або огляд того, що учні робили протягом певного періоду.
- Адміністратори можуть публікувати розклади або оголошення.
- Діти та молоді люди можуть публікувати твори мистецтва, вірші, оповідання, звіти чи інші роботи.
- Батьки можуть використовувати сайт, щоб повідомляти про спільні заходи за участю батьків і вчителів, як-от: свята чи інші масові заходи.
- Громада в цілому може використовувати його як форум для повідомлень про футбольні команди, екскурсії, діяльність поліції, дорожні роботи тощо.

Різноманітний контент може збагатити вебсайт, блог чи влог, але широка база учасників може також зробити хаотичним обслуговування вебплатформи. Важливо, щоб збір та редагування контенту було доручено невеликій групі людей. Можливо, це завдання найкраще виконуватиме учитель чи адміністратор або інша особа, обрана для виконання функцій координатора з інформаційно-комунікаційних технологій (ІКТ).

НАЛЕЖНА ПРАКТИКА

- Стежте за всіма своїми обліковими записами. Створіть папки в електронній адресі, яку ви використовуєте для підписки на ці сервіси, та сортуйте свої електронні листи, щоб завжди мати змогу знайти важливу інформацію про свої облікові записи, наприклад, про своє ім'я користувача.
- Завжди використовуйте свою адресу електронної пошти, а не обліковий запис у соціальних мережах під час реєстрації у важливих онлайн-сервісах, таких як облікові записи вебсайтів, блоги, влоги тощо. Хоч якою зручною здається можливість зареєструватися в сервісах за допомогою облікових записів Facebook, Google+ чи інших соціальних мереж, не забувайте, що тим самим ви погоджуєтесь на доступ цих служб до значної частини вашої інформації. Окрім того, хоча деякі соціальні мережі здаються такими, що існуватимуть вічно, але якщо їх послуги колись припиняться, ви, можливо, не зможете увійти до свого облікового запису (наприклад, якщо публіка недостатньо користується певним інструментом, цей інструмент може застаріти).
- Поширення контенту онлайн через вебсайт, блог або влог є чудовою можливістю поділитися своїми поглядами, але ви, можливо, захочете захистити при цьому свою конфіденційність, використовуючи псевдонім і приховуючи певні персональні дані.
- Почніть з малого, виділіть час на навчання та експерименти, перш ніж виходити зі своїм контентом на широкий загал або вводити його в класне заняття. Вам може бути корисно відвідати інші вебсайти, блоги чи влоги, щоб запозичити ідеї та отримати натхнення.
- Завжди викладайте ключову контактну інформацію, таку як адреса та номер телефону школи, на вебсайт, у блог чи влог вашої школи.
- Переконайтеся, що ваш вебконтент є зручним для користувачів та пристроїв. У наш час дедалі більше людей отримують доступ до вебконтенту через свої мобільні телефони, і це часто вимагає спеціального макету та дизайну. Належна практика також передбачає представлення вебконтенту у вигляді, доступному для осіб із інвалідністю. Перегляньте деякі ресурси на цю тему на цьому вебсайті: <http://www.w3.org/WAI/gettingstarted/Overview.html>.
- За першої можливості робіть свій вебконтент багатомовним, щоб неангломовні особи також могли скористатися ним.

ДОДАТКОВА ІНФОРМАЦІЯ

- Більше інформації про конструктори вебсайтів можна знайти в цій статті про цифрові тенденції: *<http://web.archive.org/web/20160622040107/http://www.digitaltrends.com/computing/best- website- -websites-free/>.*
- Про управління онлайн-репутацією можна дізнатися більше із цієї статті з Вікіпедії: *<https://en.wikipedia.org/wiki/Online_presence_management>*.
- Інформаційні матеріали Єврокомісії щодо нового Загального регламенту про захист даних (GDPR) містять «право на забуття»: *<http://ec.europa. eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_citizens_ rights_2016_en.pdf>.*
- Відповідні статті Конвенції ООН про права дитини:
  Стаття 13 – Діти мають право одержувати і поширювати інформацію, якщо це не шкодить їм чи іншим особам.
  Стаття 16 – Діти мають право на приватність. Закон повинен захищати їх від нападок на їхній спосіб життя, їхнє чесне ім'я, їхні сім'ї та їхні домівки.
  Стаття 29 – Освіта повинна повною мірою розвивати особистість та таланти кожної дитини. Вона повинна заохочувати дітей поважати батьків, власну та інші культури.
  Стаття 31 – Усі діти мають право на відпочинок, ігри та залучення до широкого кола заходів.

Інформаційний матеріал 3

Web 2.0, Web 3.0 та інші

Web 2.0 дозволяє нам не тільки завантажувати та споживати, але й вивантажувати та створювати. Термін Web 2.0 стосується того, що вважається вебсервісами «другого покоління», які звертають особливу увагу на створений користувачами контент, зручність використання та сумісність. Типовими прикладами є сайти соціальних мереж (див. Інформаційний матеріал 8), вікі-платформи, засоби комунікації та фолксономії, які сприяють онлайн-співпраці та обміну даними між користувачами. Web 2.0 не створюється якимись конкретними технічними оновленнями, а охоплює кумулятивні зміни, спираючись на інтерактивні засоби Web 1.0 і забезпечуючи обчислення з використанням «мережі як платформи», що дозволяє користувачам запускати програмні застосунки виключно через браузер.

Користувачі можуть володіти даними на сайті покоління 2.0 і контролювати ці дані за допомогою «архітектури участі», яка заохочує користувачів удосконалювати застосунок, коли вони ним користуються. Це надає величезні переваги порівняно з традиційними вебсайтами, які обмежують можливості відвідувачів лише переглядом, а їх контент може змінювати лише власник сайту. Сайти покоління 2.0 часто мають зручний для користувача інтерфейс, заснований на об'єднаних або «багатих» носіях, тобто передових технологіях, таких як потокове відео, завантажені аплети (програми), які миттєво взаємодіють із користувачем, та контент, який змінюється, коли на нього наводиться курсор.

WEB 3.0 ТА ІНШІ

Термін Web 3.0 (іноді ви також можете побачити Web 4.0, 5.0 тощо) обговорюється ширше. Інколи його описують як наступний етап розвитку Web 2.0, а інколи визначають як своєрідний «сполучений інтелект», який поєднує дані, поняття, програми та людей і, на думку багатьох, зрештою почне генерувати дані самостійно. Деякі люди віддають перевагу терміну «семантична мережа», тоді як інші експерти визначають семантичну мережу як лише одну з декількох конвергентних технологій та тенденцій, які визначатимуть наступний великий етап еволюції мережі.

Існують також інші типи мереж. Darknet (або темна мережа) – це мережа, яка існує як накладка на те, що ми називаємо Всесвітньою павутиною, і доступ до якої можливий лише за допомогою спеціального програмного забезпечення, налаштувань або авторизації, для яких, як правило, використовуються спеціальні протоколи зв'язку та порти. Для обміну файлами зазвичай використовуються мережі друзів (friend-to-friend, F2F – лише прямі зв'язки між людьми, які знають один одного) та однорангові мережі (між людьми з однаковими правами користувачів). Такі мережі, як Tor, працюють через анонімізовану серію з'єднань, і тому їх можна легше використовувати для незаконної діяльності.

НАСЛІДКИ ДЛЯ ШКІЛ

Інструменти Web 2.0 сприяють творчості, співпраці та спілкуванню й можуть мати глибокий вплив на навчання. Вони просувають нові педагогічні моделі, такі як перевернуті класні кімнати, де учні виконують багато традиційних класних занять удома[1]. Оскільки багато інструментів Web 2.0 є безкоштовними програмами, вони допомогли зменшити вартість програмного забезпечення та заохотили розробку нових моделей ліцензування програм для шкіл.

Існує багато відмінностей між Web 1.0, 2.0 та 3.0, як показано в таблиці нижче.

Web 1.0	Web 2.0	Web 3.0
Базується на застосунках	Базується на мережі	Застосунки для різних пристроїв/ динамічні застосунки
Ізольовані	Колаборативні (орієнтовані на співпрацю)	Поширює контент, розроблений на замовлення
Ліцензований чи придбаний	Безкоштовний	Мультиліцензійні носії, що зазнали конвергенції
Єдиний автор	Колаборативна творчість	Автори та пристрої взаємодіють
Пропрієтарний (такий, що є приватною власністю) код	Відкритий доступ до вихідних кодів	Створені спільними зусиллями, виконувані
Захищений авторським правом контент	Спільний контент	Контент, що генерується користувачами й машинами

Чотири найпоширеніші технології Web 2.0 – це соціальні мережі (див. Інформаційний матеріал 8), обмін повідомленнями, створення й перегляд відео та фільмів (за допомогою подкастів, MP4 тощо) та вікі-платформи, хоча існує також і низка інших технологій.

Термін «**Podcasting**»[2] виник із виходом на ринок iPod (портативний медіаплеєр Apple, випущений у 2001 році) і є похідним від слів «iPod» та «трансляція» (broadcast). Це був спосіб обміну аудіофайлами через Інтернет для відтворення на мобільних пристроях або комп'ютерах, також відомий як MP3 (цифровий файл MPEG із звуковим шаром). Сьогодні більшість мобільних пристроїв мають засоби відеозапису, а формат MP3 витіснено форматом MP4, який є мультимедійним і зберігає як аудіо, так і відео. Подкасти та відео у форматі MP4 полегшують для вчителів і учнів завдання нести навколишній світ до класу й обмінятися інформацією та враженнями про події.

Обмін відео став надзвичайно популярним з моменту запуску YouTube у 2005 році, а тепер це можна робити також і за допомогою багатьох платформ соціальних мереж. Teachertube[3] – це сайт, орієнтований на вчителів та використання в освітньому процесі, він базується на YouTube[4] і

1. https://en.wikipedia.org/wiki/Flipped_classroom
2. http://computer.howstuffworks.com/internet/basics/podcasting.htm
3. www.teachertube.com

також може використовуватися школами та організаціями для створення власних каналів обміну відео. На сайтах обміну відео[5] зазвичай є функція пошуку, а їхні користувачі можуть розміщувати повідомлення, коментувати відео, ставити на них мітки (теги) й переглядати їх. Існує багато спільнот, для виробництва та обміну відеозаписами, які відображають спільні інтереси. Останнім часом з'явились сайти, які дозволяють користувачам редагувати свої відеокліпи онлайн та додавати звук, субтитри тощо. Jumpcut[6] є прикладом такого сайту..

Вікі-платформи – це вебсторінки, які дозволяють читачам взаємодіяти та співпрацювати один із одним, оскільки будь-хто може редагувати такі сторінки або додавати до них інформацію. Вікі-платформа – це чудовий інструмент Web 2.0 для спільних письмових робіт у школах. Наприклад, Google Docs[7] дозволяє користувачам спільно працювати над текстами, слайд-презентаціями та таблицями. Ще одним відомим прикладом вікі-платформи є Вікіпедія – колаборативна енциклопедія, яка тепер включає більш актуальні статті, ніж Encyclopaedia Britannica.

Соціальні закладки дозволяють користувачам ділитися своїми улюбленими створеними користувачами Інтернет-продуктами або закладками. Раніше список улюблених вебсайтів користувача був частиною його Інтернет-браузера. Тепер соціальні закладки дозволяють легко ділитися цими списками, щоб кожен міг ними користуватися. Контент можна класифікувати за допомогою міток, щоб полегшити пошук та використання інформації в ньому. Вебсайт і застосунок Delicious[8] є прикладом соціальних закладок і показує користувачам, скільки інших людей зберегли адресу певного сайту.

Обмін фотографіями – це популярний інструмент, який дозволяє користувачам ділитися фотографіями з родиною та друзями. Одним із прикладів цього є Flickr[9], який дозволяє користувачам публікувати фотографії, а потім запрошувати інших переглядати їх як окремо, так і у вигляді слайд-шоу. До кожної фотографії можна додавати нотатки та мітки, а інші люди також можуть залишати коментарі.

Програмне забезпечення для **редагування та вдосконалення фотографій** тепер доступне онлайн і дозволяє користувачам вдосконалювати свої фотографії. Як приклади таких застосунків, популярність яких зростає, можна навести:

- Picasa (Google) <http://picasa.google.com>;
- iPhoto (Apple) <www.apple.com/iphoto>;
- Photo Story (Microsoft) <http://microsoft-photo-story.en.softonic.com>.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Вебінструменти дозволяють кожному завантажувати або редагувати матеріали в Інтернеті, і такий контент може бути не завжди правильним або достовірним. Це підкреслює важливість надання юним учасникам навчання широких можливостей для розвитку медіанавичок, необхідних для оцінки сайтів та контенту на предмет достовірності та упередженості.
- Педагоги не повинні використовувати спрощений підхід, за яким будь-який неправдивий контент обов'язково є поганим – він може також бути продовженням акторської гри онлайн, а також може мати освітню цінність (наприклад, підробні облікові записи відомих історичних діячів на сайтах соціальних мереж).
- Вебінструменти та програми пропонують безмежні можливості для користувачів публікувати інформацію про себе та інших. Утім, вони повинні й надалі пильно стежити за ризиками саморозкриття конфіденційної інформації та втрати приватності. Емпіричне правило полягає в тому, щоб не публікувати нічого, про що не мав би знати цілий світ (див. Інформаційний матеріал 8 про соціальні мережі).
- Щоб інтегрувати технологію в навчальний процес, потрібен час і зусилля, тому перш ніж братися до цього процесу, переконайтеся, що використання інструментів Web 2.0 та Web 3.0 матиме суттєві наслідки для ваших учнів.

4. https://support.google.com/youtube/search?q=teachers+channel
5. http://computer.howstuffworks.com/internet/basics/video-sharing.htm
6. www.jumpcut.com
7. https://www.google.com/docs/about/
8. https://del.icio.us
9. www.flickr.com/

- Не всі інструменти Web 2.0 є рівноцінними та мають однакову філософію чи бізнес-модель. Пам'ятайте, що хоча такі вебсайти, як Вікіпедія, дотримуються некомерційного, незалежного, волонтерського, колаборативного підходу, багато соціальних мереж, наприклад, Facebook, мають комерційне призначення.
- Контент, який ви вносите до Вікіпедії, буде використовуватися на благо спільноти, тоді як контент, який ви вносите до Facebook, буде використовуватися, серед іншого, для показу вам персоналізованої реклами.
- Рейтингування товарів і послуг стало популярним завдяки можливостям Web 2.0/3.0. Однак критичний підхід є зараз необхідним більш ніж коли-небудь, оскільки навіть на найпопулярніших сайтах цього типу рейтинги не обов'язково є надійними – платні рекомендації стають все більш поширеними.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Інтернет-користування: найпопулярніший вид онлайн-діяльності для 86% користувачів Інтернету – це спілкування, за яким іде отримання інформації (близько 50%) та діяльність, пов'язана зі службовим просуванням та комерцією (приблизно 25%)[10]. Обговоріть статистику інтернет-користування з вашими учнями/дітьми. Як їхня модель користування Інтернетом виглядає в порівнянні з іншими молодими людьми у своїй країні та інших країнах світу, а також із користуванням десять років тому? Які це могло мати наслідки?
- Відео: учні можуть створювати власні відеоролики, щоб ширше ділитися своїми думками та поглядами щодо певної теми. Запропонуйте учням працювати в групах, готувати розкадровку та використовувати свої мобільні телефони для створення відео. Це надасть можливість обговорити з ними такі теми, як авторські права (див. Інформаційний матеріал 14), отримання згоди знятої/сфотографованої особи (або дозволу їхніх батьків у випадку неповнолітніх) перед вивантаженням зображень в Інтернет тощо. Вони можуть поділитися своїм відео через вебсайт вашого класу чи школи або використати спеціальний канал на YouTube[11], щоб охопити мільйони користувачів Інтернету. Зараз деякі школи використовують відео для запису занять, щоб ті учні, які були відсутні, могли наздогнати пропущений матеріал.
- Вікі-платформи: перегляньте вікі-платформи, які найкраще пристосовані до вашого освітнього середовища (див. додаткову інформацію), а потім створіть спільне робоче завдання для своїх учнів. Ви зможете активно контролювати роботу окремих учнів та вести облік усіх внесених змін. Вікі надають учням ідеальні можливості для співпраці осіб із різних шкіл та країн в рамках справжніх колаборативних проєктів.
- Соціальні закладки: створіть конкретний дослідницький проєкт і розподіліть завдання між окремими учнями чи групами. Можна використовувати пошукову систему, щоб знайти інструмент соціальних закладок, який відповідав би вашим потребам. Кожна група може використовувати соціальні закладки для складання детального набору відповідних посилань. Однією з переваг такого підходу є те, що учням не потрібно отримувати доступ до того самого комп'ютера щоразу, коли вони хочуть продовжувати роботу, оскільки їхні улюблені сайти доступні з будь-якого комп'ютера в будь-який час.

10. http://www.pewglobal.org/2015/03/19/2-online-activities-in-emerging-and-developing-nations/.
11. www.youtube.com

ДОДАТКОВА ІНФОРМАЦІЯ

- Ці дві вікі-платформи можна використовувати в освітньому середовищі: *<http://mediawiki.com>* та *<http://www.pbworks.com>*.
- Учителі кількох сотень тисяч шкіл Європи сьогодні співпрацюють у безпечному навчальному середовищі з класами в інших країнах через створену Європейською Комісією мережу eTwinning за адресою: *<www.etwinning.net/en/pub/index.htm>*.
  Інформацію про заходи безпеки при використанні інструментів Web 2.0 вдома та в школі можна знайти за адресою: *<www.betterinternetforkids.eu/>*.
- Незважаючи на те, що YouTube Kids пропонує менше функцій, ніж YouTube.com, для перегляду та обміну відео, проте цей вебсайт функціонує в безпечному середовищі, пристосованому спеціально для дітей молодшого віку, та пропонує рекомендації для батьків, учителів та вихователів: *<https://kids.youtube.com/>*.
- Інформацію про інструменти Web 2.0 для використання в класі та посилання на безкоштовні завантаження можна знайти за адресою: *<http://web.archive.org/web/20160413121845/http://www.solutionwatch.com/512/back-to-school-with-the-class-of-web-20-part-1/>*.
- Корисні застосунки Web 2.0 для початкових шкіл можна знайти за адресою: *<http://web.archive.org/web/20150914224206/http://langwitches.org/blog/2007/12/22/best-web-20-applications-for-elementary-school/>.*

Інформаційний матеріал 4

Блоги та влоги

Онлайн-щоденник розвинувся у сучасний блог на початку 1990-х років. Слово «блог»[1] є скороченням від «вебжурнал (weblog)» і стосується онлайн-щоденника, які створюють та публікують групи та приватні особи. Термін «weblog» було включено до Оксфордського словника в 2003 році. Хоча деякі політики та знаменитості зайнялися веденням блогів, блоги продовжують тісніше асоціюватися з більш звичайними людьми, які висловлюють свої погляди та обговорюють своє повсякденне життя.

Блоги та влоги (відеоблоги) також стали платформами для соціальних змін, на яких блогери та влогери висвітлюють проблеми у своєму житті, тим самим проводячи просвітницьку роботу серед читачів щодо таких питань, як батьківство або життя з аутизмом, або підвищуючи їх політичну обізнаність з різних питань.

Через популярність блогів було створено багато вебсайтів, які пропонують програмне забезпечення для створення та публікації матеріалів. Кожен запис у блозі можна коментувати, що надає можливості для обговорення та може допомогти породити нові ідеї.

Блоги хостяться на спеціальних сервісах хостингу блогів або на звичайних вебхостингах, і нинішні тарифи за послуги хостингу вважаються прийнятними.

1. https://en.wikipedia.org/wiki/Blog

Моблоги

Мобільні блоги, відомі як моблоги, – це спосіб публікації контенту на вебсайті або в блозі за допомогою мобільного телефону або надолонного пристрою. Моблогінг[2] з'явився завдяки розвитку функцій електронної пошти в мобільних телефонах (див. Інформаційний матеріал 5 про мобільні технології).

Влоги

Відеоблог або відео-журнал – це те саме, що описаний вище блог, але публікації в ньому мають формат відео. Спочатку влоги були популярними на YouTube, а тепер їх можна побачити на Vine, Instagram, Facebook і навіть Pinterest.

RSS-канали

RSS[3] або збагачене зведення вебсайту зараз використовується для синдикування блогів. Ті, хто бажає опублікувати свій контент на інших вебсайтах, можуть удоступнити його за допомогою XML[4] або розширюваної версії мови розмітки для вебсиндикації.

XML – це тип коду, подібного до HTML, також відомий як «канал». У принципі він дозволяє читачам «підписатись» на контент та отримувати оновлення певного блогу, щоб їм не потрібно було відвідувати його.

Значення блогів і влогів для освіти

- Блоги та влоги уможливлюють для їхніх авторів висловлення своїх поглядів. Блогери та влогери можуть ділитися своїми інтересами, обмінюватися думками та інформувати свою аудиторію з питань, які знаходять у них відгук. Вони можуть документувати життя, ділитися пригодами та пропонувати візуальні точки зору на легко доступній для всіх платформі.
- Блогери та влогери можуть одночасно бути моблогерами, коли вони використовують свої смартфони для написання, публікації та вивантаження контенту.
- Оскільки смартфони широко доступні, більш різноманітна і часто молодша аудиторія може вести блоги та влоги без необхідності використовувати дороге комп'ютерне обладнання.
- Блоги та влоги також використовуються журналістами, дослідниками та активістами як важливий засіб та джерело інформації та спосіб висловлювання поглядів.
- Також з'явилися блоги й влоги, автори яких зосереджують свою увагу на інвалідності та особливих потребах, щоб підвищити обізнаність громадськості та запустити обговорення.

Блоги в освітньому середовищі

Блоги дають учням можливість взяти навчання під свій контроль та організувати публічний форум, на якому вони могли б виражати свої думки та почуття; їх можна також використовувати як креативний навчальний інструмент для обговорення та співпраці. Наприклад, на занятті з сучасної літератури блоги використовувалися для вивчення роману «Таємне життя бджіл». Авторка написала вступ до уроку, а учням та їх батькам було запропоновано написати про свої враження від тексту, який їм задавали читати кожного дня. Потім авторка прокоментувала ці враження (див. <http://techtraining.dpsk12.org/ilt/Bees/SLOBees.pdf>).

Експерти відзначають триетапний процес, який має місце при веденні блогу: визначення аудиторії, мети та тематики. Це описано на вебсайті <https://macln.wordpress.com/2011/01/12/three-step-process-for-blogging/> . Блогери повинні постійно шукати, відсіювати та розміщувати матеріали. Шукаючи матеріал для коментування, учень дедалі краще ознайомлюється з різними теоріями та ідеями й розвиває навички, необхідні для критичного аналізу контенту та розпізнавання правдивого контенту.

Технологія може використовуватися як мотиваційний чинник у навчанні. Учні цікавляться блогами через креативність останніх та можливості для самовираження, які вони пропонують. Їх можна використовувати як інструмент для викладання найрізноманітніших тем.

Блоги дають кожному учневі, що присутній на даному занятті, можливість взяти участь у дискусії, яка показує дітям та молоді різні погляди на проблему.

2. https://en.wikipedia.org/wiki/Mobile_blogging
3. https://en.wikipedia.org/wiki/RSS
4. https://en.wikipedia.org/wiki/XML

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Нагадуйте учням, що не слід видавати в загальнодоступних інтернет-просторах таку особисту інформацію, яку вони не розголошували б на форумі, який проводиться офлайн. Це є особливо важливою проблемою для блогів, які за самою своєю природою часто є особистими.
- Навіть анонімний блогінг не завжди є повністю анонімним, і видалення блогу не обов'язково видаляє весь його контент із поля зору.
- Подумайте про свою безпеку офлайн і поставте запитання: наскільки легко було б комусь знайти мене на основі наданої мною інформації?
- Враховуйте голос та особистість, які ви збираєтесь використовувати як блогер чи влогер. Чи вважатиме їх хтось обурливими? Чи вважатимуться вони обурливими з точки зору вашої школи чи майбутнього роботодавця?
- Блоги та влоги можуть також використовуватися для розповсюдження ненависницьких і дискримінаційних повідомлень або для просування екстремістського й радикального контенту чи контенту, що викликає занепокоєння.

ЯК ЦЕ РОБИТИ

Якщо у вас є відповідні технічні навички, ви можете створити блог з нуля. Більшість людей використовують сайти, які пропонують інструменти для створення та публікації контенту у вигляді блогу. School Blogs за адресою <http://www.schoolblogs. net/wpress/>, Blogger (див. нижче) та Wordpress є популярними хостами, які надають безкоштовні послуги. Вони містять прості покрокові інструкції, які допоможуть вам створити обліковий запис, назвати свій блог та вибрати шаблон.

Після запуску вашого блогу ви складаєте та редагуєте записи з центральної вебсторінки. Інтерфейс популярного програмного забезпечення має формат WYSIWYG5 і є надзвичайно зручним для користувача. Відвідувачі вашого блогу можуть коментувати контент, натискаючи посилання на коментарі наприкінці кожного запису.

Ви можете вирішити модерувати коментарі до своїх записів, перш ніж вони відображатимуться на вашій вебсторінці.

Обов'язково збагачуйте свої оцінки гіперпосиланнями та зображеннями. Кнопки для цих функцій слід розміщувати на панелі інструментів над текстовим полем, куди ви вводите свій контент.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Поділіть учнів на пари, де один із них буде грати роль блогера, а другий даватиме інтерв'ю з визначеної теми. Журналіст-блогер проводить інтерв'ю, а потім пише допис у блог, який має схвалити той, хто давав інтерв'ю.
- Дослідіть найпопулярніші блоги та влоги, присвячені інвалідності, особливим потребам, соціальним змінам або усвідомленню соціальних проблем. Запропонуйте учням обговорити, як вони можуть зробити свій внесок, коментуючи або створюючи допис у блозі.
- Нехай учні обміркують, що є найкращим способом передати своє повідомлення: блог, влог, серія твітів, відео на Vine чи відео на Periscope. Досконалість не має меж. Якщо учні вибирають Twitter, Vine, Periscope чи інший застосунок, нагадайте їм, що треба включити посилання на свій блог.
- Попросіть учня перерахувати 5-10 тем, що цікавлять його. Потім проведіть певну пошукову роботу, щоб з'ясувати, чи існують блоги, присвячені бажаній темі.
- Дослідіть серед учнів та молоді, чим займаються деякі популярні блогери. До яких тем вони звертаються: довкілля, політика, мода, музика, інформаційні технології?

5. «Ви бачите те, що отримуєте (What You See Is What You Get)»: https://en.wikipedia.org/wiki/WYSIWYG

КРАЩІ ПРАКТИКИ

- Блог – це чудова можливість висловити свої погляди, але ви, можливо, захочете захистити при цьому свою конфіденційність, використовуючи псевдонім і приховуючи певні персональні дані. Діти та молодь повинні бути особливо обережними при розкритті особистої інформації в блозі.
- Дотримуйтеся законів про авторські права та не використовуйте чужі дизайни блогів чи фотографії у блозі без їх дозволу. Існує багато вебсайтів, які дозволяють безкоштовно використовувати їхні фотографії з атрибуцією чи без неї.
- Створіть власний блог, щоб ознайомитись із цією практикою перед тим, як вводити її в клас. Відвідування інших блогів, щоб отримати ідеї та натхнення, може стати вам в пригоді. Вебсайт School Blogs[6] має понад 4000 учасників та надає користувачам можливість створити власний шкільний блог.
- Приділіть час на те, щоб пояснити своїм учням концепцію ведення блогу. Розкажіть їм, чому це робиться, і наведіть приклади хороших і поганих блогів. Потім дайте учням набір обов'язкових до виконання правил, які можуть включати тривалість та частоту дописів, теми, кількість гіперпосилань/фотографій тощо. Попросіть учнів вести блоги, обговорювати свої враження та коментувати в чужих блогах.

ДОДАТКОВА ІНФОРМАЦІЯ

- Blogger – це сайт, який надає інструменти для блогінгу, а останнім часом і моблогінгу: *<www.blogger.com/start>.*
- Юридичні та етичні поради для блогерів можна знайти за адресою: *<http://weblogs.about.com/od/bloggingethics/tp/Blogging-Best-Practices.htm>*.
- Фонд електронного фронтиру (Electronic Frontiers Foundation, EFF) пропонує юридичний посібник для блогерів: *<http://www.eff.org/bloggers/lg/>*.
- Weblogg-ed – цей сайт відстежує сучасні тенденції освітнього блогінгу: *<www.weblogg-ed.com/>*.
- «Блогінг і RSS – відповіді на питання «що це?» та «як це робити» стосовно потужних нових вебінструментів для педагогів»: *<http://web.archive.org/web/20160413030845/http://www.infotoday.com/MMSchools/jan04/ richardson.shtml>*.
- «Освічений блогер: використання блогів для підвищення грамотності в класі»: *<http://firstmonday.org/ojs/index.php/fm/article/view/1156/1076>*.
- Інструменти підтримки письменницької творчості учнів на всіх етапах шкільної освіти можна знайти за адресою: *<www.readwritethink.org/student_mat/ index.asp>.*
- Ресурси з блогінгу для педагогів доступні за адресою: *<http://www.socialstudiescentral.com/>*.
- Даррен Роуз був одним з перших блогерів, які повністю заробляли на життя веденням блогів. Він пропонує поради та ресурси на своєму вебсайті: *<www.problogger.net/>*.
- До вебсайтів із безкоштовними фотографіями для використання в блогах належать, зокрема, *<www.pixabay.com>*, *<www.flickr.com/ creativecommons/>*, і *<www.freedigitalphotos.net>*.
- Інструментарій «Навчаємось разом, як залишатись у безпеці», розроблений для шкіл Міністерством у справах дітей, шкіл та сімей Великої Британії, надає вчителям ресурси з таких питань, як екстремізм та радикалізація: *<www.preventforschools.org/download/file/mmu-learning-together-to-be- safe.pdf>.*
- Відповідні статті документів Ради Європи, включаючи Європейську конвенцію з прав людини: *<www.echr.coe.int/Documents/Convention_ENG.pdf>*:
  Стаття 8 – Право на повагу до приватного і сімейного життя.
  Стаття 10 – Свобода вираження поглядів.

6. http://www.schoolblogs.net/

Інформаційний матеріал 5

Інтернет на ходу

Рівень використання Інтернету на ходу, тобто використання Інтернету через портативний комп'ютер чи надолонний пристрій за допомогою мобільного чи бездротового зв'язку, зростає, оскільки люди користуються новими способами підключення, які можна використовувати, коли перебуваєш поза домом чи на роботі.

У 2012 році 36% людей у віці від 16 до 74 років у межах 28 країн ЄС використовували мобільний пристрій для підключення до Інтернету. Через два роки цей показник зріс до 51%. Дослідження[1] показують, що найпоширенішими мобільними пристроями для підключення до Інтернету були мобільні телефони або смартфони, лептопи, ноутбуки, нетбуки або планшети.

Мало хто купував мобільні телефони, коли вони вперше стали доступними в 1983 році. У 1995 році на 100 жителів Європейського Союзу припадало п'ять мобільних підключень. За даними Євростату, у 2003 році цей показник становив 80 мобільних телефонів на 100 жителів 25 країн розширеного ЄС.

Через десять років кількість підключень до смартфонів становила близько 400 мільйонів, що становило майже 40% від загальної кількості мобільних телефонів. За прогнозом фірми Ericsson, до кінця 2020 року кількість смартфонів у Європі сягла 800 мільйонів [2].

1. ttp://web.archive.org/web/20160413105315/http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_ and_individuals
2. http://web.archive.org/web/20150324081657/http://www.ericsson.com/res/docs/2014/emr-november2014-regional-appendices-europe.pdf

Межі між мобільними технологіями та персональними обчисленнями стали розмитими, оскільки більшість мобільних телефонів мають можливості перегляду Інтернету та роботи з електронною поштою, а дедалі більше комп'ютерів є бездротовими.

МОБІЛЬНА ТЕХНОЛОГІЯ

Мобільна технологія – це технологія, яка використовується для стільникового зв'язку, і деякі люди стверджують, що мобільна технологія є майбутнім комп'ютерної галузі [3].

СМС

Послуга коротких повідомлень (Short message services, SMS) – це сервіс текстових повідомлень, який функціонує в телефонних, мережевих або мобільних системах зв'язку [4].

ММС

Послуга мультимедійних повідомлень (Multimedia message services, MMS) – це функція, яка дозволяє користувачам надсилати повідомлення, що містять мультимедійний контент, на мобільні телефони та з них [5].

М-навчання

Мобільне навчання або м-навчання означає навчання за допомогою мобільних технологій, таких як мобільні телефони, надолонні комп'ютери та кишенькові комп'ютери (КПК) [6].

Геолокація

Геолокація – це спроможність установити реальне географічне розташування об'єкта, наприклад, мобільного телефона або підключеного до Інтернету комп'ютерного термінала.

Користувачі мобільної технології повинні розуміти функцію геолокації на своїх пристроях і мати можливість встановлювати стандартні налаштування конфіденційності на мобільних пристроях (для отримання додаткової інформації про налаштування конфіденційності див. Інформаційний матеріал 9).

Застосунки

Мобільний застосунок – це комп'ютерна програма, спеціально розроблена для роботи на мобільних пристроях, таких як смартфони, планшети, смарт-годинники, а в деяких випадках і на носних пристроях [7]. Для отримання додаткової інформації про носні пристрої див. Інформаційний матеріал 23.

Кількість застосунків зросла прямо пропорційно кількості користувачів мобільних телефонів, і, за оцінками, сектор застосунків створює дохід на рівні понад 10 мільярдів євро на рік в межах Європейського Союзу [8].

Доступно дуже багато різних застосунків, які є безкоштовними або платними, і бажано прочитати відгуки про них перед їх завантаженням або придбанням, оскільки безкоштовні застосунки можуть у кінцевому рахунку дорого обійтися через вбудовані до них покупки (див. Інформаційний матеріал 13 про онлайн-покупки).

Mobicash

Зі збільшенням кількості користувачів мобільних телефонів фінансові установи запровадили єдині безготівкові мобільні фінансові платформи, які пропонують обробку транзакцій і мобільні платежі.

Наприклад, платформа «Orange money», як називають послуги в сфері мобільних грошей від провайдера Orange, доступна в 13 країнах: Ботсвані, Камеруні, Кот-д'Івуарі, Єгипті (під назвою Mobicash), Гвінеї, Йорданії, Кенії, Мадагаскарі, Малі, на Маврикії, в Нігері, Сенегалі та Уганді [9].

Уряд Великої Британії повідомляє, що до 2021 року британські споживачі, найімовірніше, стануть витрачати аж 30,5 млрд. доларів на покупки через мобільні телефони [10].

3. https://en.wikipedia.org/wiki/Mobile_technology
4. https://en.wikipedia.org/wiki/Short_Message_Service
5. https://en.wikipedia.org/wiki/Multimedia_Messaging_Service
6. https://en.wikipedia.org/wiki/M-learning
7. https://en.wikipedia.org/wiki/Mobile_app
8. http://web.archive.org/web/20160617033122/http://www.visionmobile.com/product/the-european-app-economy/
9. https://goo.gl/4LQveU
10. https://goo.gl/8a7Dx7

ЗНАЧЕННЯ ДЛЯ РОЗУМІННЯ ПРОБЛЕМ

- Існує занепокоєння через те, що діти отримують мобільні телефони або планшети занадто рано, оскільки ще не проведено довгострокових досліджень для вивчення того, які проблеми розвитку може спричинити ранній доступ до мобільних телефонів або планшетів.
- Також викликає занепокоєння участь дітей у онлайн-покупках та взагалі електронній комерції без розуміння її наслідків.
- Дослідження не дали чітких результатів щодо небезпеки довгострокового радіаційного опромінення, хоч би яким низьким був рівень такого опромінення.
- Хоча використання комп'ютера часто все ще регламентується вдома, багато батьків вважають, що використання мобільних телефонів є «особистою справою». Підбадьорені новоздобутою свободою, діти можуть потрапити у фінансові проблеми, витрачаючи гроші на медіакампанії з «роздачі» призів або аксесуари, наприклад, рингтони.
- Мобільні телефони можуть використовуватися як пристрої для стеження через наявні в них можливості геолокації. Проблема співвідношення безпеки та свободи є суперечливою.
- Технологія Bluetooth[11] створює безпекові проблеми, зокрема злом та надсилання або отримання небажаних повідомлень.
- Моблогами[12] називаються блоги (вебщоденники), які ведуться за допомогою мобільних телефонів. Вони полегшують молодим людям роботу з розміщення інформації та фотографій, але створюють потенційні загрози для їхньої власної безпеки та безпеки інших людей.
- Цькування в мобільних мережах викликає дедалі більше занепокоєння і не обмежується лише смартфонами та планшетами, оскільки зараз існують смарт-годинники з попередньо встановленими програмами для соціальних мереж.
- Камери мобільних телефонів та можливості легкого доступу до Інтернету можуть загрожувати приватності: серед молодих людей існує тривожна тенденція робити «компрометаційні фотографії» (наприклад, зображення інших молодих людей в роздягальні спортзалу або в незручних ситуаціях, зображення вчителів у класі), і навіть модифікувати ці зображення перед тим, як вивантажити їх у всесвітню мережу.
- Витрати на мобільний телефон: діти часто не підозрюють про високу вартість певних сервісів, наприклад, онлайн-голосування, небажані послуги СМС преміум-класу та покупки в застосунках.
- Оскільки мобільні телефони відволікають увагу, вони можуть становити небезпеку під час керування автомобілем, а нещодавно встановлено, що вони становлять ризик і під час ходьби. Настільки багато людей одночасно йде й пише текстові повідомлення, що є навіть застосунки, які дозволяють бачити землю, коли людина пише, опустивши голову. Вони доступні на Apple[13] чи Android[14].
- Віруси[15] заражають мобільні телефони з тих самих пір, як вони стали звичайними хатніми речами, що сталося приблизно в 2004 році. За оцінками F-Secure, існують сотні мобільних вірусів, і кількість вірусів та їхніх типів постійно зростає. Перегляньте найновіші загрози в рубриці «Описи загроз»[16].

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Інтернет «на ходу» створює декілька ризиків, оскільки багато хто не замислюється про використання відповідних налаштувань конфіденційності. Можливість використання та наявність декількох пристроїв для кожного користувача роблять несанкціоновані втручання більш імовірними.
- Багато користувачів користуються перевагами безкоштовного бездротового підключення, доступного в кафе, ресторанах та інших громадських місцях, і надають особисту та фінансову інформацію в таких місцях.

11. https://en.wikipedia.org/wiki/Bluetooth
12. https://en.wikipedia.org/wiki/Mobile_blogging
13. https://itunes.apple.com/en/app/type-n-walk/id331043123?mt=8
14. https://play.google.com/store/apps/details?id=com.biztech.typewhilewalk&hl=en
15. http://en.wikipedia.org/wiki/Computer_virus; https://en.wikipedia.org/wiki/Mobile_virus and worms; http://en.wikipedia.org/wiki/Computer_worm
16. https://www.f-secure.com/en/web/labs_global/threat-descriptions

- Інтернет будь-коли та будь-де також означає, що не існує періоду спокою для ухвалення рішень щодо того, що вивантажувати чи розміщувати онлайн, які покупки чи інші дії вчиняти онлайн. Наприклад, багато застосунків дозволяють трансляцію подій у прямому ефірі, коли вони ще відбуваються, тому ваша дитина може транслювати конфузну або насильницьку сцену, що розгортається на її очах, не маючи можливості задуматися над тим, чи варто записувати або публікувати такий контент.
- Завдяки легкості, з якою навіть зовсім маленькі діти можуть робити покупки через мобільні пристрої, фахівці попереджають про тенденцію до того, що вони називають «віртуалізацією» грошей, коли дітям важко зрозуміти реальну цінність грошей.

ЯК ЦЕ РОБИТИ

Мобільні телефони користуються популярністю, і володіти ними легко і порівняно недорого. Після придбання мобільника ви можете вибрати оплату за певну кількість хвилин на замовлення, або ви можете підписатися на послуги певного постачальника та платити щомісячну плату за них.

Мобільні пристрої, наприклад, смартфони, планшети, пристрої для читання та надолонні ігри потребують лише підключення Wi-Fi, щоб забезпечити доступ до онлайн-світу.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

Оскільки мобільні телефони настільки популярні серед молоді, вчителі можуть залучати учнів до роботи шляхом використання СМС-повідомлень тощо у класних заняттях. Той факт, що надолонні пристрої можна переносити, є вигідним для вчителів, які перебувають у русі, а також учнів, які працюють у групах або виконують практичні дослідження. Установлено, що використання мобільних пристроїв у навчанні як у школі, так і поза школою спонукає учнів брати відповідальність за свою роботу та зменшує ймовірність втрати ними нотаток та завдань.

- Під час екскурсії попросіть учнів записати свої враження на мобільні пристрої, використовуючи фотографії та відео для доповнення своїх відповідей на завдання.
- Попросіть учнів використовувати різні застосунки для деталізації своїх домашніх завдань, наприклад, Vine для коротких відео, Periscope для повідомлень з місця події або Twitter та Facebook для оновлення навчальної інформації.
- Попросіть учнів назвати ризики та проблеми, які створює використання смартфонів і мобільних пристроїв у класі. Чи вважають вони, що класну кімнату можна оснастити продуктами інформаційних технологій на 100%? Чому?

НАЛЕЖНА ПРАКТИКА

- Використовуйте мобільний телефон із низьким випромінюванням[17], тобто телефон із коефіцієнтом питомого поглинання вуха не більше 0,56 Вт/кг і коефіцієнтом питомого поглинання тіла менше за 0,57 Вт/кг, а також гарнітурою – найкращі з цих пристроїв оснащені частотним фільтром.
- Заохочуйте молодих людей до обмеження використання мобільних телефонів та планшетів. Проте не забороняйте таке використання. Використання мобільних телефонів та різноманітних месенджерів є широко розповсюдженим явищем серед підлітків, і в багатьох колах це є необхідним для спілкування серед однолітків.
- Не залишайте функцію Bluetooth увімкненою, якщо вона не використовується, щоб уникнути безпекових ризиків.
- Як і з електронною поштою, приймайте дані лише з надійних джерел. Остерігайтеся СМС-спаму: діліться своїм номером мобільного лише з людьми, яких ви добре знаєте.
- Перш ніж публікувати фотографії, переконайтеся, що вони не порушують законні права інших осіб.
- Поговоріть зі своїми дітьми про обмін шкідливим контентом та підкресліть, що це може суперечити національним законам про захист молоді.
- Використовуйте телефон і планшет з повагою до інших. Людям навколо вас може не сподобатися, що їм доводиться слухати вашу розмову.

17. http://www.phonerated.com/top-rated-best-overall-low-sar-phones-global

- Якщо вас турбують небажані дзвінки або СМС, зв'яжіться зі своїм оператором мобільного зв'язку або національним телефоном довіри Insafe[18].
- Багато мобільних телефонів мають функцію фільтрування: використовуйте чорний список, щоб заблокувати небажані номери, або білий список, щоб приймати лише дзвінки з відібраних номерів (наприклад, лише номерів із адресної книги). Можна також завантажити фільтри батьківського контролю з Інтернету (безкоштовно) або придбати їх у свого мобільного оператора.
- Пам'ятайте, що мобільні телефони – не єдині пристрої, за допомогою яких можна спілкуватися: планшети та смарт-годинники також мають функції обміну повідомленнями та голосового зв'язку.
- Для дітей молодшого віку або підлітків, які ще не здатні відповідально розпоряджатися своїми фінансами, виберіть план із попередньою оплатою замість щомісячної передплати, щоб уникнути неприємних сюрпризів. Обговоріть їхні витрати та переконайтеся, що вони розуміють справжню цінність грошей.
- Не забудьте налаштувати смартфон вашої дитини одразу після покупки. Більшість пристроїв оснащені повноцінними функціями (камера, GPS, ближній безконтактний зв'язок, Bluetooth тощо) і за замовчуванням налаштовані для використання дорослими. Не соромтеся шукати онлайн-інструкції з налаштування смартфона вашої дитини. Деякі з рекомендованих кроків є такими: налаштуйте захищений паролем обліковий запис дитини, відключіть можливість покупок у застосунках, відключіть встановлення нових застосунків (для найменших дітей), відключіть геолокацію та використання GPS і встановіть програмне забезпечення для батьківського контролю.

ДОДАТКОВА ІНФОРМАЦІЯ

- Звіт GSMA може допомогти вам зрозуміти мобільну галузь: *<http://web.archive.org/web/20160411155639/http://www.gsmamobileeconomy.com/GSMA_ Global_Mobile_ Economy_Report_2015.pdf>*.
- Європейський соціальний, цифровий та мобільний ландшафт у 2014 році представлено в цій низці інфографічних матеріалів: *<http://web.archive.org/web/20151211195326/http://wearesocial.net/blog/2014/02/social- digital-mobile-europe-2014/>*.
- S212 є незалежним британським сайтом для огляду мобільних телефонів та інших пристроїв: *<http://www.s21.com/mobile-phones.htm>.*
- ЮНЕСКО опублікувала доповідь про майбутнє мобільного навчання та його наслідки для творців політики та планувальників: *<http://unesdoc.unesco.org/images/0021/002196/219637E.pdf>.*
- Онлайн-видання «Діти та мобільні телефони, порядок денний для дій» укладено Childnet International: *<http://www.childnet.com/ufiles/CMPAAA_A4.pdf>*.
- Британська комісія з класифікації фільмів взяла на себе функції Незалежної комісії з класифікації мобільного контенту (Independent Mobile Classification Body, IMCB), щоб створити розроблені незалежним органом принципи, що лежать в основі кодексу практики мобільних операторів: *<http://www.bbfc.co.uk/what-classifi ation/mobile-content>*.
- Дізнайтеся про захист Bluetooth та як він працює: *<http://web.archive.org/web/20160407133222/http://electronics.howstuffworks.com/bluetooth4.htm>*.
- Мобільний оператор Vodafone склав посібник для батьків: *<https://www.vodafone.com/content/parents/howto-guides.html>.*

18. http://www.saferinternet.org/ww/en/pub/insafe/focus/national_helplines.htm
19. http://www.creditcards.com/credit-card-news/whos-responsible-kids-unauthorized-charges-1279.php

2. Інтернет – поєднуючи ідеї та людей

> «Зрештою все поєднується між собою – люди, ідеї, предмети. Якість цих з'єднань є ключовою для якості як такої».
> *Чарлз Імс, дизайнер початку XX сторіччя*

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 6 – ЕЛЕКТРОННА ПОШТА ТА ЗВ'ЯЗОК

Чи створили ви кілька облікових записів електронної пошти та встановили окремий пароль для кожного з них?
Чи є пароль достатньо надійним (довжиною більше 8 знаків із поєднанням літер, цифр та інших символів)?
Чи чітко ви позначаєте свої електронні листи відповідними ключовими словами в рядку «Тема»?
Чи ввімкнули ви дворівневу систему безпеки для своїх облікових записів електронної пошти (ввівши додаткове захисне запитання та/або номер свого мобільного телефону)?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 7 – ЧАТ І МЕСЕНДЖЕРИ

Чи помістили ви контактні дані на своєму вебсайті або в блозі? Чи вжили ви заходів щодо захисту вашої приватності онлайн?
Чи перевірили ви контент, який використовуєте для свого вебсайту/блогу, на відповідність законодавству про авторські права?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 8 – СОЦІАЛЬНІ МЕРЕЖІ І ПОШИРЕННЯ ІНФОРМАЦІЇ В СОЦІУМІ

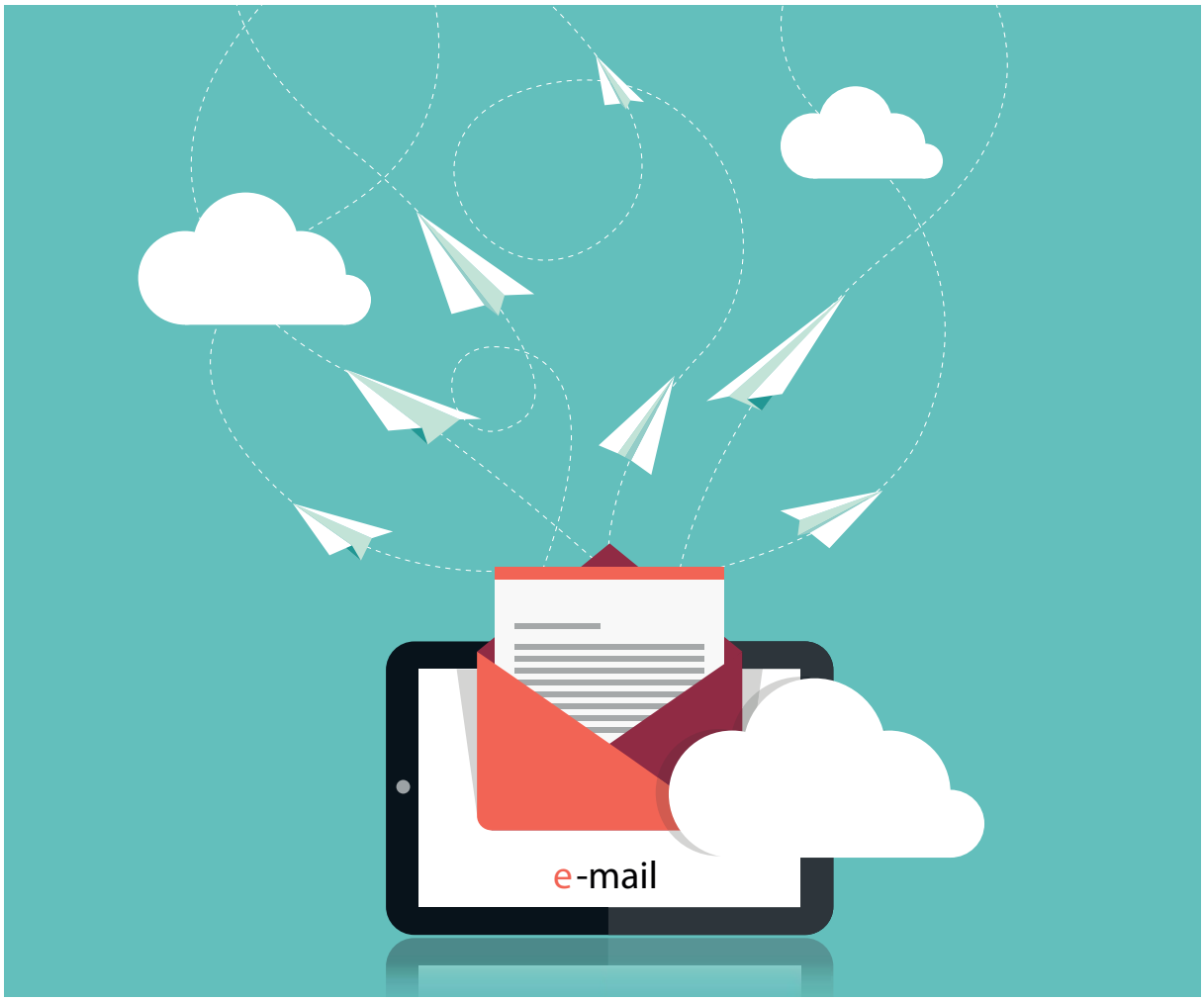
Репутація не відновлюється: чи завжди ви думаєте, перш ніж розміщувати допис? Коли ви востаннє оновлювали свої налаштування конфіденційності на вебсайтах, якими користуєтесь?
Демократія залежить від участі якомога більшої кількості громадян у публічних дебатах: Чи намагалися ви зробити свій голос чутним через відповідні сайти соціальних мереж?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 9 – КОНФІДЕНЦІЙНІСТЬ І НАЛАШТУВАННЯ КОНФІДЕНЦІЙНОСТІ

Чи справді потрібно розміщувати цю фотографію з міткою на сайті соціальної мережі?
Чи читали ви угоду про мобільний застосунок, щоб зрозуміти, чим ви ділитесь: чим володієте ви, а чим «вони»?
Завантажуючи програми, чи впевнені ви, що точно знаєте, до якої приватної інформації вони матимуть доступ? Чи справді без такого доступу застосунок не працюватиме?
Чи розумієте ви, що для вас означає Загальний регламент Європейського Союзу про захист даних?

Інформаційний матеріал 6

Електронна пошта та зв’язок



Електронна пошта[1] (E-mail англійською) – це система для надсилання повідомлень між комп’ютерами, підключеними до мережі, зокрема Інтернету. Цей термін може означати також і саме повідомлення. Зазвичай електронний лист успішно передається за лічені секунди, і одержувач може отримати до нього доступ та відповісти, коли йому буде зручно. Гнучка та ефективна система електронної пошти кардинально змінила наш спосіб роботи та спілкування. Щодня відправляються мільйони повідомлень.

Адреса електронної пошти складається з двох частин: локального та доменного імен, розділених знаком «@». Локальне ім’я часто, хоча й не завжди, вказує на ім’я користувача. Доменне ім’я може вказувати на організацію, до якої належить користувач, його компанію чи інтернет-провайдера. Доменні імена можуть також указувати на тип організації та/чи країну. Наприклад, власник адреси name@ox.ac.uk – це хтось, хто працює або навчається в Оксфордському університеті.

Незважаючи на те, що з’явилося багато інших способів спілкування, облікові записи електронної пошти все ще залишаються в центрі онлайн-життя користувача, оскільки часто лише з їх використанням можна створити облікові записи для участі в інтернет-сайтах. Отже, хоча люди тепер можуть надавати перевагу іншим засобам спілкування (соціальні мережі, обмін миттєвими повідомленнями тощо), облікові записи електронної пошти стали «ключем» до онлайн-ідентичності користувачів, часто слугуючи «логіном» для підключення до всіх онлайн-сервісів, якими вони користуються.

1. https://en.wikipedia.org/wiki/Email

ЗНАЧЕННЯ ДЛЯ ОСВІТИ

Оскільки адреси електронної пошти так часто запитують онлайн, навчання правильно керувати обліковим записом електронної пошти має велику освітню цінність, подібно до навчання сортуванню фізичної пошти шляхом класифікації особистих та важливих адміністративних повідомлень, щоб їх можна було легко знайти.

Електронна пошта також є цінним інструментом міжкультурних проєктів за участю класних колективів дітей і молоді з різних країн. Діти та молодь можуть використовувати цей інструмент для вдосконалення своїх мовних навичок та поширення інформації про свою культуру.

Деякі з більш стриманих дітей та молоді можуть висловлюватись краще за допомогою електронної пошти, ніж при особистому обговоренні в класній кімнаті.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Оскільки ваша електронна пошта є «воротами» до всіх ваших облікових записів онлайн, наслідки того, що хтось проникне у ваш обліковий запис електронної пошти, можуть бути дуже серйозними.
- Більшість електронних поштових клієнтів (комп'ютерних програм, що використовуються для доступу до електронної пошти та керування електронною поштою користувача[2]), які ви можете знайти онлайн, є безкоштовними, але багато з них використовують алгоритми для сканування вмісту ваших електронних листів та показу таргетованої реклами на сторінці вебпошти.
- Важко висловлювати емоції за допомогою електронної пошти. Ось чому вам слід завжди писати свої повідомлення обережно, щоб їх не можна було зрозуміти неправильно. «Емотикони»[3] (маленькі виразні значки, смайлики) можуть допомогти вам висловити почуття, які ви хочете передати, особливо іронію чи гумор. Однак використовуйте їх економно, щоб не відволікати увагу від вашого повідомлення.
- Велика частка отримуваних електронних листів є непрошеним та, як правило, небажаним спамом[4] (див. Інформаційний матеріал 19 про спам, шкідливі програми, шахрайство та безпеку). На щастя, спам-фільтри дедалі краще відокремлюють спам від звичайних електронних листів.
- Переконайтеся, що ви самі не сприяєте «спаму», зловживаючи пересиланням електронних листів, які ви вважаєте «смішними» або «цікавими», всім своїм контактам. Якщо ви робите це занадто часто, спам-фільтри можуть визначити вашу адресу електронної пошти як проксі-сервер для спаму та додати його до чорного списку, що унеможливить для вас зв'язок із кимось.
- Деякі переслані повідомлення є неправдивими чи шахрайськими. Прикладом можуть бути електронні листи, в яких неправдиво стверджується, що якась компанія чи організація пообіцяла сплачувати невелику суму грошей на певну благодійну мету (таку мету часто вказують; це може бути, наприклад, лікування хворої дитини, яка потребує хірургічного втручання) щоразу, коли лист пересилається.
- Ім'я легко приховати, щоб вводити людей в оману. Це можна зробити, просто змінивши ім'я в налаштуваннях або створивши фіктивну адресу вебпошти, наприклад, elvispresley@hotmail.com. Навіть якщо ви впізнаєте адресу електронної пошти як адресу когось із ваших контактів, перевірте також рядок теми, оскільки машина власника адреси могла стати «зомбі-комп'ютером»[5], ураженим хакером чи вірусом.
- Посилання може начебто спрямовувати вас на один вебсайт, а насправді вести на інший. Це особливо часто зустрічається у шахрайських операціях категорії «фішинг»[6].

2. https://en.wikipedia.org/wiki/Email_client
3. https://en.wikipedia.org/wiki/Emoticon#Basic_examples
4. https://en.wikipedia.org/wiki/Email_spam>
5. https://en.wikipedia.org/wiki/Zombie_(computer_science)
6. https://en.wikipedia.org/wiki/Phishing

НАЛЕЖНА ПРАКТИКА

- Створіть декілька облікових записів електронної пошти для різних цілей (реєстрація на сайтах соціальних мереж, придбання товарів онлайн тощо). Залиште один обліковий запис якомога приватнішим, не публікуючи його в мережі та використовуючи його виключно для важливих сервісів, якими користуєтесь ви та ваші друзі. Використовуйте інший обліковий запис, щоб зареєструватися на сервісах, якими ви можете скористатися лише один раз, або сервісах, якими користуєтеся рідко.
- Повідомлення електронної пошти повинні бути короткими та чіткими. Намагайтеся уникати довгих абзаців. Перевіряйте правопис.
- Не забувайте вписувати відповідні слова в рядок «Тема». Це допомагає одержувачу визначити ваше повідомлення як справжнє, а пізніше знайти його.
- Створіть надійні паролі для своїх облікових записів електронної пошти (довжиною більше 8 знаків із поєднанням літер, цифр та інших символів) і використовуйте різні паролі для різних облікових записів.
- Поважайте інших при визначенні обсягу електронних листів, які ви розсилаєте, і робіть розумний, продуманий вибір моделі спілкування. Якщо вам потрібно провести групове обговорення з великою кількістю людей, можливо, корисніше буде організувати конференц-дзвінок або чат на приватному форумі, а не надсилати величезну кількість електронних листів.
- Не треба перевіряти електронну пошту раз на 10 хвилин. Багато людей дозволяють електронній пошті постійно переривати свої заняття.
- Як правило, не включайте до електронного листа конфіденційну інформацію, зокрема банківські реквізити. Таку інформацію потрібно надсилати лише в рідкісних випадках, наприклад, щоб забронювати готель. Якщо сумніваєтесь, будьте обережні, перевірте онлайн-репутацію сервісу, яким ви хочете скористатися, перевірте процедуру скасування дії вашої картки або конкретної транзакції, використовуйте більш безпечні платіжні сервіси, такі як PayPal, і уникайте менш безпечних сервісів, таких як сервіси прямих грошових переказів (наприклад, Western Union). Однак ніколи не надсилайте електронним листом такі дані, як ім'я користувача та пароль до своїх облікових записів онлайн. Онлайн-сервіси ніколи не будуть просити вас про це, тож якщо ви отримаєте електронне повідомлення із запитом таких деталей, це однозначно спроба фішингу.
- Дедалі складніші фішинг-стратегії використовують електронні листи з підробними повідомленнями, які ідеально імітують повідомлення, які ви отримуєте від сервісів, якими користуєтесь (сайтів соціальних мереж), і направляють вас на підробний вебсайт, який запитує для входу ваше ім'я користувача та пароль. Обов'язково завжди перевіряйте адресу електронної пошти відправника та адресу вебсайту на наявність чогось незвичного.
- Зберігайте здоровий скептицизм щодо отримуваних вами електронних листів. Не відкривайте електронні листи, якщо ви не довіряєте їх джерелу.
- Будьте особливо обережні щодо вкладень. Якщо ви не очікували вкладення від цього відправника або не довіряєте йому з будь-якої іншої причини, видаліть його не відкриваючи. Навіть вкладення від відомих та надійних відправників слід спочатку зберегти, а потім просканувати перед відкриттям.
- Користуйтеся всіма функціями безпеки, які пропонує ваш поштовий клієнт. Зазвичай поштові клієнти дозволяють ввести додаткову адресу електронної пошти на випадок, якщо обліковий запис електронної пошти буде зламаний, і дедалі частіше поштові клієнти пропонують ввести номер свого мобільного телефону для додаткових безпекових перевірок у виняткових випадках. Якщо ваш обліковий запис зламано, правильно налаштуйте параметри безпеки, щоб вам було легше його відновити.
- Для отримання додаткових порад щодо електронної пошти обов'язково ознайомтесь із Інформаційним матеріалом 19 щодо спаму, шкідливих програм, шахрайства та безпеки.

ЯК ЦЕ РОБИТИ

- Щоб переглянути свої електронні листи, ви можете скористатися «офіційним» застосунком служби електронної пошти на своєму смартфоні, планшеті або навіть на комп'ютері, який використовує Windows 8 або новішу версію (наприклад, застосунок Gmail, Outlook або Yahoo!), перейти на вебсайт служби електронної пошти (за допомогою сервісу «вебпошти»), або ви можете використовувати якийсь поштовий клієнт, який є зовнішнім застосунком, завантажує електронні листи з вашого сервісу електронної пошти та дозволяє вам керувати ними/організовувати їх. Позитивна риса використання електронного поштового клієнта полягає в тому, що ви можете налаштувати його для завантаження електронних листів з декількох різних сервісів електронної пошти, щоб ви могли в одному місці переглядати всі свої електронні листи з різних електронних адрес. Найпопулярнішими поштовими клієнтами є Thunderbird та Outlook. Поштові клієнти в основному використовуються для професійного електронного листування.
- Додаткову інформацію про налаштування спам-фільтра див. у Інформаційному матеріалі 19 щодо спаму, шкідливих програм, шахрайства та безпеки.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

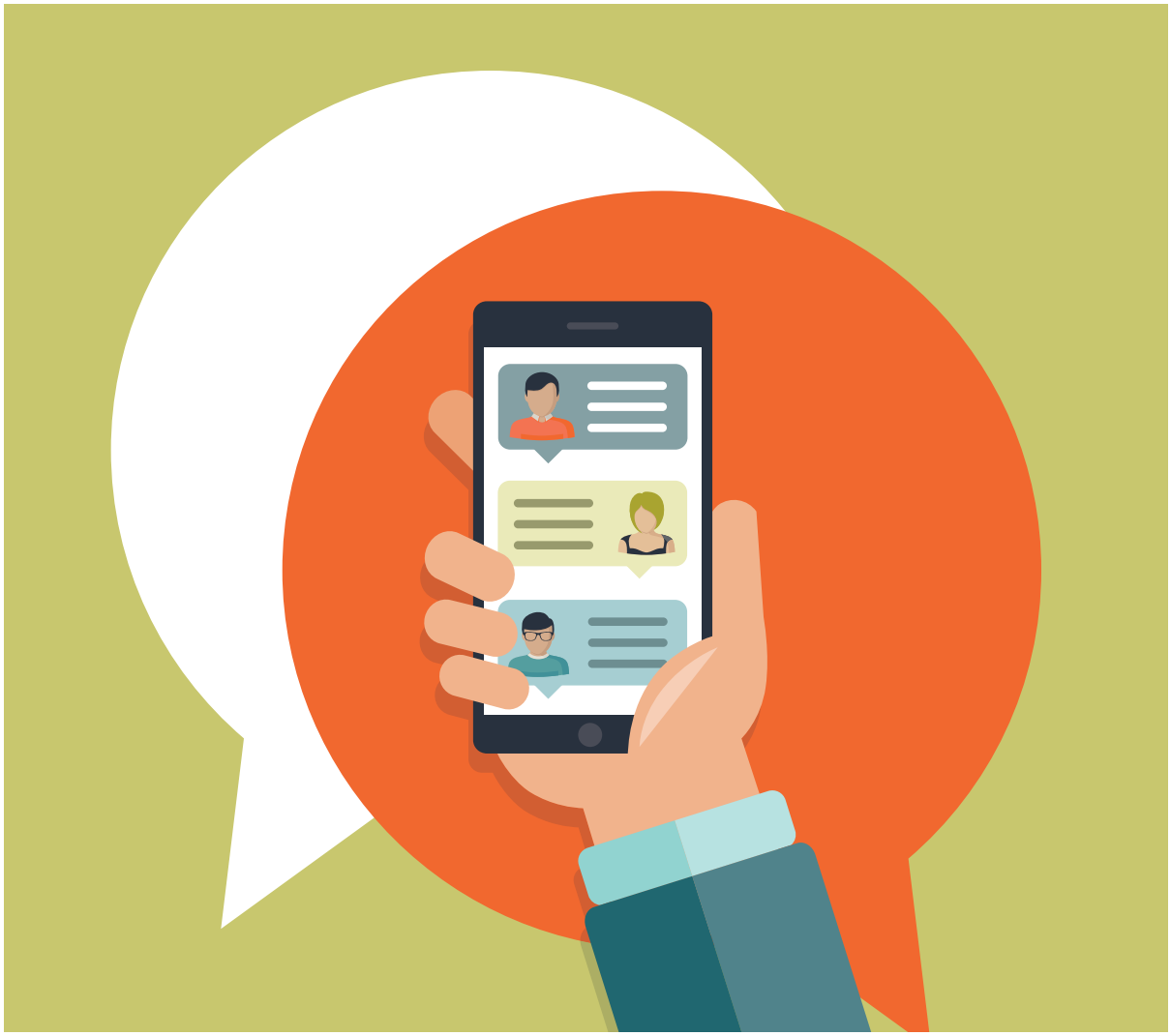
- Працюючи з учнями старшого віку, які мають електронні адреси, попросіть їх підключитися до своїх сервісів електронної пошти та вивчити налаштування безпеки, щоб захистити свої облікові записи електронної пошти, додавши додаткове безпекове запитання, другу адресу електронної пошти або номер мобільного телефону.
- Ось процедури, яких слід дотримуватись, щоб захистити свій обліковий запис електронної пошти на Gmail, Yahoo! чи Outlook.
  - <https://support.google.com/accounts/answer/46526?hl=en>
  - <http://windows.microsoft.com/en-us/windows/outlook-security>
  - <https://help.yahoo.com/kb/SLN8292.html>
- Існує багато провайдерів послуг електронної пошти, крім трьох «великих», назви яких наведено вище. Чому ми наполягаємо на вивченні саме цих трьох? Тому що, принаймні у випадку Gmail та Outlook/Hotmail вони пов'язані з багатьма іншими сервісами. Наприклад, обліковий запис Google є майже необхідністю, коли у вас є смартфон з операційною системою Android, а обліковий запис Outlook часто пов'язаний з операційною системою Windows. Це означає, що, незалежно від ваших уподобань, ви можете бути «змушені» створити обліковий запис електронної пошти в одній зі служб, наведених вище. Але ви, звичайно, можете користуватися поштовими клієнтами з вищими стандартами конфіденційності, такими як Web.de або Protonmail.com. Навіть ваш інтернет-провайдер зазвичай пропонує сервіс електронної пошти. Не соромтеся шукати інші альтернативи в Інтернеті.
- Поділіть своїх учнів на команди з трьох чи більше осіб і попросіть їх створити хороші паролі для уявного облікового запису електронної пошти. При цьому дуже чітко поясніть, що вони не повинні ділитися своїми справжніми паролями! Після 10-хвилинного мозкового штурму попросіть кожну команду представити запропонований пароль та пояснити, чому вони вважають його безпечним. Допоможіть їм визначити характеристики надійного пароля (довжиною більше 8 знаків, серед яких мають бути літери, цифри та інші символи) та типові слабкі місця ненадійних паролів (їх можна знайти у словнику, вони якимось чином пов'язані з вами – кличка собаки, прізвище тощо).

ДОДАТКОВА ІНФОРМАЦІЯ

- Добре відомими поштовими клієнтами є, наприклад, Microsoft Outlook: *<https://products.office.com/ en-us/outlook/email-and-calendar-software-microsoft-outlook>* або Mozilla Thunderbird: *<http://www.mozilla.org/projects/thunderbird/>*.
- Truth or Fiction – це вебсайт, на якому інтернет-користувачі можуть перевірити достовірність електронних листів, що часто пересилаються *<http://www.truthorfiction.com/>*. Іншим подібним вебсайтом є *<http://m.snopes.com/ whats-new/>*.
- Три найпопулярніші сайти вебпошти – це Outlook: *<https://office.live.com/start/Outlook.aspx>*, Yahoo! *<https://mail.yahoo.com>* і Gmail, що належить компанії Google *<http://www.gmail.com>*. Не соромтеся шукати альтернативних провайдерів послуг електронної пошти, особливо у вашій країні.
- Відповідні статті Конвенції ООН про права дитини:
  Стаття 13 – Діти мають право одержувати і поширювати інформацію, якщо це не шкодить їм чи іншим особам.

Інформаційний матеріал 7

Чат і месенджери



«Чат» – загальний термін, що позначає інтерактивне спілкування, яке відбувається на виділеному каналі обговорення. Користувачі можуть спілкуватися з групами людей у чатах[1] або вести приватні розмови з обраними друзями за допомогою сервісів обміну[2] миттєвими повідомленнями.

Чат – це неформальний спосіб спілкування, подібний до очних розмов, і в ньому бере участь двоє чи більше людей. Репліки в чаті зазвичай набираються як текст, але можуть також включати потокове передавання відео чи аудіо[3] за допомогою гарнітури або вебкамер. Спілкування в цій формі відбувається миттєво і, отже, відрізняється від електронної пошти, яка не вимагає присутності одержувача онлайн одночасно з відправником.

Чат у порівнянні з обміном миттєвими повідомленнями

Ці терміни використовуються як взаємозамінні, проте користувач може спілкуватися в чаті, користуючись послугами обміну миттєвими повідомленнями, але надсилання миттєвого повідомлення (МП) не є участю в чаті. Раніше спілкування в чатах було досить популярним, але, здається, воно зараз втрачає свої позиції на користь обміну миттєвими повідомленнями та інших засобів обміну повідомленнями. Багато компаній не схвалюють використання МП у робочому середо-

1. https://simple.wikipedia.org/wiki/Chat_room
2. https://en.wikipedia.org/wiki/Instant_messaging
3. https://en.wikipedia.org/wiki/Streaming_media

вищі, оскільки воно має тенденцію знижувати продуктивність праці, якщо працівників постійно відволікають повідомленнями від виконання своїх завдань.

Якими є інші засоби обміну повідомленнями?

Застосунки для обміну повідомленнями, наприклад, WhatsApp, Kik, Viber, Telegram або iMessage, дедалі частіше використовуються власниками смартфонів. Такі застосунки з автоматичним видаленням, як Snapchat та Wickr, також популярні серед власників смартфонів. Такі типи засобів обміну повідомленнями, як правило, безкоштовні, і пропонують більше «конфіденційності», ніж механізми обміну повідомленнями, які доступні на більших платформах, таких як Facebook, Twitter або LinkedIn.

Швидка доступність цих застосунків для обміну повідомленнями на смартфонах часто означає, що користувачі знімають відео, коментують, фотографують та надсилають результат, перш ніж замисляться про наслідки. Тому, на жаль, їх називають серед чинників поширення онлайн-переслідувань та цькування.

Зростання поширеності сервісів обміну миттєвими повідомленнями та інших засобів обміну повідомленнями, безсумнівно, триватиме, оскільки смартфони виходять на нові ринки. Facebook придбав WhatsApp, японська компанія Rakuten придбала Viber, а багато інших застосунків для обміну повідомленнями отримали інвестиції від зацікавлених сторін. Відтак ситуація абсолютно ясна: засоби обміну повідомленнями існуватимуть ще довго.

Чому важливо розуміти, як працюють чат та обмін миттєвими повідомленнями

Спілкування в чаті та обмін миттєвими повідомленнями – це популярні заняття вільного часу, які змінюють спосіб спілкування молодих людей між собою. Спілкування в чаті та обмін миттєвими повідомленнями використовуються з позитивним ефектом, оскільки учні обмінюються ідеями та обговорюють домашні завдання й інші академічні проєкти, але, на жаль, вони також використовуються для цькування та переслідування інших в Інтернеті (див. Інформаційний матеріал 21 про цькування та переслідування).

Вчителі часто недооцінюють, наскільки чат важливий для молоді, і можуть втратити можливість використати його як освітній інструмент. Це можна зробити, наприклад, так:

- мозкові штурми та обговорення в реальному часі, зосереджені на певних проблемах;
- рольові ігри та моделювання;
- обмін думками, дебати, тематичні обговорення в малих групах;
- індивідуальне навчання та керівництво;
- групове дослідження;
- творення онлайн-спільноти.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Коли чат ґрунтується на текстових повідомленнях, соціальні сигнали, жести та невербальна комунікація не можуть передаватися через набір тексту, а відтак непорозуміння можуть легко виникати онлайн. Потрібно бути настільки ж приємним у спілкуванні, ввічливим і вихованим, як і в реальних життєвих ситуаціях, і виховати в себе звичку дотримуватися правил мережевого етикету [4]. Гумор та емоції також можна показати за допомогою емотиконів [5] – маленьких символів, схожих на обличчя. Більшість молодих людей використовують у своїй мові скорочення, і ви можете знайти словник найпоширеніших із них за адресою: *<http://www.netlin- go.com/acronyms.php>*.
- Спілкуючись із незнайомими людьми в мережевому чаті, також важливо пам'ятати, що люди не завжди є тими та такими, якими вони представляються. Закриті чати з використанням програм для групової роботи [6], які надають можливість проведення конференцій у школі чи класі, безпечніші у використанні, оскільки доступ обмежений визначеною групою користувачів.
- Час, витрачений на спілкування в чаті або надсилання МП, значно збільшився, оскільки сучасні підлітки щодня надсилають сотні повідомлень у різних формах.

4. https://en.wikipedia.org/wiki/Etiquette_in_technology#Netiquette
5. https://en.wikipedia.org/wiki/Emoticon
6. https://en.wikipedia.org/wiki/Collaborative_software

(текстові повідомлення, МП, повідомлення в чатах, електронні листи тощо). Хоча ергономіка комп'ютерних клавіатур та комп'ютерних мишей значно покращилася, з'явилися нові синдроми, зокрема «підлітковий текстовий тендиніт». Смартфони є відносно недавніми пристроями, і надсилання повідомлень або введення довгих електронних листів може призвести до надмірного використання великих пальців. Отже, обмеження спілкування в чаті та надсилання текстових повідомлень є не лише проблемою збереження балансу між життям і роботою, але й проблемою здоров'я.

- Хоча багато програм для обміну МП виглядають «безкоштовними», завжди майте на увазі, що компанія повинна так чи інакше покривати свої операційні витрати. Багато застосунків обирають стратегію «створювати базу та продавати», залучаючи користувачів «безкоштовним» застосунком, а потім продаючи базу користувачів іншій компанії, як тільки вона стане достатньо великою. Так сталося з Whatsapp, який було куплено Facebook-ом. Інші застосунки, такі як Snapchat, спочатку створюють свою базу користувачів, а потім починають вводити рекламу. Завжди пам'ятайте про бізнес-модель того сервісу обміну МП, яким ви користуєтесь, і обирайте його обдумано, беручи до уваги зворотні сторони його переваг (менша конфіденційність, контроль за вашими даними, вплив реклами, річна/щомісячна плата тощо).
- Люди часто обмінюються файлами за допомогою засобів обміну повідомленнями та спілкування в чаті, і важливо пам'ятати, що файли можуть містити шкідливі програми. Перш ніж ділитися файлами, переконайтеся, що всі вони перевірені на віруси, і скануйте перед відкриттям все, що отримуєте (див. Інформаційний матеріал 19 з питань безпеки).
- Було багато негативної інформації щодо ризиків, з якими можуть зіткнутися молоді люди під час використання чатів. Через кілька гучних кримінальних справ батьки та вчителі часто занепокоєні можливістю контакту дітей з педофілами в чатах, особливо в процесі участі в онлайн-іграх (див. Інформаційний матеріал 16 про ігри). Хоча ці небезпеки існують, важливо тверезо оцінювати такі ризики. Величезна більшість користувачів чатів є саме тими, ким вони себе називають, і спілкування в чаті є переважно абсолютно невинним. Замість того, щоб поширювати страхи або забороняти використання чатів, дорослі повинні надавати нові можливості молодим людям, навчаючи їх заходам безпеки. Ось декілька основних правил, яких повинні дотримуватися діти та молодь:
  - Оберіть чат, який відповідає вашій віковій групі та має модератора-людину, і повідомляйте модератору про будь-які небезпечні випадки.
  - Використовуйте ґендерно-нейтральне ім'я користувача й ніколи не повідомляйте свою особисту інформацію та не публікуйте своїх фотографій (див. Інформаційний матеріал 9 щодо приватності).
  - Якщо ви дійсно збираєтеся зустрітися з другом, якого знайшли в чаті, обговоріть це спочатку зі своїми батьками та візьміть із собою дорослого, якому довіряєте. Завжди проводьте першу фізичну зустріч з кимось, кого ви зустріли онлайн, у громадському місці, наприклад, на міській площі.
  - Якщо щось, із чим ви зіткнулися під час сеансу спілкування в чаті, викликає у вас почуття дискомфорту, скажіть про це комусь із дорослих. Якщо у вас виникають проблеми в чаті чи деінде в Інтернеті, ви завжди можете обговорити це з досвідченими порадниками за вашим національним телефоном довіри[7].
  - Якщо ви хочете поспілкуватися в чаті зі знайомими вам людьми, подумайте про використання сервісу миттєвих повідомлень (наприклад, MSN, Skype) замість чату, щоб ви могли контролювати свій список контактів.

ЯК ЦЕ РОБИТИ

- У мережі доступні багато різних програм для спілкування в чаті. Можна знайти широкий асортимент таких програм, шукаючи «чат» у будь-якій пошуковій системі[8]. Багато програм для мережевих чатів, як-от Yahoo Chat[9], ICQ[10] та AOL Chat[11], пропонують широкий спектр чатів із дискусійними групами, які працюють в режимі реального часу. Часто користувачам спочатку потрібно завантажити невеликий застосунок, щоб увімкнути чат та зареєструватися у модератора, але потім вони можуть вільно входити в нього та брати в ньому участь.
- Застосунки для миттєвого обміну повідомленнями[12], які дозволяють вести приватні розмови з вибраними користувачами, тепер є популярнішими за чати. Ці можливості можна знайти, шукаючи «обмін миттєвими повідомленнями» в будь-якій пошуковій системі. Користувачі завантажують застосунок, щоб увімкнути обмін миттєвими повідомленнями, а потім складають список людей, з якими хочуть поспілкуватися в чаті. Оскільки спілкування відбувається в обмеженій групі користувачів, обмін миттєвими повідомленнями часто вважається «безпечнішим», ніж спілкування в чатах.

7. www.betterinternetforkids.eu/web/portal/practice/helplines
8. https://en.wikipedia.org/wiki/Web_search_engine
9. http://chat.yahoo.com
10. http://www.icq.com/
11. http://lifestream.aol.com
12. https://en.wikipedia.org/wiki/Instant_messaging

Як використовувати чат?

- Відкрийте обрану вами чат-програму.
- За потреби надайте ім'я користувача й пароль.
- Оберіть відповідний чат з людиною-модератором. Зазвичай існують чати для різних цілей та тем, наприклад, автомобільні групи інтересів, навчальні групи для конкретних предметів, чати для вчителів тощо.
- Після входу в систему ви побачите, як розмова учасників прокручується на головному текстовому екрані.
- Надрукуйте своє повідомлення та натисніть «enter» або клікніть «send», щоб опублікувати його і зробити видимим для учасників.
- Якщо ви хочете надіслати повідомлення певній особі, виберіть цю людину зі списку учасників, який видно у вікні.
- Багато чатів також можуть бути використані для однорангового обміну файлами[13]. Чати дозволяють обмін файлами, які є занадто великими для пересилання електронною поштою[14].
- Завжди перевіряйте свої налаштування, щоб мимоволі не додати небажаних користувачів до свого чату.

Як використовувати обмін МП?

- Відкрийте свій застосунок для обміну МП[15].
- Перевірте свій список контактів, щоб дізнатись, хто перебуває онлайн і може спілкуватися в чаті.
- Ви можете додавати нові контакти, вводячи їхні адреси електронної пошти та запрошуючи їх приєднатися до вашої групи контактів. Вони отримають запрошення електронною поштою і, якщо погодяться, будуть зареєстровані у вашому списку. Це дозволить вам спілкуватися з ними в чаті в режимі реального часу, коли ви й вони перебуватимуть онлайн.
- Клікніть на ідентифікатор обраної особи, щоб надіслати повідомлення та відкрити діалог для спілкування.
- Наберіть своє повідомлення та натисніть «enter» або клікніть «send», щоб опублікувати його і зробити видимим для учасників.
- Найкраще не брати участь у розмовах із невідомими користувачами та не відповідати на електронні листи чи МП від людей, яких ви не знаєте.
- Завжди перевіряйте свої налаштування, щоб мимоволі не додати небажаних користувачів до свого МП.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Оберіть навчальну тему. Зберіть трохи орієнтаційного матеріалу, щоб допомогти учням проводити передурочні заходи. Розбийте учнів на пари чи малі групи для роботи над завданнями. Цей робочий етап повинен бути організований за моделлю групового навчання (чат найкраще працює у малих групах по 2-6 учнів).
- Наприкінці проєкту учні готують презентації, придатні для сеансу чату. Чат починається з презентацій із різних навчальних тем у невеликих групах. Спільнота учасників навчання підбиває підсумки того, що вони дізналися під час проходження курсу.
- Оскільки сеанси чату моделюють реальні розмови, вони дають учням можливості для справжньої взаємодії, а тому корисні під час вивчення іноземних мов. Учитель може заохотити учнів до участі в обговоренні, радячи їм розміщувати короткі повідомлення. Взаємодія може бути посилена шляхом створення ролей для учнів: один може бути новатором, інший – критиком. Інші учні можуть стежити за обговореннями та згодом надати відгуки.
- Environment Online (ENO)[16] – це міжнародний мережевий проєкт екологічного навчання. На початку навчального курсу учні отримують свої теми з вебсторінок проєкту, учні збирають наукові та емпіричні екологічні дані, вимірюють різні явища або фотографують їх.

13. https://en.wikipedia.org/wiki/Peer-to-peer
14. https://en.wikipedia.org/wiki/Email
15. https://en.wikipedia.org/wiki/Instant_messaging
16. http://www.enoprogramme.org

- Протягом кожного тематичного періоду організовуються віртуальні уроки у формі інтерактивних та синхронних чатів у реальному часі[17], електронних анкет та дошок оголошень[18]. До та після уроків учні обмінюються ідеями, відстежують виконання своїх завдань за допомогою чату та обмірковують те, що вони вивчили.

НАЛЕЖНА ПРАКТИКА

Мова, що використовується під час спілкування в чаті, є фрагментованою, асоціативною і розмовною за характером; учасник чату повинен не лише діяти швидко, а й бути достатньо гнучким, щоб переходити від однієї теми до іншої й навіть від однієї дискусії до іншої. Допоміжна роль учителя дуже важлива для забезпечення якості контенту та збалансованої участі всіх, хто бере участь у чаті. Чим молодші учні, тим важливішим є, щоб чат вів та модерував учитель.

- Уважно стежте за обговоренням протягом усього сеансу спілкування в чаті.
- Узгодьте розклад сеансу заздалегідь: усі повинні бути присутніми одночасно.
- Дотримуйтесь правил мережевого етикету: будьте ввічливим, добрим і ставтеся до інших із повагою, так, ніби це зустріч віч-на-віч.
- Пам'ятайте, що недбало написане повідомлення може нашкодити, навіть якщо ви цього й не хотіли.
- Короткі повідомлення сприймаються краще. Не монополізуйте сеанс чату в режимі реального часу, вставляючи шматки попередньо написаного тексту, який інші муситимуть прочитати та відповісти на нього.
- За своїм стилем спілкування в чаті близьке до потоку свідомості. Уважно читайте повідомлення інших учасників, щоб зрозуміти, що вони намагаються сказати. Іноді для цього треба заповнювати прогалини.
- Пам'ятайте, що не слід повідомляти своє ім'я користувача та пароль. Зберігайте конфіденційність всієї своєї приватної інформації під час чатів або обміну МП. Завжди існує ризик того, що хтось зробить скриншоти вашої інформації (або коментарів) і поділиться ними з іншими.

ДОДАТКОВА ІНФОРМАЦІЯ

- Деякі ідеї для шкільних учителів можна знайти за адресою: *<http://www.educationworld.com/a_tech/chat-room-get-new-life-in-classrooms.shtml>*.
- tChat є франкомовним чатом: *<http://www.tchat-orange.fr/index.php>*.
- Інформацію про «Чат у класі як соціальний інструмент» можна знайти за адресою: *<http://www.openp2p.com/lpt/a/3071>*.
- Список основних емотиконів див. у Вікіпедії: *<https://en.wikipedia.org/wiki/Emoticon#Basic_examples>*.
- Дослідницький центр П'ю (Pew Research Center) вивчає обмін мобільними повідомленнями та соціальні мережі: *<http://web.archive. org/web/20160703022409/http://www.pewinternet.org/2015/08/19/mobile-messaging-and- social-media-2015/>*.
- «Що таке snapchat і чому діти його люблять, а батьки бояться?»: *<http://web.archive.org/web/20160619055301/http://www.forbes.com/sites/larrymagid/2013/05/01/what-is-snapchat- and-why-do-kids-love-it-and-parents-fear-it/#65fc2b447875>.*
- У Данії Cyberhus використовує «груповий чат» як корисну платформу для сприяння поліпшенню самопочуття вразливих підлітків та просування їхньої більшої участі в суспільному житті: *<http://cfdp.dk/2015-cyberhus-chat-counselling-last-year/>.*

17. http://www.netlingo.com/word/real-time-chat.php
18. https://en.wikipedia.org/wiki/Internet_forum

Інформаційний матеріал 8

Соціальні мережі і поширення інформації в соціумі

Соціальний мережевий сервіс або сайт соціальних мереж (ССМ)[1] – це платформа, що використовується для створення соціальних мереж серед людей, які мають схожі інтереси чи заняття. Ця вебсистема надає користувачам різноманітні засоби взаємодії, як-от: чат, обмін повідомленнями, електронна пошта, відео, голосовий чат, обмін файлами, ведення блогів, дискусійні групи тощо.

Соціальні мережі базуються на особистих профілях, що містять ключові персональні дані, інтереси, мережу друзів тощо. Сайти соціальних мереж об'єднують спільноти людей, які мають спільні інтереси та заняття або зацікавлені в тому, щоб дізнатися більше про інтереси та заняття інших людей. Із цією метою вони надають користувачам доступ до різних типів програмного забезпечення[2].

Сайти соціальних мереж дозволяють людям встановлювати зв'язки один із одним (як правило, за допомогою сторінок самоопису для кожного члена мережі) та пропонують побудовані на довірі системи рекомендацій для встановлення зв'язків між користувачами. Деякі сайти містять каталоги певних категорій користувачів (наприклад, колишніх однокласників).

Обмін соціальною інформацією дозволяє користувачам ділитися контентом певного вебсайту на сайті соціальної мережі або у відповідному застосунку[3].

1. https://en.wikipedia.org/wiki/Social_networking_service
2. https://en.wikipedia.org/wiki/Social_software
3. www.oxforddictionaries.com/definition/english/social-sharing

Серед популярних глобальних сайтів і застосунків соціальних мереж можна назвати такі: Twitter, Facebook, LinkedIn, Google+, Snapchat, Tumblr, Pinterest, Vine і Whatsapp.

До європейських сайтів та застосунків належать, зокрема, Badoo, Bebo, Vkontakte або VK (Росія), Delphi, Draugiem.lv (Латвія), iWiW (Угорщина), Nasza-Klasa (Польща), Soup (Австрія), Glocals у Швейцарії, Skyrock, The Sphere, StudiVZ (Німеччина), Tagged, Tuenti (переважно в Іспанії) та багато інших.

Соціальні мережі є не менш важливими для обміну думками про права та основні свободи людини, і можуть надати відповідну інформацію широкому загалу.

Більшість соціальних мереж організовані навколо особливостей життєвого досвіду, але є й інші спільноти:

- спільноти учасників угод, що сприяють купівлі-продажу, здачі в оренду нерухомості чи кімнат тощо;
- спільноти за інтересами, які зазвичай зосереджені на певній темі: фільми, здоров'я тощо;
- спільноти любителів фантастики, які базуються на уявних світах та іграх: "World of warcraft" та "Second life";
- спільноти правозахисників та/або активістів боротьби за вирішення проблем, що стосуються користувачів;
- спільноти підтримки та порад, пов'язаних із інвалідністю, особливими потребами чи іншими проблемами.

Більшість соціальних мереж також пропонують прості інструменти для управління конфіденційністю персональних даних (див. Інформаційний матеріал 9 щодо налаштувань конфіденційності). Ці інструменти дозволяють користувачам надавати доступ до частин свого профілю лише своїм друзям або лише учасникам з певними ідентифікаційними даними. Вони також дозволяють учасникам обмежувати доступ для випадкових пошуків та доступ інших учасників до присвоєння міток контенту.

ЗНАЧЕННЯ ДЛЯ ОСВІТИ

- Участь у соціальних мережах та обмін соціальною інформацією – це недорогі та швидкі способи обміну різними видами контенту, від особистої інформації до маркетингової.
- Участь у соціальних мережах дозволяє людям залишатися на зв'язку, а також відновлювати зв'язки з родиною та друзями, з якими вони, можливо, втратили контакт або живуть на відстані від них.
- Мережеві сайти також дозволяють організовувати заходи. Деякі заходи можуть бути невинними, починаючи від ювелірного шоу і закінчуючи дитячою вечіркою, а інші можуть завдати шкоди, наприклад, рейв-вечірка чи демонстрація расистів/ксенофобів/гомофобів або іншої екстремістської чи орієнтованої на приниження інших людей групи.
- Багато галузей бачать важливість участі в соціальних мережах та соціального брендингу і прагнуть отримати рекомендації (і в кінцевому рахунку наростити продажі) через участь у соціальних мережах.
- Через легкість обміну соціальною інформацією через вебсайти та застосунки на смартфонах багато молодих людей обмінюються будь-чим без особливої уваги до предметів обміну.
- Відповідальна участь у соціальних мережах є принципово важливою, оскільки потенційні роботодавці, коледжі чи університети або навіть родина та друзі можуть отримати доступ до цієї інформації.
- Відповідальну участь у соціальних мережах можна розглядати як недорогий спосіб саморекламі (наприклад, молода людина, що запускає кампанію на користь певного суспільно корисного починання), створення вірусного контенту на користь певного соціального блага, або навіть пошуку визнання (коли молода людина розміщує інформацію про нагороду або сертифікат, який вона нещодавно отримала).
- Сайти соціальних мереж можуть використовуватися для просування інформації, яка є неправдивою або заснована на упереджених поглядах, що вимагає додаткової ретельності з боку користувачів у виборі «друзів» та перевірці надійності контенту.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

Люди часто говорять про відчуття свободи від використання сайтів соціальних мереж. Вони почуваються розкутими, самовпевненими, а іноді і непереможними, даючи такі коментарі та говорячи іншим такі речі, про які вони зазвичай і не подумали б у розмові віч-на-віч. Ця проблема посилюється через те, що у віртуальному світі дуже легко перебільшувати емоції або говорити речі, які ви б тримали при собі, якби спілкувалися з кимось віч-на-віч.

Сайти соціальних мереж дозволяють користувачам залишати коментарі в профілях інших людей.

Треба обдумати тип і характер таких коментарів.

Як указує британська організація Get Safe Online[4], серед ризиків використання сайтів соціальних мереж є такі:

- розголошення приватної інформації вами чи вашими друзями/контактами;
- цькування;
- кіберстеження;
- доступ до невідповідного віку контенту;
- онлайн-зваблювання та насильство (у тому числі сексуальне) щодо дітей;
- наявність коментарів, які мають жорстокий, сексуальний, екстремістський або расистський характер, або образливих дій та ненависницького ставлення;
- спроби інших людей переконати або змусити вас шляхом переслідувань до зміни принципових переконань чи ідеології або до переходу на екстремістські позиції;
- кримінальне переслідування або звинувачення в розміщенні образливих або неприйнятних коментарів;
- фішингові електронні листи, які нібито походять із сайтів соціальних мереж, але насправді заохочують вас відвідувати шахрайські або неприйнятні вебсайти;
- пости друзів, інших людей та компаній, що заохочують вас переходити на шахрайські або неприйнятні вебсайти;
- злам або захоплення вашого облікового запису чи сторінки;
- віруси або шпигунські програми, що містяться у вкладеннях до повідомлень або фотографіях;
- ви або член вашої родини повідомляєте, що виїхали або їдете у відпустку, і цим самим оголошуєте, що ваша домівка порожня, відкриваючи до неї шлях для зломників; якщо ви зробите це, а потім подасте заяву на страхову компенсацію за крадіжку зі зломом, яка відбулася за вашої відсутності, ваша страхова компанія цілком може відхилити вашу вимогу з цієї причини[5].

Є також інші ризики, наприклад:

- потрапляння під вплив комерційного контенту та використання ваших приватних даних у комерційних цілях;
- стійка шкода для вашої онлайн-репутації, що може призвести до труднощів у працевлаштуванні або інших видів дискримінації, наприклад, фінансової ізоляції (неможливість отримати позику чи страховку тощо);
- потрапляння під вплив однобічного контенту, який відповідає вашим власним переконанням/знанням/поглядам, що може обмежити ваше особисте зростання та розвиток;
- потрапляння під надзвичайно сильний соціальний тиск людей, які вимагають від вас виглядати ідеально, мати цікаве і щасливе життя і постійно публікувати вражаючі/круті пости.

Як і у випадку з усіма онлайн-технологіями, заборонити молодим людям використовувати таку технологію – це не вихід. Для молоді слід створити можливості поводитися онлайн безпечно й розбірливо (а не споживати все без розбору), а також заохочувати їх поважати вікові обмеження, зберігати особисту інформацію конфіденційною та бути відповідальними публікаторами контенту.

Відповідальні дорослі повинні самі вивчити небезпеки та належні практики безпечного користування сайтами соціальних мереж, а не намагатися зупинити таке користування. Всі ці речі природно робляться в офлайн-світі – так чому б не робити те саме і в онлайн-світі?

4. https://www.getsafeonline.org/social-networking/social-networking-sites/
5. www.getsafeonline.org/social-networking/social-networking-sites/

Молодих людей слід заохочувати говорити про свій досвід перебування онлайн з дорослими, яким вони довіряють, наприклад, батьками та вчителями. Як і з усіма іншими проблемами безпеки в Інтернеті, найбільший позитивний вплив на поведінку молодих людей онлайн має активна участь батьків та вчителів у їхньому онлайн-житті.

Це позитивно впливає і на дорослих, оскільки вони дізнаються про позитивні риси сайтів соціальних мереж.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Попросіть учнів замислитися над інформацією, яку вони вважають прийнятною для публікації в онлайн-профілі. Коли вони складуть список, попросіть їх створити профіль на папері. Чи будуть вони раді, якщо цей профіль буде відправлено всім батькам учнів цієї школи? У більшості випадків учні цього не хотіли б, але їм слід нагадати, що кожен може переглянути їхній профіль на сайті соціальних мереж, якщо він не встановлений у налаштуваннях як приватний. Установлення цього зв'язку між реальним та віртуальним світами є важливим, оскільки воно допомагає дітям та молоді усвідомити наслідки розміщення постів онлайн.
- Перегляньте два-три сайти соціальних мереж під час уроку й попросіть учнів указати на ризиковану поведінку, якщо вони таку помітили. Обговоріть, що саме становить ризик для користувачів. Тепер попросіть своїх учнів переглянути власну онлайн-діяльність з урахуванням моментів, на які вони щойно вказали.
- Поділіть учнів на групи, які мають створити власні контрольні списки речей, які слід ураховувати, коли вони публікують матеріали онлайн на сайті соціальної мережі. Порівняйте списки та об'єднайте їх, щоб скласти єдиний контрольний список для всього класу, який учні можуть роздрукувати та взяти додому, щоб розмістити на стіні біля свого комп'ютера.
- Попросіть учнів принести цифрові фотографії, які вони хотіли б завантажити на сайт соціальної мережі. Працюючи в невеликих групах, проаналізуйте кожну фотографію, щоб побачити, яку приватну інформацію вона розкриває. Оцініть рівень безпеки кожної фотографії за шкалою від 1 до 5, присвоївши 5 будь-якій фотографії, яка ідеально захищає приватність користувача.
- Див. подальші пропозиції щодо використання цих технологій соціальних мереж у класі в розділі про Web 2.0, 3.0 та далі (Інформаційний матеріал 3).
- Підготуйте відповідний матеріал для своїх дітей чи учнів, щоб розпочати обговорення того, що таке екстремістський контент і як він може вплинути на поведінку. Попрацюйте з ними, щоб згенерувати ідеї щодо протидії екстремізму. План дій Ради Європи проти насильницького екстремізму та радикалізації буде корисним для інформування учнів та запуску процесу появи ідей[6].
- Перегляньте разом із учнями Загальний регламент про захист даних та обговоріть, чому Європейський Союз хоче обмежити доступ до соціальних мереж для дітей, які не досягли певного віку[7]. Яким має бути цей вік?

6. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3576
7. http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf

НАЛЕЖНА ПРАКТИКА

- Довіряйте своїй інтуїції – якщо щось виглядає або відчувається «неправильним», це, мабуть, так і є! Якщо ви виявили онлайн щось, що вам не подобається або викликає почуття дискомфорту, вимкніть комп'ютер і поговоріть про це з другом, якому довіряєте.
- Будьте обережні з особистою інформацією. Проблема полягає в тому, що як тільки людина розміщує особисту інформацію в Інтернеті, вона втрачає контроль над тим, хто її побачить і як вона буде використана. Зображення можна легко скопіювати та поділитися ними з тисячами людей, просто натиснувши кнопку. Через цифровий характер фотографій їх можна навіть змінити або спотворити. Вони також можуть використовуватися новими пошуковими програмами для ідентифікації людей, навіть якщо зображення не прив'язане до імені. Нам усім потрібно навчитися розміщувати лише ті фотографії, які ми були б раді показати всім, включаючи батьків та вчителів.
- Онлайн не всі є тими, ким видаються. Те, що певні вебсайти стверджують, що вони пов'язують учнів тієї самої школи, нічого не означає. Інформація, надана користувачами під час реєстрації, не перевіряється. Будь-хто може створити профіль користувача, видаючи себе за іншого. Тим паче, кожен може долучитися до будь-якої кількості шкільних спільнот незалежно від свого реального чи удаваного віку.
- Не дозволяйте своєму захопленню виходити за рамки розумного – якщо соціальні мережі стали для вас нав'язливою ідеєю, і ви не можете жити без перевірки/оновлення свого профілю, розміщення фотографій та підрахунку лайків, то, можливо, вам варто взяти «відпустку від соціальних мереж» або принаймні обмежити час, який ви проводите на цих сайтах.
- Ознайомтеся з матеріалами, що надаються більшістю провайдерів соціальних мереж і містять рекомендації щодо безпечного користування їхніми сайтами.
- Уважно переглянте матеріал, який ви розміщуєте онлайн – пам'ятайте, що, розмістивши щось, ви ніколи не зможете повністю видалити це з Інтернету.
- Будьте особливо обережні, розміщуючи зображення. Навіть якщо ви не розмістите своє ім'я поруч із зображенням, вас усе одно можна за ним ідентифікувати, і воно може залишатися доступним у вебкешах ще довго після того, як ви його видалите.
- Захищайте свою особисту інформацію, особливо інформацію, за якою вас можна ідентифікувати або встановити ваше місцезнаходження.
- Ніколи не розміщуйте нічого, що може ображати інших людей, висловлювати зневагу до них або принижувати їх.
- Пам'ятайте, що ваш профіль можна налаштувати як загальнодоступний або приватний. Слід ретельно продумати, яке налаштування підходить вам найкраще.
- Скористайтеся функціями конфіденційності, які пропонуються сайтами соціальних мереж. Добре подумайте, перш ніж відкривати свій профіль для загального перегляду.
- Пам'ятайте, що якщо ваш профіль налаштовано як загальнодоступний, його може побачити кожен. Навіть якщо він не є загальнодоступним, його можуть бачити усі в мережах, учасником яких ви є. Варто перевіряти свої налаштування час від часу, оскільки сайти соціальних мереж можуть змінити свою політику.
- Якщо у вас виникають такі проблеми, як кампанії ненависті, цькування чи цілеспрямовані повідомлення расистського, ксенофобського, гомофобського чи іншого екстремістського змісту, завжди звертайтеся за допомогою до когось, кому ви довіряєте, навіть якщо ви думаєте, що ця людина може не зрозуміти чи не схвалити ваші дії.
- Ніколи не роздавайте свої контактні дані у своєму профілі.
- Пам'ятайте, що контент, який ви розміщуєте онлайн, може бути використаний з низкою цілей, включаючи персоналізовану рекламу, і навіть з метою підвищення шансів на працевлаштування чи з політичною метою.
- Перевіряйте свої налаштування, отримуючи доступ до сайтів соціальних мереж з різних пристроїв, оскільки вони можуть запитати дозволу на доступ до вашої інформації зі смартфона, планшета чи комп'ютера.

ДОДАТКОВА ІНФОРМАЦІЯ

- Більше інформації про соціальні мережі можна отримати з доповіді «21 найважливіший сайт та застосунок соціальних мереж у 2015 році» [The world's 21 most important social media sites and apps in 2015]: <*http://web.archive.org/web/20160423200413/http://www.socialmediatoday.com/social-networks/2015-04-13/worlds-21-most-important-social-media-sites-and-apps-2015>.*
- Поради щодо безпечної участі в соціальних мережах можна отримати за адресою: *<http://web.archive.org/web/20120602054510/, http://www.getsafeonline.org/nqcontent.cfm?a_id=1459>.*
- Інформацію на різноманітні теми, пов'язані з користуванням сайтами соціальних мереж, та поради щодо збереження безпеки можна знайти за адресою: *<www.privacyrights.org/social-networking-privacy>.*
- Доповідь Дослідницької мережі соціальних наук (Social Science Research Network) про використання підлітками соціальних мереж доступна за адресою: *<http:// web.archive.org/web/20160703112245/http://papers.ssrn.com/sol3/papers.cfm?abstract_ id=1925128>*.
- Дослідницький центр П'ю (Pew Research Center) опублікував огляд матеріалів про підлітків, інформаційні технології та дружбу за адресою: *<http://web.archive.org/web/20160710143035/http://www.pewinternet.org/2015/08/06/teens-technology-and-friendships/>*.
- Відповідні документи Ради Європи: Рекомендація CM/Rec(2012)4 Комітету Міністрів державам-членам щодо захисту прав людини під час користування послугами соціальних мереж: *<https://wcd.coe.int/ViewDoc.jsp?id=1929453>*.

Інформаційний матеріал 9

Конфіденційність і налаштування конфіденційності

Конфіденційність означає ступінь контролю, який має особа щодо доступу до своєї особистої інформації та використання такої інформації. Більшість користувачів електронної пошти та Інтернету припускають, що особиста інформація не використовуватиметься без дозволу, а обмін інформацією є конфіденційним та безпечним. Однак реальна ситуація є зовсім іншою.

Щоразу, коли ви заходите на вебсайт, публікуєте контент у соціальних мережах або надсилаєте електронного листа, ви залишаєте інформацію про себе, яка може включати вашу фізичну та комп'ютерну адресу, номери телефонів і кредитних карток, дані про споживчі вподобання та багато іншого.

Слід також пам'ятати, що як тільки ваші дані з'являться в мережі, у вас можуть виникнути труднощі зі збереженням контролю над ними, і це може мати довгострокові наслідки.

Оскільки електронна комерція, включаючи онлайн-покупки та рекламу, стає прийнятним для багатьох способом ведення бізнесу, слід приділяти особливу увагу захисту закритих даних, каналів зв'язку та уподобань.

Не можна допускати створення довготермінових або постійних копій створеного дітьми контенту в Інтернеті, якщо це ставить під загрозу їх гідність, безпеку та конфіденційність або робить їх

вразливими зараз або на більш пізньому етапі їх життя (Декларація Комітету міністрів про захист гідності, безпеки та конфіденційності дітей в Інтернеті, ухвалена 20 лютого 2008)[1].

Конфіденційність тісно пов'язана з безпекою; обов'язково уважно прочитайте Інформаційний матеріал 19 з питань безпеки.

КОНФІДЕНЦІЙНІСТЬ

- Конфіденційність в Інтернеті (або онлайн) – це широкий термін, який стосується різноманітних факторів, методів і технологій, що використовуються для захисту закритих і конфіденційних даних, каналів зв'язку та уподобань[2].
- Питання про конфіденційність в Інтернеті постає щоразу, коли користувач виходить онлайн через комп'ютер, планшет, смартфон, ігрову консоль або інший пристрій із підтримкою Wi-Fi.
- Конфіденційність в Інтернеті стосується не лише того, як ви зберігаєте свої дані конфіденційними онлайн, а й ступеня доступності вашої інформації для хакерів.
- Загальний регламент про захист даних (ЗРЗД) надає користувачам більше контролю над своїми даними та підвищує рівень конфіденційності онлайн. Ключові міркування щодо ЗРЗД включають:
  - нове визначення згоди користувача – згода більше не може розглядатися як така, що надана вільно, якщо користувачі повинні дати згоду на обробку більшої кількості даних, ніж це необхідно для надання цієї послуги;
  - краща прозорість інформування користувачів про те, як обробляються їхні дані, яка досягається за допомогою піктограм/іконок та «простої мови» – це дозволить користувачам краще порівнювати сервіси та вибирати такі, що більше поважають конфіденційність;
  - право користувачів на переносимість даних, що означає, що вони зможуть отримувати свої дані у придатному для використання форматі від сервісів, якими користуються – користувацький контроль за своїми даними та принцип володіння даними значно посилюється цим положенням;
  - посилений захист для дітей – будь-яка дитина у віці від 13 (мінімум) до 16 (максимум) років отримає додатковий захист, такий як вимога дозволу батьків на обробку даних та захист від обробки даних для рекламних цілей;
  - вищі штрафи (до 4% від обороту компанії) у разі порушення цих правил.
- Якщо пароль зламано й розкрито, наслідки цього можуть бути дуже серйозними – від викрадення персональних даних до незаконних онлайн-транзакцій тощо.

Налаштування конфіденційності

Налаштування конфіденційності – це елементи управління, які дозволяють користувачам обмежувати, хто може отримати доступ до їхньої інформації та скільки інформації можуть бачити інші.

Налаштування конфіденційності в більшості соціальних мереж спочатку встановлюються за замовчуванням; зазвичай ви можете налаштувати їх відповідно до власних вимог і повинні переві ряти їх щоразу, коли платформа соціальної мережі повідомляє, що вона пройшла оновлення.

Налаштування конфіденційності слід перевіряти регулярно, і притому на всіх пристроях із підтримкою Wi-Fi. Не забувайте перевіряти також і налаштування геолокації, оскільки координати вашого місцезнаходження/розташування вашого пристрою є важливими аспектами вашої конфіденційності (див. Інформаційний матеріал 5 про мобільні технології).

Геолокалізація

Геолокація[3] – це визначення місцезнаходження об'єкта, наприклад, радара, мобільного телефона або підключеного до Інтернету комп'ютера.

Геолокалізація – це процес визначення місцезнаходження об'єкта. Застосунки для геолокації повідомляють користувачам про ваше місцезнаходження, і вони також можуть визначити відстань

1. https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2820.02.2008%29&Language=lanEnglish&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIn- tranet=FFBB55&BackColorLogged=FFAC75
2. http://web.archive.org/web/20160703014430/https://www.techopedia.com/definition/24954/internet-privacy
3. https://en.wikipedia.org/wiki/Geolocation

до реальних місць у порівнянні з вашим місцезнаходженням. Застосунки для геолокації дозволили створити нові бізнес-моделі для послуг та товарів.

Геолокація може загрожувати вашій конфіденційності, оскільки вона вказує, де ви перебуваєте, а геолокація дитини може становити ще й загрозу для її безпеки.

Кукі-файли

Кукі-файл[4] – це текстовий файл, який залишається на вашому комп'ютері після відвідування вебсайту. Він не може завдати шкоди вашому комп'ютеру, але надасть доступ до інформації про вашу поведінку та інтереси. Це може створити більш персоналізовану атмосферу для вебсерфінгу. Наприклад, під час реєстрації на вебсайті вас можуть назвати на ім'я при поверненні.

Важливо вирішити, наскільки конфіденційною ви хочете лишити свою онлайн-поведінку. Оскільки кукі-файли можна використовувати для відстеження моделей користування Інтернетом та контактної інформації, вони створюють можливість посягання на вашу конфіденційність. Вони також полегшують поведінкове націлювання реклами[5].

Ви можете використовувати антишпигунські програми[6], щоб допомогти контролювати дані, які поширює ваша система, і видалити небажані кукі-файли.

У наші дні всі вебсайти, що є власністю резидентів ЄС або орієнтовані на громадян ЄС, повинні відповідати вимогам Закону про кукі-файли (Директива ЄС 2009/136/ЄС). Це дає людям право відмовитись від використання кукі-файлів, які обмежують їхню онлайн-конфіденційність.

Захист даних

Захист персональних даних регулюється Конвенцією Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних.

Ви маєте право знати, які дані певна компанія має про вас. У вас повинна також бути можливість змінити їх, якщо вони не відповідають дійсності, а на використання цих даних має вимагатися ваша згода.

Указівки щодо захисту ваших даних найкраще викладено в Загальному регламенті про захист даних[7].

Уважно прочитайте застереження на всіх вебсайтах та в застосунках, де вас просять надати конфіденційну інформацію[8]. Це юридична угода між вами та контролером даних[9], яка повинна містити детальну інформацію про те, де і як довго зберігаються ваші дані та як їх видалити.

Переконайтесь, що ваш електронний пристрій та програми електронної пошти захищені паролем[10]. Коли ви дістаєте новий пристрій чи програмне забезпечення або реєструєтесь у інтернет-провайдера, для вас, найімовірніше, будуть установлені налаштування користувача та пароль за замовчуванням[11]. Обов'язково швидко змініть такі налаштування за замовчуванням на більш безпечні пароль та ідентифікатор.

Найкраще буде зашифрувати[12] будь-яку закриту інформацію, яка надсилається через Інтернет. На щастя, це є стандартною процедурою для більшості транзакцій електронної комерції[13], але перед передачею даних кредитної картки або номерів банківських рахунків все одно слід переконатися, що сторінка захищена.

Різні частини вашого комп'ютера можна захистити за допомогою паролів. Створюйте паролі для папок, що містять цінні документи, наприклад, конфіденційні проєкти, дослідження, оригінальні конструкції тощо.

Право на забуття

Право на забуття є важливим елементом будь-якої дискусії про конфіденційність, оскільки це право дозволяє людям відновити свою конфіденційність.

4. https://en.wikipedia.org/wiki/HTTP_cookie
5. https://en.wikipedia.org/wiki/Behavioral_targeting
6. https://en.wikipedia.org/wiki/Spyware
7. http://ec.europe.eu/justice/data-protection/reform/index_en.htm
8. https://en.wikipedia.org/wiki/Disclaimer
9. https://goo.gl/XEkvjh
10. https://en.wikipedia.org/wiki/Password
11. http://www.netlingo.com/right.cfm?term=default
12. http://en.wikipedia.org/wiki/Encryption
13. http://en.wikipedia.org/wiki/Ecommerce

В Європейському Союзі людина може вимагати від пошукової системи видалити певні результати зі свого списку результатів, які не з'являться, коли хтось шукатиме ім'я цієї людини. Але є обмеження, і цей захід завжди потрібно буде узгоджувати з основними правами інших людей, такими як свобода вираження поглядів. У будь-якому випадку, ця інформація все одно буде доступна на вебсайті, де вона знаходиться; це лише ускладнить пошук.

Щоб скористатися правом на забуття та вимагати видалення результатів із пошукової системи, потрібно заповнити форму через вебсайт пошукової системи[14].

Але пам'ятайте, краще взагалі не розміщувати конфіденційну інформацію, оскільки коли вона вже є в Інтернеті, майже неможливо повністю її видалити.

Важливість розмов про конфіденційність у класі або вдома

Технічні та соціальні аспекти конфіденційності та ризики саморозкриття є цінними темами для навчальних занять. Технічні аспекти можуть бути включені до програми занять із інформаційних технологій (ІТ), але вони повинні входити однаковою мірою також і до навчальної програми курсу життєвих навичок.

Важливим елементом освіти щодо конфіденційності має бути поняття про «профілювання» та пов'язування між собою розрізнених елементів інформації про людину для отримання більш детальної картини. Важливим наслідком цього для освіти є те, що набагато більше інформації про нас можна знайти, «склавши два і два разом». Наприклад, «анонімний» профіль соціальної мережі (який ховається за псевдонімом) може бути ототожнений із вашим справжнім ім'ям шляхом зіставлення фотографій, присутніх у анонімному профілі та повному профілі на іншому сайті.

Думка про те, що конфіденційність порушується лише розголошенням класичної особистої інформації, потребує ретельного перегляду. Нові маркетингові прийоми, які розрізняють людей на основі їх поведінкових рис (а саме поведінкове таргетування), також можуть розглядатися як такі, що порушують конфіденційність.

Конфіденційність дедалі більше підривається швидкістю та легкістю, з якою діти та молодь можуть публікувати та/або передавати цифрові зображення в Інтернет через вебзастосунки та за допомогою камери й засобів обміну мультимедіа-повідомленнями на мобільних телефонах. Просте правило: ніколи не публікуйте того, чого не повинні побачити ваші вчителі чи батьки.

Кожна людина повинна мати навички, необхідні для безпечної роботи в Інтернеті, і це включає знання про самозахист, ефективне спілкування та відповідальність перед іншими.

Ця тема природно пов'язана з громадянським вихованням як частиною будь-якої навчальної програми. Проблеми онлайн-конфіденційності точно віддзеркалюють соціальні проблеми, які є пріоритетними для більшості культур у наш час. Дослідження мотивацій хакерів[15], зломників та активістів у галузі конфіденційності пропонують широкі можливості для обговорення цінності демократичних принципів.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Онлайн-конфіденційність є однією з найскладніших етичних та правових тем, які стосуються Інтернету.
- Кожна людина має право на конфіденційність і повинна бути захищена від зловмисних намірів.
- Ризики для конфіденційності в Інтернеті включають фішинг (злом через Інтернет із метою викрадення захищених даних користувачів); фармінг (злом через Інтернет для перенаправлення відвідувача справжнього вебсайту на іншу IP-адресу); шпигунські програми (офлайн-застосунки, які отримують дані без згоди користувача); шкідливі програми (застосунки, що використовуються для незаконного завдання шкоди користувачам онлайн та офлайн через троянські програми, віруси та шпигунські програми)[16].
- Секстинг, тобто акт надсилання відвертого контенту чи контенту, який натякає на секс, у тому числі зображень (часто селфі), повідомлень і відео через телефон, комп'ютер, вебкамеру чи інший пристрій, або створення сексуальних дописів онлайн має серйозні наслідки не лише з юридичної точки зору, а й у плані репутаційних ризиків для причетної особи, оскільки повідомлення, зображення або відео можуть розміщуватися на сайтах соціальних мереж або використовуватися на порнографічних вебсайтах та у відповідних відео.

14. https://en.wikipedia.org/wiki/Right_to_be_forgotten
15. http://en.wikipedia.org/wiki/Hacker
16. http://web.archive.org/web/20160703014430/https://www.techopedia.com/definition/24954/internet-privacy

- Ми несемо відповідальність за всі рішення, які ухвалюємо щодо власних та чужих прав, наприклад, авторських прав[17] та інтелектуальної власності[18].
- Свобода слова є правом, однак на практиці це сіра зона без простих відповідей. Що є прийнятним і неприйнятним? Як проводити в життя правила, не зазіхаючи на права мовця?

ЯК ЦЕ РОБИТИ

Використання налаштувань конфіденційності на всьому обладнанні з підтримкою Wi-Fi та доступом до Інтернету є одним із найкращих способів захистити вашу конфіденційність.

Залежно від вашого браузера, швидко проведіть пошук у налаштуваннях конфіденційності, щоб побачити, як ви можете:

- блокувати рекламу та відстеження;
- блокувати сторонні кукі-файли;
- блокувати доступ до свого місцезнаходження для вебсайтів.

Не забувайте встановлювати налаштування конфіденційності на смартфонах, планшетах та ігрових консолях. Камери найновіших моделей мають налаштування геолокації, які також слід перевіряти.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Доручіть учням пошукати в Google власні імена. Обов'язково слід виконати пошук і серед зображень та відео. Попросіть їх створити сповіщення Google на власні імена, щоб вони дізналися, коли їх імена буде розміщено онлайн.
- Працюючи разом із класом, створіть базу основних знань щодо конфіденційності. Визначте поняття, як технічні, так і соціальні, та виділіть забобони й міфи для обговорення. Уже сама постановка запитань «Що таке конфіденційність?» та «Чи необхідна конфіденційність?» повинна спонукати людей до висловлювання твердих поглядів.
- Шукайте в Інтернеті сайти з питань конфіденційності та використовуйте програми контролю проходження сигналу[19] для пошуку фізичних адрес цих сайтів, щоб продемонструвати різноманітні геофізичні проблеми, що впливають на дотримання законності в Інтернеті. Дослідіть інші проблеми (культурні, політичні та історичні), які вийшли на поверхню завдяки результатам контролю проходження сигналу. Наприклад, виберіть сайт пересилання листів[20] або анонімний проксі-сервіс, запустіть контроль проходження сигналу, а потім пошукайте причини, з яких ці сервіси розташовані в цих країнах.
- Рольова гра на тему захисту даних та конфіденційності Play-Decide[21] пропонує цікавий спосіб вивчити наслідки реалізації законодавства про конфіденційність, авторське право та свободу слова й інформації, які мають місце одночасно в різних державах або для різних вікових та культурних груп.
- Навчіть учнів створювати надійні паролі[22].

НАЛЕЖНА ПРАКТИКА

- Два золотих правила:
  - не діліться своєю особистою інформацією з людиною, яку ви не знаєте і якій не довіряєте;
  - не використовуйте особисту інформацію чи фотографію іншої особи без її згоди.

17. http://en.wikipedia.org/wiki/Copyright
18. http://en.wikipedia.org/wiki/Intellectual_property
19. http://en.wikipedia.org/wiki/Traceroute
20. http://en.wikipedia.org/wiki/Remailer
21. http://paneuyouth.eu/files/2013/06/PD-kit-privacy-and-data-protection.pdf
22. http://en.wikipedia.org/wiki/Password#Factors_in_the_security_of_an_individual_password

- Створіть резервну копію[23] вашої системи та регулярно виконуйте резервне копіювання.
- Оновіть заходи безпеки у вашій системі та проведіть за адресою: *<http://www.epic.org/privacy/tools.html>* дослідження додаткових інструментів, які забезпечуватимуть дотримання ваших онлайн-уподобань.
- Абсолютно необхідно встановити антивірус[24] та брандмауер[25]. Варто розглянути й інші інструменти, наприклад, блокувальники спливаючих вікон[26] та антишпигунські програми[27]. Обов'язково регулярно перевіряйте свою систему.
- Використовуйте «надійні паролі»[28] для захисту свого ПК, електронної пошти та з'єднань із Інтернетом. Надійні паролі складаються з літер, цифр і спеціальних символів.
- Перш ніж видавати приватні дані, перевірте наявність знаку закритого замка, який відображається на панелі інструментів. Це знак того, що ваша транзакція відбувається через безпечне з'єднання. Перед здійсненням онлайн-транзакцій переконайтесь, що URL-адреса містить HTTPS; літера S означає «захищений» у протоколі передачі гіпертекстових даних (HTTP) і автентифікує вебсайт та пов'язаний вебсервер, який захищає його від сторонніх атак.
- Уникайте онлайн-покупок на ненадійних вебсайтах та розкриття персональних даних на вебсайтах із нижчим рівнем безпеки.
- Обов'язково перевірте свої права; ви можете бути більш захищеними, ніж ви думаєте. Користувачі завжди є найслабшою ланкою у сфері конфіденційності та захисту даних.

ДОДАТКОВА ІНФОРМАЦІЯ

- Щоб прочитати більше про Закон щодо кукі-файлів та Директиву ЄС, див.:*<http://www.cookielaw.org/the-cookie-law/>*.
- Існує Інформаційний матеріал Єврокомісії про право на забуття: *<http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>*.
- Існує також Інформаційний матеріал Єврокомісії про захист даних: *<http://ec.europa.eu/justice/data-protection/fiactsheets/factsheet_data_protection_eurobarometer_240615_en.pdf>* та інша інформація про пов'язані з цим реформи *<http://ec.europe.eu/justice/data-protection/ reform/index_en.htm>.*
- Інформаційний центр із електронної конфіденційності (ІЦЕК) веде реєстр інструментів та статей щодо конфіденційності: *<http://www.epic.org/privacy/tools.html>*.
- Дізнайтеся за допомогою BrowserSpy, що ваш ПК повідомляє кожному зацікавленому учасникові мережі: *<http://gemal.dk/browserspy/>*.
- Турбуєтеся про свої громадянські свободи? Ці обговорення щодо конфіденційності можуть на деякий час забезпечити темами ваші заняття з громадянського виховання. Фонд електронного фронтиру за адресою: *<http://www.eff.org/>*, Epic.org за адресою: *< http://www.epic.org>*, Privacy International за адресою: *<http://www.privacyinternational.org/>* і Privacy.net за адресою: *<http://www.privacy.net/>*.
- TuCows за адресою: *<http://www.tucows.com/>*, є вебсайтом, який надає доступ до понад 40 000 умовно безкоштовних та безкоштовних програм. Він обіцяє швидке, локальне та безпечне завантаження продуктів, вільних від вірусів та шпигунських програм.
- Zone Alarm за адресою: *<http://www.zonelabs.com/store/content/home.jsp>* є однією з найвідоміших брандмауерних програм. Вона дозволяє вам установити контроль доступу для різних програм, які надсилають інформацію через Інтернет.
- CryptoHeaven – це пакет шифрування, який пропонує захищену пошту, обмін файлами та чат із симетричним та асиметричним шифруванням: *<http://www.cryptoheaven.com/>*.

23. http://en.wikipedia.org/wiki/Back_up
24. http://en.wikipedia.org/wiki/Antivirus
25. http://en.wikipedia.org/wiki/Firewall_%28networking%29
26. http://en.wikipedia.org/wiki/Pop_up#Add-on_programs_that_block_pop-up_ads
27. http://en.wikipedia.org/wiki/Spyware
28. http://en.wikipedia.org/wiki/Password#Factors_in_the_security_of_an_individual_password

- Довідковий центр Facebook надає інформацію про налаштування конфіденційності: *<https://www.facebook.com/help/193677450678703>.*
- Статистичні дані про те, як діти та молодь розуміють конфіденційність та налаштування конфіденційності онлайн, можна знайти за адресою: *<http://web.archive.org/web/20160703155259/https://www.techopedia.com/2/30101/internet/online-privacy/do-millenials-understand-online-privacy>*.
- Статистику про сучасне становище молоді в Європі див. за адресою: *<http://web.archive.org/web/ 20160604111543/http://ec.europa.eu/eurostat/statistics-explained/index.php/Being_young_ in_Europe_today_-_digital_world>.*
- Інформацію про європейські цифрові права див. за адресою: *<http://www.edri.org>*.
- Відповідні документи Ради Європи:
  - Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETSNo. 108): *<http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>*.
  - Декларація Комітету міністрів про захист гідності, безпеки та конфіденційності дітей в Інтернеті: *<https://wcd.coe.int/ViewDoc.jsp?id=1252427>*.
  - Сторінка Ради Європи про роботу Ради Європи у сфері конфіденційності та захисту даних: *<http://www.coe.int/en/web/internet-users-rights/privacy-and-data-protection>*, а також інформація про ваші права та обов'язки онлайн.

3. Інтернет – Беручи участь в суспільстві знань

> «Знання – сила. Інформація визволяє. Освіта є передумовою поступу в кожному суспільстві, у кожній родині».
> *Кофі Аннан, колишній Генеральний секретар ООН (січень 1997 – грудень 2006)*

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 10 – ПОШУК ІНФОРМАЦІЇ

Чи читаєте ви застереження, коли звертаєтесь до певного вебсайту?
Як ви можете бути впевнені, що інформація, яку ви знайдете, буде точною та об'єктивною? Чи звертаєтесь ви до кількох вебсайтів, щоб перевірити отримані факти?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 11 – ЯК ЗНАЙТИ ЯКІСНУ ІНФОРМАЦІЮ В МЕРЕЖІ

Перш ніж завантажувати файли, чи перевіряєте ви, що ваш антивірус запущено?
Якщо ви отримуєте свої новини з Інтернету, чи шукаєте ви кілька поглядів на один і той же сюжет?
Час від часу видаляйте свої кукі-файли, щоб уникнути «профілювання» з боку пошукових систем.

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 12 – ДИСТАНЦІЙНЕ НАВЧАННЯ ТА МАСОВІ ВІДКРИТІ ОНЛАЙН КУРСИ

Оберіть підходящий для вас метод дистанційного навчання: визначте, який саме тип навчання (синхронне, асинхронне, із відкритим графіком, гібридне дистанційне навчання) найкраще допоможе вам досягти ваших цілей.
Перш ніж обрати дистанційний навчальний курс, вивчіть відгуки як студентів, так і викладачів.
Уживайте адекватних заходів безпеки, щоб забезпечити захист свого комп'ютерного обладнання та програмного забезпечення від хакерів, вірусів та інших загроз.

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 13 – ОНЛАЙН-ПОКУПКИ

Не робіть онлайн-покупок через незахищені Інтернет-з'єднання.
Розберіться в ключовій інформації про товар чи послугу та прийміть її. Вимкніть покупки в застосунку на вашому смартфоні чи планшеті.
Не вірте всім рекомендаціям користувачів, які ви бачите, оскільки створення рекомендацій «від імені користувачів» також може бути прибутковим бізнесом.

Інформаційний матеріал 10

Пошук інформації

На самому початку існування Інтернету не існувало пошукових систем. Спробуйте уявити світ без пошукових систем. Людям доводилося шукати друковану інформацію про вебсайти у паперових документах або в журналах, а потім вводити адресу у своєму браузері. Якщо щастило, цей вебсайт мав посилання на інший вебсайт, і, клікаючи на посилання одне за одним, вони могли «досліджувати» Всесвітню павутину. Поступово створювались інтернет-портали або каталоги[1], які трохи нагадували телефонну книгу: величезний перелік вебсайтів, відсортованих за категоріями.

Деякі з цих каталогів чи порталів досі існують, наприклад, Yahoo! та MSN. Інші форми порталів включають:

- портали з «офіційним» контентом (вебсайт ООН або вебсайт Ради Європи);
- портали, що спеціалізуються на конкретному контенті або послугах (Booking.com для готелів або Amazon.com для покупок);

1. https://en.wikipedia.org/wiki/Web_portal

- портали, засновані на створеному користувачами контенті, який може бути дуже різноманітним – соціальні мережі (Facebook) також можна розглядати як різновид порталів.

Потім були створені пошукові системи, які революціонізували спосіб пошуку контенту в Інтернеті. Але як ці системи працюють? Сьогодні пошукові системи спираються у своїй роботі на пошукових роботів[2] та дуже складні алгоритми, які аналізують, класифікують контент у індексах[3] і вирішують, які вебсайти слід вибрати з цих індексів залежно від ключових слів, які ви використовуєте у своєму пошуку.

Характер налаштування алгоритму надзвичайно важливий, оскільки більшість людей зупиняються на перших кількох сторінках результатів пошуку. На сьогодні Google є найпопулярнішою пошуковою системою, і вона стала популярною завдяки своєму алгоритму, який використовував оригінальний метод ранжування важливості вебсайту за кількістю зворотних посилань[4]. Це в принципі означає кількість зовнішніх вебсайтів, які містять посилання на ваш вебсайт. Наприклад, якщо на вебсайт wikipedia.org посилається велика кількість інших вебсайтів, він отримує вищий ранг.

Але алгоритми постійно вдосконалюються для підвищення точності. Наприклад, Google планує додати елемент, який розраховує «достовірність» вебсайтів на основі порівняння їх контенту з фактами, що зберігаються в сховищі знань Google. Ба більше, алгоритми також можна налаштувати для комерційних цілей, як буде показано нижче.

Перегляньте запропоноване Google анімаційне пояснення того, як працює його пошукова система: *<https://www.google.com/insidesearch/howsearchworks/thestory/>*.

ОСВІТНЯ ЦІННІСТЬ: ЧОМУ ЦЕ АКТУАЛЬНО Й ВАЖЛИВО?

Навчитися правильно користуватися пошуковою системою – це, можливо, найважливіша навичка, яку слід розвивати не лише для відповідального серфінгу в Інтернеті, але й для набуття пов'язаних із нею навичок, наприклад, критичне мислення (шляхом пошуку та порівняння різних джерел онлайн). Як тільки ви зрозумієте, як користуватися пошуковою системою, це може допомогти вам знайти якісну інформацію для розвитку тисячі інших навичок або отримати поглиблені знання на будь-яку тему, в тому числі й про відповідальну поведінку в Інтернеті!

Наприклад, ви можете розвинути свої навички використання цифрових технологій, шукаючи рішення проблем, які виникають у вас із пристроями, або просто задовольняючи свою цікавість щодо того, як вони працюють. Знайти цей посібник з інтернет-грамотності, саме той, який ви зараз читаєте, можна саме завдяки використанню пошукової системи.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Деякі портали можуть вимагати членства або реєстрації, і це може бути платним сервісом. Перш ніж реєструватися (навіть на «безкоштовних» сервісах), переконайтеся, що ви розумієте умови надання послуг та що ви переглянули та зрозуміли політику конфіденційності вебсайту (див. ***<http://www.netlingo.com/right.cfm?term=privacy%20policy>***).
- Вебсайти використовують різноманітні засоби, включаючи платежі на користь пошукових систем, для підвищення свого рангу в результатах пошуку. Деякі пошукові системи, такі як Google, чітко вказують, які результати є платними оголошеннями. Багато інших не здійснюють такого розрізнення.
- Самі алгоритми ніколи не є нейтральними, піддаються суперечкам та зазнають критики[5]. Наприклад, відомо, що Google підвищував видимість власних сервісів, наприклад, Google Shopping, Google+ або YouTube, на шкоду своїм конкурентам (Amazon, Facebook, Dailymotion тощо). Пошуковими системами також можна маніпулювати з політичних причин. За загальним правилом, ніколи не вірте, що результат пошуку відповідає «істині» лише тому, що він має вищий ранг, або що вебсайти з нижчим рангом є «неважливими» або «малозначимими».

2. https://en.wikipedia.org/wiki/Web_crawler
3. https://en.wikipedia.org/wiki/Web_indexing
4. https://en.wikipedia.org/wiki/Backlink
5. https://en.wikipedia.org/wiki/Criticism_of_Google

- Ось чому важливо мати кілька каналів доступу та пошукових систем, здатних здійснювати пошук в мережі, щоб отримувати більш різноманітні результати та підтримувати здорову конкуренцію, яка може сприяти більшій точності та нейтральності пошуку. Як користувач, ви відіграєте важливу роль у формуванні онлайн-середовища: не забувайте використовувати інші пошукові системи:Yahoo!, Bing, Qwant, IXquick або DuckDuckGo. Використовуючи менш відомі пошукові системи, ви сприяєте їхньому подальшому існуванню і тим самим забезпечуєте збереження різноманітності[6].
- Майте на увазі, що ваша геолокація[7] та кукі-файли з попередніх пошукових запитів вплинуть на ваші результати пошуку. Незважаючи на те, що збирання пошуковою системою даних про вашу геолокацію є неминучим[8], періодичне видалення кукі-файлів (див. Інформаційний матеріал 9 про конфіденційність та захист конфіденційності) та (меншою мірою) історії перегляду зменшить кількість таргетованої реклами, пов'язаної з вашими останніми пошуковими запитами (наприклад, про місце призначення вашої подорожі). Це також допоможе вам забезпечити себе достатнім обсягом інформації з важливих соціальних та політичних питань, яка б не обмежувалася тим, що пошукова система вважає вашими поглядами[9]. Ви також можете повністю відключити кукі-файли, переглянувши свої налаштування в інтернет-браузері; однак пам'ятайте, що деякі вебсайти можуть після цього працювати неправильно.
- Нарешті, майте на увазі, що результати, які ви отримаєте під час пошуку, будуть залежати від того, що ви шукаєте. Наприклад, якщо ви шукаєте контент, пов'язаний із насильством, саме це ви швидше за все й знайдете, але такий контент може бути занадто жорстоким для вас. Формування стійкості до шокуючого або тривожного контенту триває все життя, тому не поспішайте, робіть це покроково.

ЯК ЦЕ РОБИТИ

Оскільки пошукові системи є найважливішими каналами доступу до інформації, важливо глибоко розуміти, як вони працюють. Самообмеження першою сторінкою результатів пошуку може дати вам надзвичайно обмежене бачення того, що важливо, а що ні. Найважливіші розширені функції пошуку, про які слід пам'ятати:

- Лапки: це, мабуть, одна з найкорисніших і найвідоміших функцій розширеного пошуку. Якщо ви хочете зробити так, щоб пошукова система напевно шукала саме потрібне вам словосполучення, ставте навколо нього лапки. Це може бути корисно, якщо ви хочете знайти конкретну фразу або словосполучення.
- Знак мінус «-»: він призначений для того випадку, коли ви щось шукаєте, але хочете виключити з результатів певний термін. Наприклад, якщо ви шукаєте «сутінки», всі перші результати будуть присвячені серіалу. Але якщо ви шукатимете «сутінки – вампір», ви отримаєте визначення слова «сутінки». Отже, знак мінус дуже корисний, коли якесь слово занадто часто асоціюється з чимось іншим, і ви хочете переконатися, що ці два значення не змішуються у вашому пошуку.
- Параметри запиту: ви можете додати певний параметр до пошуку, використовуючи певні ключові слова. Наприклад, якщо ви введете «define: птах», система буде шукати визначення поняття «птах» замість того, щоб шукати взагалі це слово. Якщо ви введете «site: wikipedia.org яблуко», Google буде здійснювати пошук лише на вебсайті Wikipedia. Це дуже корисно під час пошуку на порталах, як буде показано нижче. Існує багато інших параметрів запиту, тож перевірте їх за посиланням нижче.
- Спеціалізовані пошуки: більшість пошукових систем, включаючи IXquick, Qwant, DuckDuckGo, Google, Yahoo! та Bing, пропонують параметри спеціалізованого пошуку, наприклад, пошук мультимедійного контенту (зображень, відео тощо), наукових праць, книг, карт тощо. Ознайомтесь із цими можливостями спеціалізованого пошуку, оскільки вони оснащені власними розширеними параметрами. Наприклад, ви можете фільтрувати зображення за розміром, кольором, типом файлу і навіть характером авторського права та типом ліцензії.
- Інструменти пошуку: «інструменти пошуку», які стають доступними безпосередньо під рядком пошуку, як тільки ви здійснили пошук, також є надзвичайно корисними. Можна відсіяти результати за країною та часом. Це дуже корисно, наприклад, якщо ви шукаєте новини, оскільки ви можете обмежити пошук найновішими новинами або новинами, опублікованими рівно рік тому.

6. https://en.wikipedia.org/wiki/Web_search_engine
7. http://www.advancedwebranking.com/blog/geo-location/
8. http://www.allaboutcookies.org/cookies/cookie-profiling.html
9. http://www.pcadvisor.co.uk/how-to/internet/how-delete-cookies-web-browsing-history-3218163/

- Розширений пошук: параметр «розширений пошук» можна знайти, натиснувши на верхню праву кнопку «параметри». Розширений пошук надає всі перераховані вище функції пошуку в зручному для користувача вигляді, тому, якщо вам незручно користуватися операторами або конкретними параметрами запиту, використовуйте «розширений пошук»[10].

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Визначте мету пошуку для будь-якої теми: створіть команди, які використовують різні портали/пошукові системи, а також команду, яка використовує деякі з описаних вище методів пошуку для пошуку інформації. Дозвольте командам порівнювати результати, зручність доступу та якість інформації.
- Створіть тему для дослідження, наприклад, зображення дітей у мистецтві XVIII століття, або екосистемну динаміку певного виду живих істот океану. Надайте своєму класу URL-адреси порталів[11], які ведуть до посилань, що відповідають планові уроку. Оскільки посилань буде, найімовірніше, забагато для перегляду окремими людьми, створіть команди, щоб розділити між ними посилання та охопити якомога більше з них, дозволяючи кожній команді представити свої результати. Результати команд можуть відрізнятися, таким чином дозволяючи зосередитися на конкретних шляхах подальшого вдосконалення знань учнів.
- Профілактика чи лікування: попросіть учнів знайти свої імена в пошуковій системі та побачити, скільки небажаної інформації вони знайдуть про себе. Як вони можуть запобігти загальному доступу до такої інформації, і як положення про захист даних можуть допомогти їм видалити небажаний контент?

НАЛЕЖНА ПРАКТИКА

- Зберігайте здоровий скептицизм щодо знайденого вами матеріалу. Інтернет є вільним простором, у якому люди можуть ділитися поглядами та висувати ідеї. Обов'язково оцінюйте їх критично та шукайте різні погляди й інформацію, щоб не стати розповсюджувачем міфів або жертвою неправдивих тверджень.
- Уникайте плагіату, до якого може призвести використання готових творів чи уже виконаної роботи. Наскільки це можливо, вказуйте на автора та джерело матеріалу, який ви цитуєте чи використовуєте. Це важливо, оскільки:
  - цим ви визнаєте заслуги автора й роль джерела;
  - це захищає вас від звинувачень у плагіаті;
  - це допомагає іншим скласти власне враження про достовірність матеріалу;
  - пам'ятайте про проблему авторських прав, якщо ви використовуєте матеріали, знайдені в Інтернеті (див. нижче розділ «Як це робити» та Інформаційний матеріал 14 про музику та зображення).
- Приділіть час управлінню кукі-файлами та історією перегляду/видаленню кукі-файлів й історії перегляду. Можна взагалі відключити кукі-файли для посилення конфіденційності, але майте на увазі, що деякі вебсайти можуть не працювати належним чином без них.
- Завжди пробуйте кілька пошукових термінів, методи розширеного пошуку та різні пошукові системи, щоб отримати максимальну віддачу від пошуку та знайти різноманітні джерела за своїм запитом.
- Робіть закладки корисних вебсайтів або порталів, щоб вам не довелося їх шукати знову.
- Іноді ви шукатимете щось, пов'язане з певним порталом, наприклад, офіційний документ, виданий вашим органом державної влади, визначення слова, порівняння цін на готелі чи на авіаквитки, або інформацію про покупку товару. Для всіх цих запитів ви можете використовувати комбінацію пошукових систем та відомих порталів Booking.com, Wikipedia або Amazon. Багато порталів мають власні внутрішні пошукові системи, але ви також можете використовувати зовнішню пошукову систему, обмеживши пошук у ній цим порталом. Наприклад, шукайте «готель Брюссель site:booking.com». Спробувати обидва методи є належним підходом, щоб знайти те, що ви шукаєте.

10. https://www.google.com/advanced_search?hl=en; https://en.wikipedia.org/wiki/Google_Search#Search_options
11. http://en.wikipedia.org/wiki/URL

- Якщо ви знайшли корисний матеріал, роздрукуйте його, зробіть скриншот або збережіть його. Ви можете не знайти його знову, або його можуть зняти з сайту без попередження.
- Якщо ви не можете знайти відповіді через пошукову систему, опублікуйте цей запит на відповідній дошці оголошень, дискусійному форумі чи в соціальній мережі.
- Не забувайте робити свій внесок у створення контенту онлайн. Усі відповіді, які ви шукаєте під час користування пошуковою системою, були кимось набрані та створені. Те, що ви поділитеся власними знаннями та вміннями, може колись допомогти комусь іншому (див. Інформаційний матеріал 15 про творчість).

ДОДАТКОВА ІНФОРМАЦІЯ

- Вікіпедія – це вільна енциклопедія, яка пишеться спільно користувачами з усього світу: *<http://www.wikipedia.org/>*.
- На порталі Europeana розміщено величезну кількість оцифрованого контенту, що представляє культурну спадщину Європи: *<http://www.europeana.eu/portal/>*.
- Ці європейські пошукові системи дотримуються високих стандартів захисту конфіденційності: *<https://www.qwant.com/>* і *<https://ixquick.com/>*.
- Існує також американська пошукова система з високими стандартами захисту конфіденційності: *<https://duckduckgo.com/>*.
- Наступний сайт розповідає, як шукати в пошуковій системі Google: *<https://support.google.com/websearch/answer/134479?hl=en>*.
- Поради щодо використання Bing на Microsoft у Windows 8 див. за адресою: *<http://onlinehelp.microsoft.com/en-us/bing/jj684589.aspx>*.
- Як працюють пошукові системи? Див.: *<http://web.archive.org/web/20160509142554/http://www.bbc.co.uk/guides/ztbjq6f>*.
- Відповідні статті Конвенції ООН про права дитини:
  Стаття 13 – Діти мають право одержувати і поширювати інформацію, якщо це не шкодить їм чи іншим особам.
  Стаття 16 – Діти мають право на приватність. Закон повинен захищати їх від нападок на їхній спосіб життя, їхнє чесне ім'я, їхні сім'ї та їхні домівки.
  Стаття 17 – Діти мають право отримувати достовірну інформацію із засобів масової інформації. Телебачення, радіо та газети повинні надавати інформацію, яку діти можуть зрозуміти, і не повинні просувати матеріали, які можуть завдати шкоди дітям.
- Відповідні документи Ради Європи:
  - Рекомендація CM/Rec(2012)3 Комітету Міністрів державам-членам щодо захисту прав людини під час використання пошукових систем: *<https://wcd.coe.int/ViewDoc.jsp?id=1929429&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&Back- ColorLogged=F5D383>*.
  - Рекомендація CM/Rec(2008)6 Комітету Міністрів державам-членам про заходи щодо сприяння додержання свободи вираження поглядів та інформації у зв'язку з Інтернет-фільтрами: *<https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282008%296&Lan- guage=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFB-B55&BackColorLogged=FFAC75>*.

Інформаційний матеріал 11

Як знайти якісну інформацію в мережі

Інтернет створювався[1] для формування електронної бібліотеки, яка б дозволяла зручний доступ до інформації та її зручне розповсюдження.[2] Багато в чому цієї мети досягнуто: сьогодні Інтернет функціонує як величезна бібліотека, де присутні більшість публічних і приватних бібліотек із усього світу. Вони надають інформацію про послуги, програми та заходи, а також доступ до фізичних книг, указаних в каталогах, які можна замовити через Інтернет. Цифрові бібліотеки надають доступ до книг та колекцій онлайн, які, як правило, оцифровуються як HTML-скрипт[3], що надає їм вигляд вебсторінки[4], як документи Word або PDF[5] або як звичайний текст (ASCII)[6]. Деякі великі бібліотеки та музеї надають можливість переглядати оцифровані версії рідкісних книг та колекцій артефактів[7].

1. http://www.livinginternet.com/i/ii_summary.htm
2. http://www.livinginternet.com/i/ii_summary.htm
3. https://en.wikipedia.org/wiki/HTML
4. http://en.wikipedia.org/wiki/Html
5. http://www.census.gov/main/www/pdf.html
6. http://en.wikipedia.org/wiki/ASCII
7. http://www.bl.uk/manuscripts/Default.aspx

Інтернет також виходить далеко за рамки бібліотек у процесі надання інформації і може надати актуальну, достовірну інформацію про те, що вас цікавить: поточні події, сучасні технології, хобі, розваги, мистецтво, спорт тощо. Це доступно через широкий діапазон джерел, включаючи цілодобові канали новин[8], газети[9], журнали[10] та агрегатори новин, загальновідомі як стрічки новин або RSS-канали (збагачені зведення вебсайтів, див. <www.whatisrss.com>), і вони доступні через багато вебсайтів та платформ соціальних мереж. Користувачі підписуються на них, щоб регулярно отримувати найновіший зведений вебконтент із інтернет-газет, блогів, подкастів та відеоблогів (влогів) в одному місці для зручного перегляду.

Сьогодні багато європейців залишаються в курсі національних та міжнародних новин завдяки Інтернету й використовують його для отримання медичної інформації. Отримання новин через платформи соціальних мереж також є дедалі сильнішою тенденцією. Форуми для обговорення новин та групи новин пропонують платформи для плідних дискусій та є способом дізнатися про різні погляди на актуальні проблеми, водночас удосконалюючи дискусійні навички учнів. У світі існують сотні тисяч таких форумів, і більш активні групи щодня отримують сотні нових повідомлень. Повідомлення поділяються на гілки, які записують та відображають ім'я відправника та час надсилання повідомлення. Сьогодні більшість серверів та браузерів можуть указати вам на форуми, що цікавлять ваших учнів[11].

Twitter є ще одним засобом отримання оновленої інформації з Інтернету. Ви можете використовувати власну адресу в Twitter, щоб стежити за новинами, журналістами та експертами у сферах, які вас цікавлять, або зареєструватися в певному списку розсилки Twitter, щоб ви могли стежити за ними анонімно[12]. Сповіщення Google також можна використовувати для відстеження новин на певні теми, але якщо ключові терміни не є ретельно і чітко визначеними, ви можете отримувати настільки багато сповіщень, що це нічого не дасть. Платформи соціальних мереж поступово додають нові функції, щоб ви були в курсі також і світових новин.

ЗНАЧЕННЯ ДЛЯ ОСВІТИ

- Дослідницькі навички, необхідні для користування як традиційними, так і онлайн-бібліотеками, є подібними. Дуже важливо, щоб батьки та вчителі керували діяльністю дітей із засвоєння та відпрацювання цих навичок із перших їхніх кроків у Інтернеті.
- Існують тисячі спеціалізованих бібліотек у мережі за адресами <http://vlib.org/> та <http://www.sldirectory.com/libsf/resf/libplans.html>, які стосуються конкретних тем та сфер навчальних програм. «За своєю суттю, мережеві квести – це міні-проєкти, в яких значна частка внеску учасників та матеріалів походить із Інтернету. Мережеві квести можуть створюватися вчителями або учнями залежно від навчального заходу, обраного вчителем».[13] Модель, запропонована за адресою <http://webquest.org/>, може бути дуже корисною під час створення заходів для учасників класного заняття з використанням бібліотечних засобів в Інтернеті, і при цьому розвивається низка базових навичок:дослідження, архівування, грамотність, аналіз та оцінка.
- Групи новин та дискусійні форуми є корисним ресурсом для розвитку критичного мислення та навичок обговорення за умови, що молодих людей заохочують перевіряти використовувані ними факти шляхом звернення до кількох різних джерел. Вони також можуть надати платформу для обміну інформацією та вивчення досвіду інших людей.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Кукі-файли (невеликі файли, залишені на вашому онлайн-пристрої для зберігання інформації про вас та ваші вподобання) можуть підвищити якість перегляду вебсайтів, оскільки вони запам'ятовують ваші вподобання або дозволяють не реєструватися щоразу, коли ви відвідуєте певні вебсайти. Однак, використовуючи кукі-файли, пошукові системи вестимуть вас лише до вебсайтів, з позиціями яких ви згодні, а відтак можуть поступово звузити вашу точку зору на новини та актуальні теми.

8. http://wwitv.com/news_tv_live/
9. http://www.onlinenewspapers.com
10. http://www.e-journals.org
11. http://www.newsforum.com
12. https://en.wikipedia.org/wiki/Twitter
13. https://www.teachingenglish.org.uk/article/webquests

- Інтернет демократизував журналістику, давши людям різного віку можливість активно створювати контент. Тому пропозиція інформації в Інтернеті стає нескінченною, підкреслюючи, як ніколи раніше, важливість розрізнення між якісним та недостовірним контентом, а також між інформацією та рекламно-інформаційними повідомленнями, тобто рекламою, яка виглядає як об'єктивна інформація.
- Дуже мало груп новин або дискусійних форумів повністю модеруються, а їхніх користувачів не відстежують. Тому їх можна використовувати для незаконних дій, зокрема розповсюдження захищених авторським правом матеріалів, расистської пропаганди, екстремізму або матеріалів, які містять сцени сексуального насильства над дітьми. Використання таких платформ вимагає наявності певного почуття відповідальності та розуміння прийнятних суспільних норм, оскільки уявна анонімність може призвести до антигромадської поведінки, наприклад, розміщення образливих повідомлень, цькування та розпалювання конфліктів[14]. Слід також підводити учнів до роздумів над проблемами конфіденційності, які постають, коли вони користуються такими форумами[15].
- Більшість бібліотек надають доступ за певними правилами. Ці правила[16] вимагатимуть від користувача щонайменше дотримання норм авторських прав щодо запитуваного матеріалу. Пам'ятайте, що якщо такі матеріали не належать до загальнодоступного надбання, ви не можете розповсюджувати або публікувати їх без дозволу видавця. Дотримання авторських прав є також предметом особистої відповідальності. Плагіат – це використання чужої роботи без посилання на джерело. Обов'язково посилайтесь на джерела та прищеплюйте цю звичку учням.

ЯК ЦЕ РОБИТИ

- Usenet[17] – це всесвітня розподілена дискусійна система, що складається з набору найменованих «груп новин», які класифікуються ієрархічно за темами. Доступ до цих груп новин визначається вашим інтернет-провайдером або шкільним чи університетським сервером або сервером підприємства[18]. Доступ до деяких платформ безкоштовний, тоді як «преміум»-сервіси надаються за передплатою.
- Існує багато інструментів для створення новинної стрічки або RSS-стрічки. Відео «Організуйтесь: впорядкуйте свої новинні стрічки»[19] містить покроковий опис використання інструментів, які найкраще відповідають вашим потребам.
- Щоб налаштувати сповіщення Google, спочатку потрібно створити обліковий запис Google. Потім ви можете ввести список слів, встановити кілька інших параметрів, і сповіщення Google повідомить вас електронною поштою або в стрічці про появу цих пошукових термінів онлайн. Ви отримаєте список URL-адрес, що відображатимуть оновлення інформації щодо вашого терміну, або ви можете додати сповіщення до обраної вами програми для читання RSS-стрічок.
- Використовуючи якусь поточну тему у своєму класі, визначте відповідну бібліотеку певної категорії за адресою <http://vlib.org/>. Подумайте про створення мережевого квесту на підставі ресурсів із цієї бібліотеки або скористайтеся наявним мережевим квестом за адресою: <http://webquest.org/> та <http://www.spiritsd.ca/teacherresources/default.asp>. Мережеві квести можна знайти через пошукову систему[20]. Збагатіть свій мережевий квест, створивши сповіщення Google або приєднавшись до списку розсилки Twitter[21], і порівняйте якість інформації, яку ви отримуєте від кожного з цих джерел.
- Дорослі, діти та молодь можуть знайти якісні новинні вебсайти та заходи на багатомовній вебсторінці Міжнародної федерації бібліотечних асоціацій та установ (IFLA)[22], що базується в Шотландії. Вона пропонує широкий спектр тем від мистецтва та історії до точних наук та математики. Інші такі теми доступні на вебсайті Great websites for kids[23], розробленому підрозділом Американської бібліотечної асоціації. Додаткову інформацію про бібліотечні та інформаційні послуги також можна знайти на сайті IFLA, який вважається глобальним голосом бібліотечно-інформаційної професійної спільноти.

14. http://en.wikipedia.org/wiki/Flaming
15. http://www.webwewant.eu/information
16. http://web.archive.org/web/20160102210205/http://www.gallowglass.org/jadwiga/SCA/libraries.html#Copyright Plagiarism
17. http://en.wikipedia.org/wiki/Usenet
18. https://en.wikipedia.org/wiki/Server_(computing)
19. http://web.archive.org/web/20151231202307/http://www.pcmag.com/article2/0,2817,2458165,00.asp
20. http://en.wikipedia.org/wiki/Search_engine
21. https://media.twitter.com/best-practice/create-and-use-twitter-lists
22. http://www.ifla.org/activities-and-groups
23. http://gws.ala.org

НАЛЕЖНА ПРАКТИКА

- Перш ніж заохочувати учнів користуватися онлайн-бібліотеками, обов'язково розгляньте базові навички користувача бібліотеки та дослідницькі стратегії[24]. Також вживайте заходів, щоб вони чітко розуміли, що означає захист матеріалу авторським правом.
- Переконайтеся, що на всіх пристроях, які використовуються для завантаження файлів, стоїть антивірусний фільтр. Перш ніж завантажувати файли[25] на шкільний сервер, перевірте у адміністратора вашої шкільної мережі наявність належного захисту та достатнього місця для зберігання файлів, а також їх належного архівування[26].
- Визначаючи завдання пошуку інформації для свого класу, найдоцільнішим підходом може бути надати власний список використовуваних для цього URL-адрес[27]. Так ви можете бути впевнені, що адреси працюють і що їхній контент підходить учням.
- Багато завантажуваних вами файлів матимуть формат Adobe PDF для захисту авторських прав. Переконайтеся, що ви завантажили та встановили останню версію програми Acrobat Reader, щоб учні могли відкрити ці файли. Це можна зробити через сайт Adobe Systems[28].
- Основні принципи безпеки, які ви застосовуєте під час користування Інтернетом, повинні застосовуватися і при користуванні онлайн-бібліотеками. Перевірте заяви про конфіденційність і умови використання та проскануйте файли на наявність вірусів.
- Коли ви вперше приєднуєтесь до групи новин, обов'язково ознайомтеся з поширеними запитаннями, або FAQ[29], щоб зорієнтуватися в ситуації. Це дасть вам уявлення про мережевий етикет цієї групи новин. Різні групи новин дотримуються різних правил.
- Складайте якомога коротші повідомлення, але обов'язково надавайте в них усю інформацію, що стосується справи. Наприклад, якщо ви шукаєте вирішення технічної проблеми, вкажіть точну інформацію про апаратне та програмне забезпечення, яке ви використовуєте.

ДОДАТКОВА ІНФОРМАЦІЯ

- Групи новин Google за адресою:: <*http://groups.google.com/*> містять повний перелік груп новин та архів із понад одиним мільярдом дописів.
- Девід Лоуренс і Расс Олбері дають поради щодо створення групи новин, яка б увійшла до «Великої вісімки»: <*http://web.archive.org/web/20140330141231/http://www.faqs.org/faqs/usenet/creat- ing-newsgroups/part1/*>.
- У Вікіпедії є стаття про групи новин: <*http://en.wikipedia.org/wiki/Newsgroups*>.
- Британська бібліотека пропонує оцифровані колекції: <*http://www.bl.uk/manuscripts/Default.aspx*>.
- Всесвітній фонд електронних книг пропонує тисячі текстів: <*http://www.netlibrary.net/*>.
- Сайт Library Spot надає безкоштовний ресурсний центр для віртуальних бібліотек: <*http://www.libraryspot.com/*>.
- «Teacher tap» містить список із 1000 мережевих квестів та пов'язаних із ними ресурсів: <*http://eduscapes.com/tap/topic4.htm*>.
- Підліткове видання the Web we want [Мережа, якої ми хочемо] містить розділ Information is not knowledge [Інформація – це ще не знання]: <*http://www.webwewant.eu/web/guest/information*> пропонує інтерактивні заходи для підлітків, які дозволяють їм відточити своє критичне мислення та журналістські навички.

24. https://www.pinterest.com/explore/library-skills/
25. http://www.walthowe.com/glossary/d.html#download
26. http://en.wikipedia.org/wiki/Archiving#Computing_sense
27. http://en.wikipedia.org/wiki/URL
28. http://www.adobe.com/products/acrobat/readstep2.html
29. http://en.wikipedia.org/wiki/Faq

Інформаційний матеріал 12

Дистанційне навчання та масові відкриті онлайн-курси

Дистанційне навчання – це формалізована система навчання, в якій учні та вчителі фізично не присутні разом у класі. Навчальний процес відбувається за допомогою електронних носіїв інформації; із розвитком інформаційних технологій розвивається й дистанційне навчання. Нині ми бачимо віртуальні класи, де учні та вчителі обмінюються контентом за допомогою електронної пошти, миттєвих повідомлень, відеоконференцій, чатів, дошок оголошень тощо.

Незалежно від використовуваної технології, дистанційне навчання залишається перевіреним методом, який відкриває можливості для навчання протягом усього життя для студентів із усіх країн та будь-якого віку, що дозволяє їм отримувати дипломи, сертифікати та дипломи про вищу освіту (у тому числі неповну) практично від будь-якого онлайн-університету в світі. Студенти також можуть дискутувати з іншими студентами або викладачами, які можуть перебувати за сотні чи навіть тисячі кілометрів від них, що, безумовно, збагачує процес навчання.

Дистанційне навчання розпочалося в середині XIX століття, коли цілі покоління дорослих почали прагнути отримати підвищену освіту вдома, у війську чи на роботі. Раніше навчальні курси проводились із використанням листування, матеріали передавались в обидва боки через традиційну поштову систему. Утім, у наш час дистанційне навчання змінилося так, щоб використати переваги

сучасних технологій. Воно розвивається завдяки використанню Інтернету, і студенти можуть отримати вищу освіту (у тому числі неповну), жодного разу не ввійшовши до матеріальної аудиторії.

На сьогодні дистанційне навчання існує у різних формах, починаючи від класичного визначення, наведеного вище, до масових відкритих онлайн-курсів (МВОК), однорангового наставництва на YouTube та вебсемінарів, або ж використання Periscope для віртуальних екскурсій. Хоча технології пережили швидке вдосконалення, основна ідея дистанційного навчання залишається незмінною: надання освіти.

ТИПИ ДИСТАНЦІЙНОГО НАВЧАННЯ

МВОК

- МВОК були вперше запроваджені в 2008 році з метою доставки контенту через Інтернет кожному, хто хоче пройти курс, без обмеження кількості його відвідувачів. Було створено інтерактивні форуми спільнот, що дозволяють студентам та викладачам обмінюватися думками.
- До 2012 року МВОК здобули підтримку офіційно визнаних навчальних закладів, і такі університети, як Стенфордський, Прінстонський, Університет Мічигану та Університет Пенсільванії почали співпрацювати з Coursera, комерційною компанією на ринку освітніх технологій.
- Серед інших успішних програм МВОК можна назвати Udacity, яка також є партнером Стенфордського університету, та edX – провайдера МВОК, заснованого Массачусетським технологічним інститутом та Гарвардським університетом.
- Масові відкриті онлайн курси базуються на моделі викладача та студента, тоді як існування YouTube створило іншу модель дистанційного навчання, а саме однорангову.

Наставництво за одноранговою моделлю

- Наставництво за одноранговою моделлю можна охарактеризувати як заняття, на яких люди вчаться у колег зі схожим досвідом. Прикладом можуть бути діти, які навчають дітей, юристи, які навчають юристів, тощо.
- Цю модель спільного викладання легко знайти на YouTube, де «викладачі» з YouTube, які мають мільйони передплатників, пропонують навчальні курси з програмного забезпечення, вебдизайну, макіяжу, письменницької майстерності та тисяч інших предметів.

Вебінари

- Вебінари або семінари на базі мережі також можна знайти повсюдно в Інтернеті. Тренери, працівники освіти та будь-хто, хто заявляє про намір поділитися знаннями, можуть запропонувати провести вебінар.
- Формати вебінару включають презентації, лекції, презентації в PowerPoint, відео, матеріали воркшопів тощо.
- Вебінари можуть також включати матеріали для завантаження, над якими учасники працюватимуть пізніше.

Periscope

- Periscope – це застосунок для трансляції, який дозволяє людям бачити те, що бачите ви, в режимі реального часу. Цей застосунок мав неперевершений успіх протягом першого року свого існування, і викладачі все ще шукають нові сфери, де його можна з користю застосувати.
- Деякі працівники освіти вважають, що віртуальні екскурсії, спільне використання аудиторій чи отримання запитань від студентів-глядачів у реальному часі можуть бути корисними; однак за цим інструментом дистанційного навчання майбутнє.

Успіхи дистанційного навчання революціонізували навчальне середовище – від початкової школи до вищої освіти. Наприклад:

- Лекції можна читати через потокові медіа[1] або надавати як друкований матеріал, збережений у файлах, які зберігаються на сервері працівника освіти[2].

1. http://en.wikipedia.org/wiki/Streaming_media
2. http://en.wikipedia.org/wiki/Web_server

- Студенти спілкуються з викладачем та між собою за допомогою форумів[3], електронної пошти[4] та чату[5].
- Відкриті освітні ресурси (ВОР) – це документи та медіа (як правило, з відкритою ліцензією), які є придатними для викладання, навчання та оцінювання, а також для дослідницьких цілей. ВОР є ще одним засобом, за допомогою якого педагоги можуть використовувати контент та обмінюватися ним з іншими навчальними закладами, працівниками освіти та мешканцями інших континентів. ВОР іноді також створюються експертами з певних тем, які не є педагогами, і ними можна легко ділитися та обирати їх через сховище, наприклад, OER Commons[6].
- Із таких інструментів, які зазначені вище, виникла «перевернута класна кімната», тобто навчальна стратегія та тип змішаного навчання, які змінюють традиційні навчальні схеми шляхом донесення навчального контенту (часто онлайн) за межами класної кімнати та переміщення видів діяльності, включаючи ті, що традиційно вважалися домашніми завданнями, до класної кімнати. Дізнайтеся більше про ці інструменти на сайті Edutopia[7].
- Студенти/учні можуть завантажувати завдання у сховище, що зазвичай є безкоштовною послугою, за допомогою якої зареєстровані користувачі можуть безпечно зберігати файли, синхронізувати їх та легко ділитися ними з ким завгодно. Навіть опитування та іспити можна автоматизувати та проводити онлайн.
- Завдяки використанню МВОК та дистанційного навчання матеріали курсу завжди доступні та можуть бути легко оновлені. Більше того, ці нові формати навчального середовища забезпечують неперевершену гнучкість для самостійної роботи.

ЗНАЧЕННЯ ДИСТАНЦІЙНОГО НАВЧАННЯ

- Інтернет ідеально підходить для створення віртуального навчального середовища. Наприклад, студенти можуть залишатися у своєму рідному місті під час навчання у віртуальному університеті за кордоном або розподіляти час навчання між різними місцями, наприклад, між компанією та навчальним закладом для студентів, які навчаються за спеціальностями підприємницького напряму.
- Надання студентам доступу до всієї бази навчального матеріалу дає їм можливість стати більш самостійними та глибше зрозуміти, що й чому вони вивчають.
- Студенти тоді відчувають більшу відповідальність за власне навчання, а роль викладача трансформується в роль тренера.
- Курси не обмежуються робочим часом «звичайних» шкіл чи університетів, відтак кожен може скористатися розширеними можливостями для навчання протягом усього життя.
- Дистанційне навчання змінює поведінку як викладача, так і студента. Успішні студенти стають наполегливішими та розвивають свої організаторські здібності, а викладачу треба краще освоїти інформаційні технології.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

Акредитація

- Здатність до розрізнення акредитованих та неакредитованих програм корисна при визначенні правомірності надання освітніх послуг їх постачальником.
- Значки акредитації для дистанційного навчання[8] з'являються в багатьох напрямах освіти і є важливим кроком для досягнення рівного доступу до навчання.
- Коли програми не мають дійсної акредитації, але є партнерами відомих, давно створених університетів, вони часто проводять перевірку кваліфікації в тій чи іншій формі.

3. https://en.wikipedia.org/wiki/Internet_forum
4. https://en.wikipedia.org/wiki/Email
5. https://en.wikipedia.org/wiki/Online_chat
6. https://www.oercommons.org
7. http://www.edutopia.org/blog/flipped-learning-lets-talk-tech-jon-bergmann
8. https://wiki.mozilla.org/Badges

Викладач та педагогічний колектив

- Дистанційне навчання не змінює того факту, що наявність компетентних викладачів є основоположною вимогою. Воно як ніколи підкреслює необхідність надання викладачам більших можливостей для власного навчання, щоб не відставати від нових освітніх тенденцій.
- Цінність очного навчання не можна заперечувати, але переваги застосування інформаційних технологій в освіті також заслуговують на увагу.
- Оскільки кожен може створити власний вебінар або онлайн-курс навчання за одноранговою моделлю і навіть подавати себе як «експерта», критичне мислення користувачів тут є не менш важливим, ніж для всіх інших форм вебконтенту.

ЯК ЦЕ РОБИТИ

Ви повинні пам'ятати, що ви як користувач несете відповідальність за вжиття певних запобіжних заходів при виборі дипломної програми неповної чи повної вищої освіти чи іншої програми дистанційного навчання. Ось на що треба звернути увагу:

- пам'ятайте, що поряд із справжніми існують сумнівні заклади дистанційного навчання. Не забудьте ретельно вивчити програму/організацію перед вступом;
- проблеми безпеки завжди є ключовими, як і при будь-якому обміні інформацією через Інтернет. Віруси (див. Інформаційний матеріал 19 про безпеку) та хакери[9] можуть спричинити хаос у системі дистанційного навчання, тому обов'язково ознайомтесь з Інформаційними матеріалами[9] щодо конфіденційності 19 щодо безпеки, щоб побачити, які заходи безпеки слід вжити;
- авторські права[10] зазвичай захищені законодавством країни проживання студента. Однак, беручи участь у програмах дистанційного навчання в інших країнах, обов'язково переконайтесь, що джерела навчання охоплені міжнародними авторськими правами.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Розділіть студентів на пари, одна з яких буде «викладачами», а інша «студентами». Доручіть студентам дослідити певну тему курсу та навести причини, чому один тип дистанційного навчання буде кращим за інший для даної теми.
- Коли студенти домовляться про метод дистанційного навчання та тему з курсу, попросіть як групу «викладачів», так і групу «студентів» дослідити вимоги до ідеального курсу. Порівняйте потреби викладачів і студентів.
- Оберіть метод дистанційного навчання та досліджень і перевірте, який тип сертифікації доступний для нього. Чи має цей заклад хорошу репутацію? За якими показниками ви це визначаєте? Чи надає цей заклад сертифікати або значки?
- Обговоріть, чим навчальні застосунки відрізняються від навчальних курсів. Як обидві категорії можуть надати нові можливості для навчання людям із інвалідністю?
- Запропонуйте студентам створити власний короткий навчальний курс з будь-якої теми в їхній улюбленій предметній області та заохочуйте інших студентів пройти цей курс. Доручіть групі за досвідом цієї роботи скласти перелік критеріїв, які роблять онлайн-навчання більш ефективним.

9. https://en.wikipedia.org/wiki/Hacker_(computer_security)
10. http://en.wikipedia.org/wiki/Copyright

НАЛЕЖНА ПРАКТИКА

- Інтернет змінює спосіб нашого навчання, і для студентів дуже важливо мати доступ до всієї доступної інформації та інструментів, які допоможуть їм навчатися.
- «Цифровий розрив»[11] розглядається як провідна проблема для економічного та соціального зростання багатьох країн, і використання дистанційного навчання може зменшити цей розрив. Однак прихильники протилежної думки зазначають, що якщо існує цифровий розрив і люди не можуть отримати доступ до Інтернету (і дистанційного навчання), то розрив збільшиться.
- Дистанційне навчання може підвищити навчальну активність студентів таким чином, що це підвищення можна виміряти. Воно забезпечує навчання в Інтернеті з практичним досвідом для студентів, їх сімей та викладачів.
- Дистанційне навчання дає студентам можливість набути нових навичок та кваліфікацій і розвиватися у нових напрямках.
- Дистанційне навчання може також забезпечити доступ для студентів із інвалідністю, які раніше не могли відвідувати класні заняття. Студенти можуть брати участь в класному занятті онлайн та обмінюватися думками з іншими студентами та викладачем.

ДОДАТКОВА ІНФОРМАЦІЯ

- Портал дистанційного навчання надає інформацію про програми та установи дистанційного навчання у всьому світі: *<http://www.distancelearningportal.com/>*.
- Міжнародна рада з відкритої та дистанційної освіти надає інформацію та ресурси про міжнародні заклади: *<http://www.icde.org/>*.
- Європейська шкільна мережа (European Schoolnet), яка є консорціумом, створеним європейськими міністрами освіти, надає репозитарій ВОР для педагогів: *<http://lreforschools.eun.org/web/guest>*. Він також надає освітні ресурси для роботи з особливими дітьми: *<http://lreforschools.eun.org/web/guest/sennet>*.

11. https://en.wikipedia.org/wiki/Digital_divide

Інформаційний матеріал 13

Онлайн-торгівля

Електронну торгівлю можна визначити як набір послуг, програмного забезпечення та процедур, що дозволяє продавати товари та послуги онлайн. Онлайн можна придбати майже все – від книг до відпочинку, від одягу до електроніки. Окрім матеріальних благ, ви також можете оплатити такі послуги, як доступ до онлайн-контенту.

Електронна торгівля, безсумнівно, принесла явні переваги, оскільки покупки стають простішими та зручнішими; однак транзакції в рамках електронної торгівлі не позбавлені ризиків. Із зростанням цієї галузі користь та ризики від неї також зростатимуть.

Нова тенденція полягає в тому, що дедалі більше дітей здійснюють онлайн-покупки (часто через рахунок кредитної картки когось із батьків) до досягнення 18-річного віку або навіть до того, як почати працювати на умовах неповної зайнятості, що є допустимим для учня. Це призвело до занепокоєння щодо того, що діти «віртуалізують» гроші і стають нездатними сформувати уявлення про їх вартість, що може мати серйозний економічний вплив на їхнє майбутнє.

ПОКУПКИ В ЗАСТОСУНКУ

- Поняття «покупки в застосунку» означає здатність смартфона або мобільного пристрою сприяти продажу товарів або послуг у межах певного застосунку[1].
- Хоча покупки в застосунках приносять прибуток підприємствам, вони можуть стати проблемою для тих, хто не розуміє, як такі покупки працюють.
- Покупки в застосунках становлять особливу проблему для дітей та молодих споживачів, які можуть не мати права робити покупки, але здатні зробити це лише за пару кліків.

ПРАВА СПОЖИВАЧІВ

- Якщо ви купуєте товар чи послугу онлайн, на вас розповсюджуються правила захисту прав споживачів, включаючи: доставку протягом узгодженого часу, можливість повернення небажаних товарів та оплату лише за речі, які ви прямо погодились придбати. Наприклад, у ЄС ви маєте право повернути небажані товари протягом 14 днів з моменту їх отримання.
- Якщо ви купуєте товар або послугу онлайн, торговець повинен надати вам до того, як ви здійсните покупку, ключову інформацію про товар або послугу, яка є чіткою, правильною та зрозумілою.
- Щоб дізнатися перелік ключової інформації, зверніться до вебсайтів Європейського Союзу, зазначених у Додатковій інформації до цього розділу.

ЗНАЧЕННЯ ДЛЯ РОЗУМІННЯ ПРОБЛЕМ

Діти та молодь повинні бути добре обізнаними споживачами: вони повинні знати, чи мають вони право робити покупки онлайн, якими є умови покупки та як вимагати дотримання своїх прав у разі виникнення проблем. Оскільки онлайн-торгівля набуває дедалі більшої важливості, життєво важливо, щоб діти та молодь розуміли, як стати відповідальними споживачами, здатними скористатися перевагами та уникнути ризиків, пов'язаних з онлайн-торгівлею.

- Непоінформовані покупці, особливо молоді та літні, можуть бути вразливими до онлайн-шахрайства та шахрайства, пов'язаного з онлайн-торгівлею.
- Покупці та продавці-учасники електронної торгівлі, як правило, не знають один одного, і ця анонімність може знизити прагнення людей дотримуватися моральних норм.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Захищайте дані своєї кредитної картки, номери телефонів та іншу інформацію, яку можна прив'язати до вашої особи. Хакери можуть отримати інформацію про кредитну картку, ввійшовши у ваш комп'ютер або проникнувши на незахищені вебсайти, що містять вашу інформацію. Бережіться вебсайтів, які просять зберегти дані вашої кредитної картки, оскільки цю інформацію можна вкрасти.
- Не проводьте платежів за допомогою загальнодоступного з'єднання Wi-Fi. Завдяки повсюдності пунктів доступу, розташованих у кав'ярнях, готелях, аеропортах і навіть громадських парках, хакери можуть увійти в такі пункти та записати вашу особисту інформацію.
- Зловмисники також отримують інформацію про кредитні картки або банківські рахунки, обманом схиляючи людей добровільно видавати таку інформацію. Фішинг[2] належить до цієї категорії. Ці атаки часто націлені на користувачів онлайн-магазинів або платіжних сайтів, причому нападники просять їх «підтвердити» реквізити.
- Оскільки онлайн-покупки часто передбачають оплату кредитною карткою, споживачам потрібно обережно розпоряджатися своїми фінансами, щоб уникнути перевитрат. Регулярно переглядайте виписку за кредитною карткою, щоб переконатися, що ви не зробили жодної ненавмисної покупки та не було несанкціонованих покупок.

1. http://www.techopedia.com/definition/27510/in-app-purchasing
2. http://en.wikipedia.org/wiki/Phishing

- Звертайте увагу на пропозиції, які є «занадто вигідними, щоб бути правдою». Перейдіть на сайт продавця, щоб підтвердити дійсність такої пропозиції.
- Способи оплати в Інтернеті множаться і включають PayPal, біткоїни, грошові перекази, мобільні платежі тощо. Майте на увазі, що жоден спосіб оплати не є абсолютно безпечним, тому завжди дотримуйтесь обережності при оплаті будь-чого онлайн.

ЯК ЦЕ РОБИТИ

Щоб безпечно робити онлайн-покупки, споживачі повинні пам'ятати, що такі покупки вимагають додаткових заходів безпеки.

- Здійснюйте покупки лише у перевірених продавців. Це може стати важко, оскільки дедалі більше продавців виходить на ринок, але ви маєте вивчати ситуацію.
- Переконайтеся, що налаштування вашого комп'ютера, планшета чи смартфона є оптимальними.
- Переконайтеся, що область оформлення замовлення зашифрована. Багато сайтів використовують технологію SSL (рівень захищених з'єднань). Шукайте значок замка та адресу вебсайту, що вказує на його безпеку: «https» замість «http».
- Збережіть копію замовлення, надрукувавши примірник або зробивши скриншот. Ви зможете використовувати це як доказ у разі оскарження транзакції.
- Часто перевіряйте свої виписки, щоб переконатися, що вам не виставили рахунок за покупку, якої ви не робили.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Навчайте учнів дізнаватись інформацію про торгівця та умови продажу.
- Пропонуйте учням шукати, самостійно чи в групах, товари чи послуги на конкретних комерційних вебсайтах з певною метою. Наприклад, планування відпустки за фіксованим бюджетом (див. Інформаційний матеріал 10 про пошук інформації).
- Сплануйте вебсайт електронної торгівлі зі своїми учнями (наприклад, для продажу товарів для школи) або проведіть подальшу роботу над наявними подібними ініціативами, вже здійсненими в рамках школи. Вивчіть структуру хорошого вебсайту для електронної торгівлі.

НАЛЕЖНА ПРАКТИКА

- Дізнайтеся більше про торгівця чи продавця. Наприклад, eBay дозволяє продавцям формувати репутацію відповідно до їхніх показників та відгуків. Не купуйте з ненадійних джерел, особливо тих, що рекламуються в спам-розсилках (див. Інформаційний матеріал 19).
- Обов'язково застрахуйтеся від шахрайського використання ваших кредитних карток. Уважно перевіряйте свої виписки на предмет несанкціонованих покупок.
- Читайте умови транзакцій. Текст може бути довгим і використовувати професійну термінологію, але все одно не клікайте на значок, який означає, що ви прочитали та зрозуміли цей текст, якщо ви цього не зробили.
- Перевірте ціну на наявність прихованих компонентів. Це можуть бути податки або збори за доставку, стягувані з боку продавця. Також можуть стягуватися митні збори, якщо ви замовляєте товари з-за кордону.
- Чи захищений цей сайт? Символ у вигляді замка чи ключа в нижньому правому куті веббраузера означає, що сторінки захищені. Шукайте сертифікати SSL[3], які забезпечують шифрування даних перед їх відправленням.

3. http://en.wikipedia.org/wiki/Secure_Sockets_Layer

- Переконайтеся, що ви контролюєте свої персональні дані, і зверніться до Загального регламенту про захист даних для кращого розуміння. Зверніть увагу на поля, що стосуються прав продавця зберегти ваші дані або зв'язатися з вами із маркетинговою метою.
- Якщо у вас є хоч якісь сумніви щодо серйозності вебсайту, не соромтеся провести новий пошук онлайн та пошукати інші відгуки чи враження споживачів. Дані таких вебсайтів, як Trustpilot, як правило, є хорошим показником серйозності вебсайту та вражень клієнтів[4].

ДОДАТКОВА ІНФОРМАЦІЯ

- Зверніться до вебсайту Європейського Союзу щодо онлайн-покупок: *<http://europa.eu/youreurope/ citizens/shopping/buy-sell-online/rights-e-commerce/index_en.htm>*.
- Навчайте своїх учнів знанням про інтернет-торгівлю, наприклад, за допомогою вебсайту Microsoft: *<http:// web.archive.org/web/20050405134258/http://www.microsoft.com/office/previous/frontpage/ columns/edcolumn04.asp>.*
- ECC-Net «сприяє розумінню споживачами ЄС своїх прав та допомагає розв'язувати конфлікти щодо покупок, здійснених в іншій країні-члені мережі під час подорожей, або покупок онлайн»: *<http://ec.europa.eu/consumers/solving_consumer_disputes/non-judicial_redress/ecc-net/index_en.htm>*.
- TrustArc (раніше TRUSTe) – це незалежна, некомерційна, глобальна ініціатива, спрямована на зміцнення довіри та впевненості при здійсненні онлайн-транзакцій: *< https://www.trustarc.com>.*
- Вебсайт Europea.eu пропонує інформацію про онлайн-покупки: *<http://europa.eu/youreurope/citizens/consumers/shopping/index_en.htm>.*
- Інформацію про Загальний регламент про захист даних див. за адресою: *<http://ec.europa.eu/justice/ data-protection/index_en.htm>.*
- Paypal пропонує поради щодо запобігання шахрайству: *<https://www.paypal.com/eBay/cgi-bin/webscr?cmd=p/ gen/fraud-tips-buyers-outside>.*
- Інформацію про Рекомендацію ОЕСР щодо захисту споживачів в електронній торгівлі, прийняту в 2016 році, див. за адресою: *<https://www.oecd.org/sti/consumer/ECommerce-Recommenda- tion-2016.pdf>*.

4. https://www.trustpilot.com/

4. Інтернет для кожного

> «Творчість вимагає мужності, щоб відмовитись від безсумнівних істин»
>
> *Еріх Фромм, психолог*

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 14 – ВІДЕО, МУЗИКА ТА ЗОБРАЖЕННЯ В ІНТЕРНЕТІ

Перевірте ліцензію будь-якого контенту, який ви хочете використати в своїй роботі.
Використовуйте гриф Creative Commons щодо контенту, який ви створюєте та розміщуєте онлайн.
Підтримуйте чесні моделі онлайн-бізнесу, що дозволяють вам платити за контент, запропонований вашим улюбленим митцем, музикантом або авторами контенту.

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 15 – ТВОРЧІСТЬ

Одне зображення може сказати стільки ж, скільки й тисяча слів, особливо якщо ми необережно ставимося до своєї та чужої приватної інформації.
Чи розумієте ви, як забезпечити, щоб ваше право власності на вашу творчість поважалось іншими? Плагіат демонструє неповагу до власності на творчість і може мати потужний негативний вплив на різні аспекти життя суспільства. Чи знаєте ви про численні шляхи впливу плагіату на суспільство?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 16 – ІГРИ

Баланс у житті є важливим: Чи не забирають онлайн-ігри, в які ви граєте, час, потрібний для занять на відкритому повітрі та зустрічей віч-на-віч?
Коли ігри, в які ви граєте онлайн, спонукають вас зустрічатися та спілкуватися з незнайомцями, пам'ятайте, що не всі є тими, ким себе називають. Для зовсім маленьких дітей обирайте «модеровані людиною» ігри або ігри з «безпечним чатом», в якому використовуються заздалегідь підібрані фрази.
У деяких іграх покупки в застосунках можуть стати пасткою для необережних учасників. Чи переглянули ви поради з Інформаційного матеріалу 13?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 17 – ЦИФРОВЕ ГРОМАДЯНСТВО

Чи знаєте ви свої права та обов'язки онлайн?
Чи перевіряли ви свій цифровий слід останнім часом? Введіть своє ім'я в пошукову систему і подивіться, які результати вона видасть.
Які цифрові навички потрібні, щоб стати повноцінним цифровим громадянином?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 18 – ЦИФРОВЕ БАТЬКІВСТВО: ПОЗИТИВНЕ ТА ІНІЦІАТИВНЕ

Будьте позитивно налаштовані, виховуючи дітей у цей новий цифровий час, й докладайте всіх зусиль, щоб говорити з дитиною про те, що вона робить онлайн, які сайти відвідує та з ким спілкується.
Зрозумійте, що, незважаючи на те, що сучасні технології зробили величезні кроки вперед, завдання батьківства залишаються в основному незмінними: брати активну участь у житті своїх дітей, заохочуючи їх бути хорошими (цифровими) громадянами та підкреслюючи необхідність доброти й співпереживання.
Незалежно від того, чи є ви батьком малюка чи підлітка, пам'ятайте про проблеми розвитку вашої дитини, які виникають у зв'язку з інформаційними технологіями. Використовуйте ці технології таким чином, щоб допомагати, а не перешкоджати розвитку своєї дитини.

Інформаційний матеріал 14

Відео, музика та зображення в Інтернеті

Як мультимедійна платформа, Інтернет пропонує велику кількість режимів спілкування, включаючи обмін аудіо-, відеофайлами та цифровими фотографіями. Застосунки та онлайн-платформи значною мірою посприяли формуванню та розповсюдженню такого роду контенту, виходячи за межі лінгвістичних, культурних та національних бар'єрів і порушуючи важливі питання, пов'язані не тільки з розкриттям особистої інформації (див. Інформаційний матеріал 9 про конфіденційність), але й з порушеннями авторських прав та протизаконним або шкідливим контентом.

АВТОРСЬКІ ПРАВА

- Діє низка міжнародних законів та угод із цього питання. У 1996 році понад 100 країн підписали два договори про Всесвітню організацію інтелектуальної власності (ВОІВ), спрямовані на вирішення проблем цифрового контенту[1].
- Автор аудіовізуального матеріалу автоматично має авторські права на нього, якщо тільки він не відмовиться від них.

1. http://www.wipo.int/treaties/en/

- Закони більшості країн зберігають авторські права протягом 50-70 років після смерті автора.
- Зазвичай є кілька власників авторських прав на певний музичний твір. Автор, виконавець, звукозаписувальна компанія та видавець можуть усі володіти цими правами або «суміжними правами».
- Окрім економічного аспекту, автор аудіовізуального контенту має «особисті немайнові права»[2]. Це означає право бути визнаним автором та права на те, щоб твір не змінювався та не редагувався без його дозволу.
- Музику та фільми можна придбати онлайн (див. Інформаційний матеріал 13 про онлайн-покупки). Існує багато сайтів для придбання музики онлайн, наприклад, iTunes[3] та Amazon[4]. Але є також багато інших онлайн-магазинів, де можна придбати музику, зображення чи відео, тому за бажання пошукайте їх.
- Купуючи музику чи фільми онлайн, покупець, як правило, набуває обмежене право копіювання чи розповсюдження або не набуває такого права взагалі. Наприклад, онлайн-магазин музики компанії Apple iTunes дозволяє запустити придбаний запис музики на щонайбільше п'яти комп'ютерах в одному домогосподарстві[5].
- Зі змінами характеру споживання мультимедійного контенту виникають нові бізнес-моделі. Замість того, щоб купувати пісню, можна щомісячно платити за підписку на онлайн-платформу для потокової трансляції контенту та слухати будь-яку пісню або дивитися будь-який фільм, доступний на цій платформі. Як приклад таких сервісів, можна навести Netflix[6] для фільмів та Spotify[7] для музики. Знову ж таки, існує багато інших платформ, тому при бажанні пошукайте їх.
- Музична індустрія порушила справи як проти компаній-розробників програм одноранговогo обміну контентом, так і проти конкретних поширювачів файлів. Вивантажувачів – тих, хто удоступнює файли – частіше притягують до кримінальної відповідальності, ніж завантажувачів.
- Creative Commons[8] – це некомерційна організація, яка пропонує альтернативу повним авторським правам.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- На цей момент продажі цифрової музики становлять 46% від загального обсягу продажів звукозаписувальної індустрії, і вони зросли на 6,9% у 2014 році. Це пов'язано зі збільшенням кількості легальних точок продажу або трансляції цифрової музики (див. http://www.ifpi.org/facts-and-stats.php).
- Музична індустрія також відповіла на піратство, подавши низку позовів проти вебсайтів та окремих користувачів.
- Використання програм одноранговогo обміну файлами[9] може становити загрозу безпеці вашого комп'ютера, оскільки шкідливі програми часто поширюються шляхом прикріплення до музичних файлів та файлів зображень.
- Споживання мультимедійного контенту значно змінилося з поширенням Інтернету. Замість того, щоб постійно слухати один і той же улюблений компакт-диск, користувачі Інтернету люблять слухати найрізноманітніші пісні та мелодії, враховуючи великий вибір, який їм пропонує Інтернет. Середньостатистичний американець щодня прослуховує три з половиною години музики[10]. За іронією долі, піратство було серед причин, які змусили галузь переглянути «традиційну» бізнес-модель придбання повного альбому та обрати натомість платформи на основі підписки, які пропонують необмежену потокову трансляцію контенту. Пам'ятайте, що рішення, які ви ухвалюєте під час вибору платформи потокової трансляції, допомагають підтримати її бізнес-модель.

ОСВІТА

У деяких випадках навчальним закладам дозволяється відтворювати твори та поширювати їх серед громадськості. Вивчайте національне законодавство або Директиви Європейського Союзу 2001/29/ЄС від 22 травня 2001 року про гармонізацію деяких аспектів авторських і суміжних прав в інформаційному суспільстві. Слід дотриматися таких умов:

2. https://en.wikipedia.org/wiki/Moral_rights
3. http://www.apple.com/itunes/
4. http://www.amazon.com/
5. http://www.apple.com/itunes/overview/
6. https://www.netflix.com
7. https://www.spotify.com
8. http://creativecommons.org/
9. https://en.wikipedia.org/wiki/Peer-to-peer
10. http://www.digitalstrategyconsulting.com/intelligence/2014/10/us_media_consumption_trends_music_tops_the_charts.php

- Твори мають використовуватися виключно для цілей навчання або наукових досліджень.
- Потрібно вказати джерело, включаючи ім'я автора – за винятком випадків, коли це неможливо зробити.
- Від використання цього контенту не можна отримувати прямих або опосередкованих економічних чи комерційних переваг.

Отримайте письмовий дозвіл від батьків чи опікунів перед тим, як публікувати фотографії дітей або молоді онлайн.

У випадку контенту, опублікованого на вебсайті школи, увесь контент, включаючи той, що надходить від дітей та молоді, перебуває під контролем та на відповідальності школи.

У КЛАСІ

- Обговоріть моральні аспекти. Чи є піратство аудіовізуального матеріалу крадіжкою?
- Поінформуйте дітей та молодь про ризики зараження вірусами та установки шпигунського програмного забезпечення при завантаженні файлів.
- Поінформуйте дітей та молодь про можливість штрафу за завантаження музики та фільмів, захищених авторським правом.
- Організуйте дітей та молодь у команди для творення художніх/творчих робіт. Це може включати написання вірша, малювання картини, написання оповідання, створення відеофільму або складання пісні. Попросіть їх переглянути ліцензії Creative Commons і обрати тип ліцензії, яку вони хотіли б застосувати до свого контенту. Коли це завдання буде виконано, попросіть їх поділитися своїм рішенням щодо обраної ними ліцензії і пояснити свій вибір: наприклад, вони вирішили мати дуже обмежувальну ліцензію, оскільки мають намір продати свій творчий продукт, або залишити його відкритим для змін і повторного використання й повністю розуміють, що їхня робота може бути використана чи перетворена кимось іншим.

ПРОТИЗАКОННИЙ КОНТЕНТ

- Визначення протизаконного контенту в різних країнах відрізняється, але найчастіше воно охоплює дитячу порнографію чи матеріали, що містять сцени жорстокого поводження з дітьми, сцени особливо жорстокого насильства, політичний екстремізм, наклепи чи підбурювання до ненависті до меншин.
- У багатьох країнах існує гаряча лінія для повідомлення про протизаконний контент. INHOPE[11] є мережею національних гарячих ліній.
- Боротьба з протизаконним контентом може ускладнюватися чи уповільнюватися залежно від характеру контенту та місця його розміщення. Гарячі лінії співпрацюють із інтернет-провайдерами та поліцією й найкраще підходять для боротьби з протизаконним контентом.
- Більшість онлайн-платформ використовують різноманітні методи виявлення та видалення протизаконного контенту, наприклад, за допомогою людської та/або автоматизованої модерації, технології фото/відео-ДНК-аналізу та механізмів звітування.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Є підстави вважати протизаконний контент набагато серйознішим кримінальним злочином, ніж порушення авторських прав. У той час як у законодавстві про авторські права існують такі поняття, як «добросовісне використання» та винятки з некомерційною або освітньою метою, операції з протизаконним контентом завжди будуть розглядатися як серйозний кримінальний злочин, особливо у таких випадках, як матеріали сексуального насильства над дітьми або пропаганда тероризму. Незважаючи на те, що спроби перевірити на міцність обмеження різних свобод, наприклад: свободи вираження поглядів, є природною рисою людини, особливо характерною для дітей та молоді, існують певні межі, які ніколи не слід переходити.
- Операції з протизаконним контентом часто пов'язані з іншими протизаконними діями, такими як нелегальний продаж зброї чи наркотиків. Значна частина цих операцій відбувається в так званій «темній мережі», тобто тій частині Інтернету, до якої не можна отримати доступ за допомогою традиційних пошукових систем. Публікація, поширення або пошук протизаконного контенту може, таким чином, легко перерости в дуже серйозні злочини.

11. http://www.inhope.org/gns/home.aspx

- Ваша школа чи компанія повинна здійснювати політику прийнятного користування (ППК) або політику відповідального користування (ПВК), яка би включала питання авторських прав та протизаконного матеріалу.
- Щоразу, коли ви знаходите онлайн будь-який контент, який ви хотіли б використати, обов'язково перевірте його ліцензію. Є багато різних ліцензій. Контент, вироблений звичайними користувачами Інтернету, охоплюється різними ліцензіями. Найбільш «відкрита» ліцензія дозволяє вам повторно використовувати та змінювати контент без необхідності повідомляти власника, навіть якщо це робиться в комерційних проєктах. Інші ліцензії вимагають надання належних посилань, обмежують використання матеріалу неприбутковими цілями або забороняють внесення будь-яких змін. Такі пошукові системи, як Google або Bing, пропонують фільтрувати пошук зображень та відео за характером ліцензії. Є також багато платформ, де ви можете придбати контент для використання у своїх проєктах.
- Обов'язково застосуйте до свого матеріалу ліцензію, що вказує на авторське право. Ви можете вибрати більш традиційні авторські права, такі, які використовуються звукозаписувальними компаніями, або використовувати грифи Creative Commons[12] для створеного вами матеріалу, щоб пояснити, як інші можуть його використовувати.
- Хоча може виникнути спокуса пошукати «безкоштовну» музику, зображення або відео онлайн, пам'ятайте, що ви в кінцевому підсумку платите за це так чи інакше: зазнаючи нескінченних атак реклами, заражаючи свій комп'ютер шкідливими програмами, які можуть викрасти ваші дані, або навіть отримуючи судовий позов від власників авторських прав. Підтримуючи платформи, що забезпечують хороший сервіс та вигідне співвідношення ціни та якості, ви сприяєте позитивному розвиткові Інтернету, уникаючи наповнення його рекламою, що марно витрачає ваш час, або низькоякісним чи шкідливим контентом, а також чесно винагороджуючи митців за їх роботу.
- У наш час контент масово виробляється користувачами щодня в усьому світі. Це можуть бути короткі відеоролики, розміщені на платформі потокового відео: YouTube або Dailymotion, фотографії та зображення, розміщені в соціальних мережах, або музика, вивантажена на платформи потокової трансляції музики. Але незалежно від того, чи вказав на ліцензію користувач, який вивантажив певний контент, майте на увазі, що будь-який вивантажений контент захищено авторським правом. Закони про авторське право не застосовуються, лише якщо автор прямо зазначив, що він відмовляється від будь-яких прав на створений ним контент.
- Дальшим обмеженням використання контенту є захист даних. Репост конфузного відео чи зображення, наприклад, є порушенням конфіденційності чужих даних і може становити кіберцькування. За загальним правилом, завжди запитуйте користувача, який уперше розмістив певний контент, чи можете ви використовувати його повторно, змінювати, робити репост чи щось подібне. Прохання про дозвіл та надання належного посилання – це більше, ніж юридичний обов'язок, це допомагає створити більш позитивне та привабливе середовище для творчості та участі в онлайн-діяльності. Для отримання більш детальної інформації про захист даних відвідайте вебсайт правосуддя ЄС, рубрика «Реформа правил захисту даних ЄС»[13].

НАЛЕЖНА ПРАКТИКА

- Програмні фільтри можуть допомогти заблокувати деякі нелегальні вебсайти, але вони ніколи не бувають справжнім рішенням проблеми. Жоден фільтр не може захистити вас, якщо ви шукаєте протизаконний контент.
- Якщо ви батько чи мати, вчитель або старший брат чи сестра, обов'язково запустіть у родині та класі обговорення щодо вражень від перебування онлайн. Незаконний контент – це не лише питання авторських прав, він часто оточений також шкідливим або шокуючим контентом, шкідливим програмним забезпеченням, спамом тощо.

12. http://creativecommons.org/
13. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

- Повідомте про протизаконний контент на гарячу лінію (див. INHOPE нижче) або скористайтеся механізмами повідомлення, що надаються платформою, якою ви користуєтесь.
- Переконайтеся, що у вашій школі діє сувора політика щодо протизаконного контенту, а діти та молодь належним чином інформуються про потенційні наслідки публікації, поширення або перегляду протизаконного контенту.
- Обговоріть шкідливий і протизаконний контент. Дослідження показують, що багато дітей та молоді навмисно чи випадково знаходять такий контент в Інтернеті, але мало хто розповідає про це комусь із дорослих.

ДОДАТКОВА ІНФОРМАЦІЯ

- Відвідайте вебсайт Всесвітньої організації інтелектуальної власності (ВОІВ), щоб отримати додаткову інформацію щодо питання авторських прав і пов'язаних із цим питань: *<http://www.wipo.int>.*
- Дізнайтеся, що ваш улюблений музичний колектив хоче сказати про музичне піратство в статті «Виконавці говорять про музичне піратство»: *<https://www.upvenue.com/article/1590-musician-stances-on-music-piracy.html>*.
- INHOPE – це мережа гарячих ліній для повідомлення про протизаконний контент у Інтернеті: *<http://www.inhope.org/gns/home.aspx>*.
- Сторінка Ради Європи, присвячена ЗМІ, містить інформацію про її роботу в галузі авторського права: *<http://www.coe.int/media>*.
- Вебсайт Європейської комісії пропонує інформацію про права інтелектуальної власності: *<http://europa.eu/youreurope/business/start-grow/intellectual-property-rights/index_en.htm>*.
- IFPI, яка представляє індустрію звукозапису у всьому світі, пропонує посібник для батьків та вчителів, щоб допомогти дітям безпечно та легально вивчати музику в Інтернеті: *<http://www.ifpi.org/music-and- the-internet-guide.php>*.
- У Цифровому порядку денному для Європи, опублікованому Європейською комісією, містяться додаткові поради щодо авторських прав: *<https://ec.europa.eu/digital-agenda/en/copyright>*.
- Для отримання додаткової інформації про темну мережу див. відповідну сторінку Вікіпедії: *<https://en.wikipedia.org/wiki/Darknet>*.
- Відповідні статті Конвенції ООН про права дитини:
  Стаття 13 – Діти мають право одержувати і поширювати інформацію, якщо це не шкодить їм чи іншим особам.
  Стаття 17 – Діти мають право отримувати достовірну інформацію із засобів масової інформації. Телебачення, радіо та газети повинні надавати інформацію, яку діти можуть зрозуміти, і не повинні просувати матеріали, які можуть завдати шкоди дітям.
  Стаття 33 – Уряд повинен забезпечувати захист дітей від небезпечних наркотиків.
  Стаття 34 – Уряд повинен захищати дітей від сексуального насильства.
  Стаття 36 – Дітей слід захищати від будь-якої діяльності, яка може зашкодити їхньому розвитку.
  Стаття 37 – Ніхто не має права карати дітей жорстоким або шкідливим способом. З дітьми, які порушують закон, не слід поводитися жорстоко. Їх не слід ув'язнювати разом із дорослими і вони повинні мати можливість підтримувати контакт зі своїми сім'ями.
  Стаття 40 – Діти, яких звинувачують у порушенні закону, мають право на правову допомогу та справедливе ставлення в системі правосуддя, яка поважає їх права. Уряди повинні встановити мінімальний вік, до досягнення якого діти не можуть бути притягнуті до кримінальної відповідальності, й надати мінімальні гарантії справедливості та швидкого завершення судових процесів або альтернативних процедур.

Інформаційний матеріал 15

Творчість

ЯКИМ ЧИНОМ ІНТЕРНЕТ СПРИЯЄ ТВОРЧОСТІ?

Через гнучку природу Інтернету сучасна обстановка в класі є менш жорсткою, ніж будь-коли раніше. Технологія, що швидко розвивається, дає учням широкі можливості досліджувати теми, які їх цікавлять, і навчатися з використанням нетрадиційних методів (див. Інформаційний матеріал 3 про Web 2.0, 3.0 та інших).

Використовуючи інструменти, надані сучасними технологіями, учні можуть створювати матеріали професійного рівня, які можна публікувати для аудиторії в будь-якій точці світу. Вони можуть виробляти власні онлайн-продукти та проводити всілякі експерименти й моделювання в класі або в інтерактивному режимі з іншими учнями в Інтернеті.

Інтернет глобалізував освіту і надає можливість учням в режимі реального часу зв'язатися з однолітками по всій земній кулі. Для повного використання цих можливостей важливо, щоб молоді користувачі Інтернету стали творцями, а не просто споживачами; ця мета лежить в основі багатьох ініціатив навчання кодуванню (наприклад, див. *<Http://codeweek.eu>*), які реалізуються в багатьох країнах сьогодні.

ПОСИЛЕННЯ ТВОРЧИХ ПРОЦЕСІВ У НАВЧАННІ

- Успішна інтеграція інформаційних технологій у роботу в класі дає учням можливість показати свою здатність до інновацій, індивідуальність та креативність, і розвинути свій підприємницький потенціал.
- Використання програмного забезпечення для творчості та Інтернету сприяє підвищенню мотивації та значно підвищує якість навчання у класі й поза ним. Кодування допомагає сформувати глибше розуміння того, як працюють інформаційні технології, а отже, може сприяти появі більш відповідальних стратегій користувачів.
- Можливість проявити творчі здібності й узяти на себе більш активну роль у навчальному процесі заохочує залученість та участь – два основні елементи активної громадянської позиції.
- Інтернет і мобільні технології пропонують безліч захопливих можливостей для вчителів та учнів створювати та вивантажувати власний аудіовізуальний контент. Вони також можуть скористатися Інтернетом, щоб зв'язатися з митцями в будь-якій точці світу й попросити порад та оцінок щодо своєї роботи. Митці можуть використовувати інструменти відеоконференції[1] та віртуальні зустрічі (див. Інформаційний матеріал 12 про дистанційне навчання) для проведення воркшопів.
- Використання соціальних мереж[2] та спеціальних соціальних платформ[3] під час навчання в класі стимулює учнів до спільної роботи і співпраці за спільними проєктами онлайн. Це забезпечує новий вихід для творчості, а мозковий штурм, який проводиться при цьому, може стимулювати творчий процес.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- **Питання справедливості:** чи всі мають необхідне обладнання та підключення для доступу до Інтернету? Чи всі діти та молодь у всьому світі, незалежно від віку, здібностей чи особливих потреб, можуть скористатися рівними можливостями для творчості, тобто знають, як використовувати всі доступні технології для творчості?
- **Фактор онлайн-безпеки**: чи фільтри[4], встановлені для захисту юних користувачів, особливо дуже маленьких дітей та дітей з особливими освітніми потребами, перешкоджають якимось чином доступу до матеріалів, необхідних для творчості? Як можна вирішити це питання, щоб учні могли користуватися безпечним доступом до необхідного їм контенту (див. Інформаційний лист 20 щодо маркування та фільтрування)?
- **Можливості навчання для вчителів**: учні часто можуть бути більш підкованими в Інтернеті, ніж їхні вчителі. Учителям потрібні більші можливості для навчання, щоб належним чином орієнтувати своїх учнів у всіх аспектах ІКТ, включаючи використання мобільних телефонів (див. Інформаційний матеріал 5 про мобільні технології та Інформаційний матеріал 12 про дистанційне навчання).
- **Питання технічної підтримки:** у школах необхідна адекватна технічна підтримка, щоб технічні проблеми не перешкоджали реалізації програм та проєктів.
- **Буферизоване середовище**: творчість дозволяє людині виражати свої особисті почуття. Хоча в ідеалі ми повинні уникати накладання будь-яких обмежень на творчі процеси молодої людини, важливо підкреслити принципи толерантності, співпереживання та поваги у результатах роботи, особливо під час групових мозкових штурмів. Для спрямування роботи в конструктивному напрямі необхідна присутність учителя або делегата класу.
- **Конфіденційність**: Web 2.0 та 3.0 значно полегшили вивантаження фотографій та зображень до Інтернету. Учні повинні знати, що одне зображення може сказати стільки ж, скільки й тисяча слів, і може загрожувати розголошенням їхньої власної та чужої конфіденційної інформації.
- **Авторські права**: молоді люди повинні якомога раніше навчитися поважати власність на творчий доробок і розуміти ціну плагіату для суспільства[5].

1. http://web.archive.org/web/20080614214250/http://www.netlingo.com/right.cfm?term=video%20conferencing
2. http://www.eun.org/teaching/smile
3. http://www.etwinning.net
4. https://en.wikipedia.org/wiki/Content-control_software
5. https://www.teachingcopyright.org/handout/copyright-faq.html

ПІДВИЩЕННЯ РІВНЯ ТВОРЧОЇ АКТИВНОСТІ В КЛАСІ

- Мережевий квест[6] – це заснований на дослідженні підхід до інтеграції Інтернету в роботу у класі.
- Учні можуть поставити собі складне завдання, вивчаючи основи кодування[7] для створення власних вебсайтів. Це стимулює процеси творчого мислення різними способами, оскільки вимагає висловити свою думку щодо графіки та контенту.
- Учні можуть співпрацювати в проєктах, що розвивають навички написання текстів та аудіовізуальної творчості шляхом створення онлайн-оповідань та іншого контенту. Мобільні телефони можна використовувати, наприклад, для зйомки зображень і відео про культурні та професійні аспекти власної країни та подальшого обміну ними з учнями з-за кордону. Це може допомогти їм на практиці дізнатися про поняття, пов'язані з конфіденційністю, дозволами на фотографування тощо.
- Заохочуйте учнів створювати інтерактивні вікторини та мережеві заходи за допомогою програмного забезпечення, наприклад, Hot Potatoes[8], або інтерактивні оповідання з багатьма можливими розв'язками, для яких використовується таке програмне забезпечення, як те, що доступне на вебсайті Quia[9].
- Учні середніх шкіл і студенти університетів можуть створити власне навчальне 3D-середовище за допомогою такого програмного забезпечення, як Active Worlds[10]. Вони можуть побудувати свій ідеальний ландшафт або власне віртуальне шкільне/університетське містечко, а також співпрацювати з іншими учнями/студентами в проєктах на різні теми.

НАЛЕЖНА ПРАКТИКА

- Інтернет може бути використаний як основний інструмент дослідження базової інформації щодо різних тем. Відтак учні/студенти можуть застосувати отримані знання при виконанні завдання, яке стимулює творчість. Інформаційні технології надають учням/студентам можливість розвивати мислення вищого порядку.
- Інтернет та інші сучасні технології забезпечують активне спілкування та співпрацю між учнями/студентами з різних країн, які належать до різних культур. Більше ніж коли-небудь раніше, учні/студенти мають можливість провести мозковий штурм для знаходження творчих рішень за участю однолітків.
- Програмне забезпечення з відкритим кодом дозволяє учням/студентам з усього світу, особливо дітям з менш забезпечених сімей, безкоштовно втілювати свої творчі наміри. Таке програмне забезпечення, як Open Office, Gimp, Audacity або Blender, дозволяє дітям безкоштовно створювати документи, редагувати зображення або аудіофайли або навіть робити перші кроки в 3D-анімації. Окрім того, програмне забезпечення з відкритим кодом надає можливість навчитися кодуванню та поділитися своїми навичками, приєднавшись до спільноти мотивованих кодерів-добровольців для вдосконалення та оновлення програмного забезпечення, яке ви використовуєте. Обов'язково вкажіть на такі альтернативи своїм дітям/учням.
- Учителі виявили, що впровадження інформаційних технологій у класі з використанням практичних занять дає учням можливості для вирішення проблем та створення інновацій.
- Пам'ятайте про цілі навчання: ключовою умовою досягнення цих цілей є зосередження на процесі, необхідному для створення продукту, а не на самому продукті.
- Коли учні публікують результати творчої діяльності онлайн, вони повинні поважати авторські права[11] та, можливо, дізнатися більше про Creative Commons[12]. Нагадуйте їм про необхідність посилатися на джерела, коли вони використовують матеріали, створені іншими.

6. http://webquest.org
7. https://scratch.mit.edu/educators/
8. http://hotpot.uvic.ca/
9. http://www.quia.com/
10. http://www.activeworlds.com/
11. https://en.wikipedia.org/wiki/Copyright
12. https://en.wikipedia.org/wiki/Creative_Commons

ДОДАТКОВА ІНФОРМАЦІЯ

Низку вебсайтів можна використовувати як вихідну точку для залучення учнів до проєктів, де заохочується творчість, а співпраця є необхідною:

- Міжнародний кіберярмарок шкіл (International Schools Cyberfair) – це місце для онлайн-зустрічей, де батьки, учні та педагоги можуть співпрацювати, взаємодіяти, розробляти, публікувати та знаходити навчальні ресурси: *<http://www.globalschoolnet.org/GSH/>*. Європейська шкільна мережа пропонує подібні ресурси для шкіл: *<http://www.eun.org>*.
- Міжнародна програма вирішення проблем майбутнього залучає учнів до творчого вирішення проблем шляхом стимуляції навичок критичного та творчого мислення: *<http://www.fpsp.org>*.
- Ідеї та ресурси для сприяння творчості можна знайти на сайті Education Scotland: *<http://www.educationscotland.gov.uk/learningandteaching/approaches/creativity/>*.
- Проєкт педагогічного факультету Університету Джонса Гопкінса «Нові горизонти для навчання» *<http://education.jhu.edu/PD/newhorizons/>* пропонує набір нових дидактичних практик для сприяння творчому навчанню.
- Розділ 6 «Ваш внутрішній художник» посібника «Мережа, якої ми хочемо» (Web We Want) *<http://www.webwewant.eu>* описує низку заходів, які спонукають молодих людей перевіряти власне творче надбання та дізнаватися більше про плагіат, авторські права тощо.

Інформаційний матеріал 16

Ігри

Відеоігри можна охарактеризувати як розваги, що передбачають взаємодію людини з користувацьким інтерфейсом, метою якої є генерування візуального зворотного зв'язку на відеопристрої, наприклад, телевізійному екрані, комп'ютері, планшеті або смартфоні. Цей термін охоплює величезну кількість жанрів – від аркад та рольових ігор до стратегічних ігор та фантастичних світів. eSports – це термін для ігрових змагань, учасники яких (часто це напівпрофесійні геймери) змагаються за грошові призи на очах аудиторії, яка швидко зростає, як вживу, так і онлайн – це може бути будь-яка гра, не тільки спортивна. У ігри можна грати наодинці, з партнерами в кількісно обмежених командах, або в них можуть брати участь тисячі, а іноді і мільйони незнайомців, які грають разом. До таких масових багатокористувацьких онлайн-ігор (МБОІ) належать World of Warcraft та Game of Thrones. Відеоігри зараз є третім за величиною сектором ринку розваг у всьому світі після ефірного та кабельного телебачення, при цьому обсяг продажів у ньому склав 74 мільярди доларів США станом на 2015 рік, подвоївшись між 2013 і 2014 роками[1].

1. https://en.wikipedia.org/wiki/Video_game

Смартфони та планшети й присутність в Інтернеті дедалі молодших та старших користувачів мали значний вплив на ігрові тенденції; дослідження 2015 року[2] показує, що приблизно кожна третя дитина віком до 18 років грає в онлайн-ігри, але середній вік онлайн-геймерів становить 31 рік. Хоча раніше в цій сфері переважали чоловіки, сьогодні жінки роблять 50% усіх покупок і становлять 48% гравців у електронні ігри у всьому світі та 52% у Великій Британії. Характер використання спеціальних ігрових консолей також змінився, і тепер власники витрачають більше половини часу, проведеного за консолями, переглядаючи телебачення, потокове відео, диски Blu-ray та мандруючи Інтернетом[3].

Ігри тепер відіграють більшу роль як у сімейних заходах, так і в класних заняттях. З-поміж учителів перших 9 класів 74% заявляють, що включають онлайн-ігри у заняття в класі, причому 4/5 із цих ігор є «навчальними». До того ж 56% батьків відзначають, що ігри позитивно впливають на їхніх дітей. З огляду на дедалі більшу популярність ігор та їх вплив на права людини, Рада Європи опублікувала набір керівних принципів для постачальників ігор, розроблений у співпраці з постачальниками ігор та експертами із захисту дітей, освіти та прав людини[4].

Це свідчить про те, що онлайн-ігри справді є великим бізнесом, адже мільйони користувачів щодня грають в дуже велику кількість ігор через Інтернет та на мобільних телефонах.

ПЕРСОНАЛЬНИЙ РОЗВИТОК ТА ОСВІТНЯ ЦІННІСТЬ

- Ігри – це більше, ніж розвага; це збагачуюча спільна діяльність, у якій беруть участь діти та дорослі різного віку. Це сприяє творчості та взаємодії й відіграє важливу роль у соціальному та інтелектуальному розвитку.
- Участь у іграх належить до рідкісних випадків, коли дорослі та діти можуть нарівні обмінюватися думками (спілкування між поколіннями).
- Діти дізнаються про демократію, граючи в різних соціальних структурах, у середовищі, обмеженому правилами та параметрами.
- Ігри часто передбачають необхідність ділитися чимось та повагу до прав і власності інших людей, іноді навіть вводячи гравців у контакт з іншими культурами та міжкультурними практиками. Діти можуть практикувати соціальні навички, не боячись невдач і зберігаючи контроль за ситуацією. Оскільки ігри вимагають від дітей дотримання правил і вказівок, вони збільшують їхню здатність до самодисципліни та самостійності.
- Головоломки, настільні ігри, пригоди та квести надають гравцям можливість розвинути стратегічне мислення та навички вирішення проблем. Деякі ігри можна використовувати для розвитку тонкої моторики та навичок просторового мислення у дітей молодшого віку та в терапевтичних цілях у роботі з дітьми з інвалідністю.
- Деякі дослідження свідчать про те, що ігри можуть бути корисними при аутизмі, і в цьому плані особливо відзначають такі ігри, як Minecraft.
- Онлайн-ігри корисні для ознайомлення новачків із інформаційними технологіями та кодуванням, а також для загального розвитку інтересу до ІКТ та їх розуміння[5].
- Ігри можуть бути інтегровані майже в будь-яку область навчальної програми, починаючи від математики і закінчуючи суспільними науками та мовами.

2. http://web.archive.org/web/20160420163852/http://www.bigfishgames.com/blog/2015-global-video-game-stats-whos-playing-what-and-why/
3. http://web.archive.org/web/20151023082205/http://www.nielsen.com/us/en/insights/news/2015/game-consoles-in-2015-one-stop-shop-for-games- and-entertainment.html
4. http://www.coe.int/en/web/portal/guidelines-for-providers
5. https://en.wikipedia.org/wiki/Information_technology

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Дискусії про зв'язки між відеоіграми та залежністю, агресією, насильством, низьким соціальним розвитком і різноманітними проблемами стереотипізації та сексуальної моралі ведуться вже протягом декількох десятиліть, і поки немає переконливих доказів того, що ці аспекти в іграх є більш впливовими, ніж у інших носіях інформації[6].
- Відповідність ігор віку важлива, особливо для найменших дітей.
- Часто вказують на ризик виникнення залежності. Американська психіатрична асоціація (АПА) у 2013 році дійшла висновку, що доказів для включення ігрової залежності до офіційного списку психічних розладів недостатньо, але запропонувала термін «розлад, пов'язаний із іграми в Інтернеті», і закликала до подальших досліджень для визначення критеріїв цього розладу. Хоча розлад, пов'язаний із іграми в Інтернеті, пропонується визнати як розлад, все ще є предметом суперечок, наскільки цей розлад викликаний самою ігровою діяльністю, та чи є він до певної міри наслідком інших розладів[7].
- Баланс у житті є важливим аспектом при розгляді ігор, як і всіх видів діяльності в Інтернеті. Ігри не повинні забирати час, потрібний для занять на відкритому повітрі та зустрічей віч-на-віч.
- Деякі онлайн-ігри дозволяють гравцям зустрічатися та спілкуватися з незнайомцями. Переконайтеся, що ігри, що заохочують взаємодію користувачів, особливо ті, що призначені для найменших дітей, контролюються за допомогою модерації людиною або пропонують «безпечний чат», у якому використовуються заздалегідь підібрані фрази.
- Через покупки в застосунках у деяких іграх діти можуть мимоволі витратити значні суми грошей своїх батьків на об'єкти колекціонування та інструменти.

НАЛЕЖНА ПРАКТИКА

- Системи маркування та рейтингування спонукають суб'єктів ігрової індустрії діяти відповідально, вимагаючи від них надавати визначення та описи своїх продуктів. Це також допомагає покупцям ігор оцінити вміст і вікову придатність ігор, а також безпечніше діяти на ігровому ринку. PEGI (Pan European Game Information, Загальноєвропейська інформація про ігри) є єдиною загальноєвропейською системою класифікації, яка надає докладні рекомендації щодо вікової придатності ігрового контенту. Рейтинги приблизно 20 000 ігор можна знайти на її вебсайті <*www.pegi.info*>. PEGI також є частиною IARC (International Age Rating Coalition, Міжнародна коаліція вікових рейтингів), яка надає послуги рейтингування та вікової класифікації в світовому масштабі ігор та застосунків, що постачаються за допомогою цифрових технологій[8]. Як результат, рейтинги PEGI тепер також доступні для всіх продуктів у Google Play Store та Mozilla Firefox Marketplace. Дуже скоро до них приєднаються магазини застосунків Microsoft Windows Mobile та Windows 10.
- Відстежуйте кількість годин, проведених за іграми. Вживайте заходів, якщо через це діти та молодь уникають інших соціальних заходів або пропускають навчання, щоб провести час за іграми.
- Ігрові спільноти можуть формувати почуття приналежності, що може зробити дітей занадто довірливими. Нагадуйте їм, що онлайн-друзі можуть не завжди бути тими, ким вони себе називають. Важливо нікому не передавати особисту інформацію онлайн.
- Онлайн-ігри стають популярним сімейним заняттям і надають цінну можливість ініціювати сімейні розмови про відповідальне користування Інтернетом. Якщо ви як батьки чи вчителі стурбовані тим, що ваші діти витрачають занадто багато часу на електронні ігри, ознайомтеся з багатьма «тестами на ігрову залежність», які ви можете знайти за допомогою пошукової системи – і це також є ідеальним вихідним пунктом для розмови.
- Рада Європи створила привабливу, інтерактивну онлайн-гру[9] з метою сприяння дотриманню прав дітей та захисту їх від насильства в будь-якій формі.

6. https://en.wikipedia.org/wiki/Video_game_controversies#Crime_and_violence
7. https://en.wikipedia.org/wiki/Video_game_addiction
8. http://www.globalratings.com
9. http://www.wildwebwoods.org

ДОДАТКОВА ІНФОРМАЦІЯ

- Перегляньте вебсайт Ask about games *<http://www.askaboutgames.com/>*, щоб краще розібратися у відеоіграх.
- Прочитайте про сучасні дослідження ігор в International Journal of Computer Game Research: *<http://www.gamestudies.org/>*.
- Законодавство про відеоігри – це величезна тема, яка може включати кримінальне, регуляторне, конституційне, адміністративне, корпоративне, договірне право, а в деяких юрисдикціях також антимонопольне право. Присвячений державній політиці розділ сайту ISFE (Interactive Software Federation of Europe, Федерація інтерактивного програмного забезпечення Європи – *<http://www.isfe.eu/objectives/public-policy>*) надає цінну інформацію для розуміння відповідного законодавства ЄС та світового законодавства.
- Вебсайт PEGI містить інформацію про рейтингування та маркування: *<http://www.pegi.info/pegi/index>*. Доповнення до цієї системи, яке називається PEGI Online, має на меті забезпечити більш безпечне ігрове онлайн-середовище. Ліцензовані PEGI Online та відповідно марковані постачальники ігор відповідають стандартам Кодексу безпеки PEGI Online <www.pegionline.eu>, які включають, серед іншого, зобов'язання вживати заходів для захисту вебсайтів від протизаконного та образливого контенту, створеного користувачами, та небажаних посилань, захищати конфіденційність та мати незалежний механізм розгляду скарг.
- Перевірка віку є складною справою в ігровій індустрії, як і в інших онлайн-секторах, які приваблюють маленьких дітей. У Європі тривають пілотні проєкти, метою яких є перевірити, чи можливо створити «біржу атрибутів», за допомогою якої компанії, що продають або надають доступ до товарів та послуг із віковими обмеженнями, могли б об'єднувати свою інформацію та обмінюватися нею, щоб зробити перевірку віку більш ефективною.
- Щотижня публікуються новини про онлайн-ігри, оскільки цей сектор ринку розваг зростає найшвидше. Зверніться до кількох сайтів, щоб отримати збалансоване уявлення про найпопулярніші ігри, новини ігрового ринку, описи, звіти про дослідження та статистику. Корисними вихідними точками для цього є вебсайти Bigfishgames, IFSE, PEGI та Nielsen. Ви також можете підписатись на стрічки новин/бюлетені, пропоновані цими вебсайтами, або встановити чітко визначене сповіщення Google, щоб залишатись у курсі подій.

Інформаційний матеріал 17

Цифрове громадянство

Широке використання Інтернету та нових комунікаційних технологій стало потужним рушієм зростання та створення робочих місць і підвищило якість життя багатьох громадян. Щоденне користування Інтернетом стало звичним явищем для багатьох; проте глибше розуміння цифрового громадянства та цифрових прав може при цьому бути відсутнім.

Інформована участь усіх громадян у тому, що називають цифровим середовищем, залежить від формування грамотних уявлень з набагато ширшого кола питань. Сюди входить здатність критично аналізувати різноманітну інформацію, яку ми сприймаємо (тобто аудіовізуальний контент), самостійно формувати свої думки, брати активну участь у вирішенні проблем спільноти та освоювати нові форми соціальної взаємодії. У публікації, яка вийшла ще два десятиліття тому, ЮНЕСКО описала ці можливості як чотири стовпи освіти: навчатися знати, робити, бути і жити разом[1]. Більше того, щоб бути цифровим громадянином, потрібно вміти користуватися вебінструментами (див. Інформаційний матеріал 3 про Web 2.0, Web 3.0 та інші) та розумітися на питаннях електронної конфіденційності (див. Інформаційний матеріал 9).

1. http://www.unesco.org/education/pdf/15_62.pdf

ЩО ТАКЕ ЦИФРОВЕ ГРОМАДЯНСТВО?

- Цифрове громадянство – це термін, який описує, як людина повинна діяти[2], використовуючи цифрові технології онлайн[3].
- Деякі експерти пропонують дев'ять елементів, як складові цифрового громадянства: цифровий доступ, цифровий споживацтво, цифрові комунікації, цифрова грамотність, цифровий етикет, цифрове законодавство, цифрові права та обов'язки, цифрове здоров'я та самопочуття й цифрова безпека[4].
- Яким би не був склад цифрового громадянства, очевидно, що всі користувачі Інтернету несуть відповідальність і, можливо, навіть мають обов'язок діяти відповідально при використанні Інтернету та комунікаційних технологій.

Цифровий слід

- Цифровий слід – це дані, які залишають після себе користувачі цифрових послуг.
- Пасивний цифровий слід створюється, коли дані збираються без відома власника, тоді як активні цифрові сліди створюються, коли персональні дані навмисно оприлюднюються користувачем з метою поширення інформації про себе за допомогою вебсайтів або соціальних мереж[5].

Цифрова ідентичність

- Цифрова ідентичність – це інформація, що використовується для представлення людей, організацій чи машин в інформаційних системах та мережах[6].

Цифрова грамотність

- Цифрова грамотність – це знання, навички та варіанти поведінки, що використовуються для широкого діапазону цифрових пристроїв: смартфонів, планшетів, ноутбуків та настільних ПК[7].
- Інформаційно-комунікаційні технології вже охопили всі аспекти нашого повсякденного життя, змінивши тип навичок, необхідних для того, щоб бути активним членом суспільства.
- Оскільки Інтернет продовжує розвиватися зі зростанням бездротових мереж[8], все більше значення буде надаватися здатності людей використовувати сучасні технології для ефективного отримання та передачі інформації таким чином, що виходить за межі як медіаграмотності, так і Інтернет-грамотності.

Цифрові права

- Рада Європи підготувала довідник «Права людини для користувачів Інтернету», який роз'яснює цифрові права та обов'язки у зручному для користувача форматі та підкреслює, що права людини діють однаковою мірою як онлайн, так і офлайн[9].
- Термін «цифрові права»[10] означає права людини[11], які дозволяють людям отримувати доступ до цифрових носіїв інформації, використовувати, створювати та публікувати такі носії, а також отримувати доступ до комп'ютерів та інших електронних пристроїв чи мереж зв'язку й користуватися ними.
- Цей термін особливо стосується захисту та реалізації наявних прав, таких як право на приватне життя[12], у контексті нових цифрових технологій та, особливо, Інтернету[13].
- Що стосується цифрових прав молоді в Європі, Молодіжний маніфест ЄС є онлайн-декларацією європейської молоді про те, як зробити Інтернет кращим[14].

2. https://en.wikipedia.org/wiki/Digital_citizen
3. https://en.wikipedia.org/wiki/Digital_electronics; https://en.wikipedia.org/wiki/Etiquette_in_technology#Online_etiquette
4. http://www.digitalcitizenship.net/Nine_Elements.html
5. https://en.wikipedia.org/wiki/Digital_footprint
6. https://en.wikipedia.org/wiki/Digital_identity
7. https://en.wikipedia.org/wiki/Digital_literacy
8. https://en.wikipedia.org/wiki/Wireless_network; http://en.wikipedia.org/wiki/3G
9. https://www.coe.int/en/web/internet-users-rights/guide
10. https://en.wikipedia.org/wiki/Digital_rights
11. https://en.wikipedia.org/wiki/Human_rights
12. https://en.wikipedia.org/wiki/Right_to_privacy або свобода вираження поглядів https://en.wikipedia.org/wiki/Freedom_of_speech
13. https://en.wikipedia.org/wiki/Internet
14. http://www.youthmanifesto.eu/

Цифрове громадянство та електронна демократія

- Електронна демократія включає використання електронних комунікаційних технологій, зокрема Інтернету, для посилення демократичних процесів у демократичній республіці або державі з представницьким демократичним устроєм. Це політичний процес, який посилюється завдяки використанню соціальних мереж, які дозволяють користувачам висловлювати власні думки та надавати «публічні» коментарі з актуальних питань. Одна з теорій полягає в тому, що використання соціальних мереж в межах електронної демократії може забезпечити більш широкий вплив на результати політики, оскільки більша кількість залучених осіб може генерувати більш доцільний політичний курс та підвищити прозорість і підзвітність.
- У наш час політики багатьох країн використовують сайти соціальних мереж, щоб взаємодіяти з молоддю та дізнаватися її погляди. Ця теза заперечується деякими авторами, але ми вважаємо, що важливо йти туди, де перебуває молодь, щоб домогтися контакту з нею.
- Однією з проблем електронної демократії є вплив цифрового розриву на тих, хто не може отримати доступ до носіїв інформації. Однак, оскільки люди різного віку дедалі більше отримують доступ до Інтернету, цифровий розрив сам по собі не слід розглядати як аргумент на користь невизнання переваг сайтів соціальних мереж для електронної демократії.
- В офлайн-спілкуванні влада часто розглядається як ієрархічне явище, тоді як онлайн вона стає розпорошеною, а її носії постійно змінюються. Подібним чином, онлайн-межі стають проникними, ролі учасників є гнучкими, мінливими і не спираються на невербальні характеристики або ієрархію. Самих цих причин достатньо, щоб проілюструвати переваги використання сайтів соціальних мереж для просування електронної демократії.
- Однак якщо ми хочемо, щоб електронна демократія мала позитивні наслідки, користувачі повинні бути відкритими для ненасильницької комунікації та суперечливих поглядів і бути готовими взяти участь у спокійному обговоренні за умов взаємної поваги. Коли спільноти однодумців формуються та обговорюють проблеми, не враховуючи інших точок зору, це може послабити, а не посилити електронну демократію, і навіть призвести до радикалізації поглядів.

ЗНАЧЕННЯ ДЛЯ ОСВІТИ

- Інтернет дає можливість не тільки швидше публікувати набагато більше інформації, але й постійно оновлювати цю інформацію, щоб громадяни отримували інформацію про останні події у своїх сферах інтересів.
- Право на інформацію та право на участь – це права, які визнаються за всіма дітьми відповідно до статей 13 та 17 Конвенції ООН про права дитини.
- Раніше ми мусили покладатися на ті версії заяв та подій, які преса вирішила опублікувати, щоб поінформувати нас про це; в наш час ми дуже часто можемо звернутися безпосередньо до джерела, щоб отримати інформацію з перших вуст.
- У наш час, коли громадяни у всьому світі стають «повсякденними журналістами» завдяки своїм смартфонам із підтримкою відео, ми часто завалені «прямоефірними» сценами, що розгортаються на наших очах. Здатність уважно вивчати те, що представлено на відео, і те, що відбувалося до і після початку зйомки, часто відсутня в такій повсякденній журналістиці, про що свідчать стрічки Twitter, відео YouTube, потокові трансляції Vine та інші платформи соціальних медіа.
- Той факт, що громадяни краще поінформовані, дає їм змогу брати якіснішу участь у демократичному житті як власної країни, так і в загальноєвропейському та міжнародному масштабі, і громадяни здатні використовувати Інтернет, щоб віднайти неупереджений погляд на подробиці більшості питань.
- Географічна, транспортна, культурна та туристична інформація, що збирається державними та приватними організаціями, значно збагачує життя громадян. У деяких країнах громадяни можуть навіть скористатися Інтернетом, щоб офіційно змінити адресу, подати заявку на поновлення паспорта або здійснити різні інші дії, на які раніше витрачалося багато часу. Однак не забувайте, що під час розкриття приватної інформації онлайн слід дотримуватися певних заходів безпеки (див. Інформаційні матеріали 9 щодо конфіденційності та 19 щодо безпеки).

- Інтернет також дозволяє громадянам брати участь в онлайн-обговореннях і дебатах на теми, що становлять інтерес для суспільства чи місцевої громади, і навіть брати участь у виборах шляхом електронного голосування[15].
- Громадяни можуть робити покупки і навчатися онлайн (див. Інформаційний матеріал 12 про дистанційне навчання), брати участь у культурних дискусіях, медитувати, займатися йогою – майже будь-який вид діяльності доступний онлайн.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

Отримуючи доступ до постійно оновлюваної, якісної інформації, громадяни мають кращі можливості для реалізації своїх основних прав людини. Однак ми повинні й надалі з обережністю ставитися до негативних наслідків, які технологія може мати для цих прав, зокрема:

- не всі мають рівний доступ до інформації. Поняття цифрового розриву характеризує сьогоднішнє дворівневе суспільство та розрив між інформаційними «багачами» й «бідняками». Якщо таке становище триватиме, демократії буде загрожувати небезпека, оскільки ті, кому пощастило менше, поступово втрачатимуть можливість самостійно висловлювати свої думки. Коли ми не маємо прямого доступу до інформації, ми менш здатні формувати власну думку, і тому тим, хто вільно користується новими технологіями, легше маніпулювати нами. Крім того, інформація від державних установ дуже важлива для демократичного та громадянського життя, особливо важлива вона тому, що є ключовим ресурсом для економічної діяльності. Якщо ми хочемо забезпечити рівні можливості для всіх, тоді нам потрібно забезпечити для всіх рівний доступ до інформації та надійну підготовку з критичного мислення;
- сучасні технології та онлайн-платформи не обов'язково нейтральні, коли справа стосується доступу до інформації. Алгоритми, використовувані пошуковими системами, або цензура в соціальних мережах формують ту інформацію, яку виставляють напоказ;
- інформаційно-комунікаційні технології відіграють сьогодні настільки важливу роль у нашому житті, що незабаром лише ті, хто вільно користується ними, зможуть бути почутими. Однак ІКТ самі по собі є лише технічними засобами, і більш інтенсивне спілкування не означає поваги до свободи вираження поглядів. Такі цінності, як спокійне обговорення та мовлення, критичне мислення та відкритість, є надзвичайно важливими для формування позитивного онлайн-середовища та просування свободи вираження поглядів;
- величезне зростання потужності засобів передачі інформації та обміну інформацією означає, що ми повинні подбати про захист даних про себе, а отже, і про своє право на конфіденційність (див. розділ «Належна практика» нижче).

ЯК ЦЕ РОБИТИ

- Щоб стати активними електронними громадянами, всі інтернет-користувачі повинні розуміти свої основні права та обов'язки. Користувачі повинні розуміти, що їм дозволяється робити, а також те, що дозволяється робити підприємствам цієї галузі, урядам та іншим інтернет-користувачам.
- Необхідним є принципове розуміння кукі-файлів та того, як інші вебсайти можуть збирати та використовувати ваші персональні дані (див. Інформаційний матеріал 9 щодо конфіденційності).
- Щоб уникнути надмірного ускладнення цих питань для маленьких дітей, ті ж основні принципи доброго громадянства слід просто поширити на онлайн-діяльність: повагу, доброту та схильність думати, перш ніж діяти.

15. https://en.wikipedia.org/wiki/Electronic_voting

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Доручіть учням переглянути Конвенцію ООН про права дитини та проаналізувати, які розділи безпосередньо стосуються цифрових прав[16].
- Попросіть учнів обрати кілька доповідачів, які виступатимуть на тему громадянства на Twitter, Facebook та/або Periscope, та взяти участь в дискусії. Запитайте доповідачів, яка їхня точка зору щодо цифрового громадянства та відповідальності користувачів. Попросіть учнів розробити інші запитання.
- Учні повинні отримати доступ до європейських вебсайтів, що пропонують інформацію щодо цифрових прав. Попросіть учнів скласти огляд позиції Ради Європи та Європейської комісії щодо європейських цифрових прав.
- Серед хороших ресурсів, які можуть бути основою для вашої навчальної програми з громадянського виховання, слід назвати програму онлайн-заходів Ради Європи з питань прав людини[17]. Ви також можете попросити свій клас скласти власну хартію прав людини. Нехай вони застосують свої нові знання про права людини до віртуального середовища, наприклад, покажуть, як вони можуть зробити Інтернет кращим місцем для своєї роботи та ігор.
- У рамках програми з історії, що розповідає про Французьку революцію, допоможіть своїм учням відрізнити факти від гіпотез, порівнявши героїчні революційні картини, що зображають штурм Бастилії, та сучасні розповіді про цю подію. Вони повинні бути здатні «пояснити, як і чому штурм Бастилії трактувався по-різному». Це може бути пов'язано з поняттями зі сфери медіаосвіти, наприклад, представлення реальності для різних цілей та достовірність інформації.
- У рамках якогось географічного проєкту, наприклад, «Паспорт у світ», запропонуйте учням обговорити способи представлення різних місць світу в Інтернеті та проаналізувати, як вебсайти відрізняються за акцентами розповіді чи ставленням до певного місця.
- Щоб допомогти учням дізнатися про контент-аналіз, оберіть тему, а потім знайдіть її на сайтах новин з різних джерел та проаналізуйте їх на уроці. Чи застосовують різні організації різні підходи? Як ви думаєте, чому це так?
- Оскільки мобільні телефони є невід'ємною частиною життя учнів поза класом, розберіть на уроці, як їх можна використовувати для збору інформації про громаду та активної участі в демократичному процесі. Перелічіть послуги, які вони удоступнюють, та обговоріть їх вплив на конфіденційність та демократію (див. інформацію про мобільні послуги в Інформаційному матеріалі 5 «Інтернет на ходу»).
- Імітуйте онлайн-дебати, розмістивши повідомлення на дошці та роздавши учням стикери для нотаток. Кожному учневі буде присвоєно номер і він зможе підійти та прочитати допис після встановленої кількості хвилин, що відповідає його номеру. Після прочитання первинного допису та заслуховування коментарів, якщо такі надійдуть, учням буде дозволено писати та розміщувати власні коментарі та стежити за обговоренням, щоб «відповідати» на інші дописи. Учні також матимуть можливість «підтримати» допис від іншого учня, який буде розміщено в помітнішому місці біля первинного допису. Ця вправа спрямована на те, щоб навчити учнів, чим онлайн-дебати відрізняються від дебатів у реальному житті, а також навчає «свободи вираження поглядів» та уникнення скочування до флейму чи іншої неприйнятної поведінки онлайн.

16. http://web.archive.org/web/20160501101507/http://blogs.lse.ac.uk/mediapolicyproject/2014/09/12/sonia-livingstone-digital-media-and-chil- drens-rights
17. https://www.coe.int/t/dg4/youth/Training/Training_courses/HRE_Youth_Programme_en.asp

НАЛЕЖНА ПРАКТИКА

- Кожен громадянин має право контролювати власні персональні дані, і для цього треба знати, яку особисту інформацію про нього зібрано. Загальний регламент про захист даних був введений в Європейському Союзі у 2016 році частково саме для того, щоб допомогти громадянам реалізувати ці та інші основні права, пов'язані з конфіденційністю та захистом даних[18]. Ключові моменти для громадян викладені в прес-релізі Європейської комісії від 15 грудня 2015 року[19].
- Завжди читайте повідомлення дрібним шрифтом у анкетах, щоб побачити, як буде використана інформація, яку ви надаєте про себе, і не забудьте ознайомитися з Інформаційним матеріалом 9 щодо конфіденційності, щоб отримати додаткові поради.
- Поширення навичок грамотності та їх передача протягом шкільного навчання, під час здобуття вищої освіти та у процесі діяльності громадянського суспільства є надзвичайно важливими для збільшення участі громадян у демократичному процесі.
- Подумайте, чи не варто вам пройти онлайн-курс із цифрового громадянства або цифрових прав.
- На цей момент низка шкіл працює над програмами користування Інтернетом, і метою цього є забезпечити, щоб у їхніх учнів формувалися навички, необхідні для життя, роботи та гри в сучасному інформаційному суспільстві. До них належать:
  - навички орієнтування в лабіринті інформації, доступної в Інтернеті;
  - формування здатності розрізняти інформацію та дезінформацію;
  - аналіз інформації щодо її актуальності та дійсності;
  - розуміння етичних наслідків онлайн-інструментів для демократії;
  - використання інформації в проєктному навчанні;
  - розуміння та використання численних можливостей, які можуть запропонувати браузер та Інтернет.

ДОДАТКОВА ІНФОРМАЦІЯ

- Інформація про Загальний регламент щодо захисту даних: *<http://ec.europa.eu/justice/data-protection/reform/index_en.htm>*.
- Молодіжний маніфест ЄС є онлайн-«декларацією» європейської молоді про те, як зробити Інтернет кращим: *<http://www.youthmanifesto.eu>*.
- Більше інформації про європейські цифрові права: *<https://edri.org>*.
- Amnesty International at *<http://www.amnesty.org/>* та Human Rights Watch *<http://www.hrw.org/>* є неурядовими організаціями, які борються за дотримання прав людини. Amnesty створила багатомовний посібник для вчителів «Перші кроки», призначений допомогти молодим людям дізнатися про права людини, особливо в Центральній та Східній Європі.
- Європейська комісія має інформацію щодо захисту дітей та людської гідності під час надання аудіовізуальних послуг: *<http://ec.europa.eu/avpolicy/index_en.htm>*.
- Більше інформації про права дітей можна знайти в Конвенції ООН про права дитини: *<http://www.ohchr.org/en/professionalinterest/pages/crc.aspx>*.
- Кодекс онлайн-прав ЄС – це базовий набір прав та принципів, закріплених у законодавстві ЄС, які захищають громадян під час доступу до онлайн-мереж та послуг, їх використання: *<https://ec.europa. eu/digital-agenda/en/code-eu-online-rights>*.

18. http://ec.europa.eu/justice/data-protection/reform/index_en.htm
19. http://europa.eu/rapid/press-release_IP-15-6321_en.htm

- Дев'ять елементів цифрового громадянства див. за адресою: *<http://www.digitalcitizenship.net/Nine_Elements.html>*.
- Паризька декларація, прийнята Європейською Комісією та Європейською Радою Міністрів у 2015 році, просуває громадянську активність та спільні цінності свободи, толерантності, недискримінації й інклюзії через освіту: *<http://ec.europa.eu/education/library/study/2016/neset-education-tolerance-2016_en.pdf>*.
- Відповідні документи Ради Європи включають «Права людини для інтернет-користувачів»: *<http://www.coe.int/en/web/internet-users-rights/guide>* (ключові теми нижче):
  - доступ та недискримінація;
  - свобода вираження поглядів та інформації;
  - свобода зборів, асоціацій та участі;
  - конфіденційність і захист даних;
  - освіта та грамотність;
  - діти та молодь;
  - ефективні засоби правового захисту та компенсації.

Інформаційний матеріал 18

Цифрове батьківство: позитивне та ініціативне

«Цифрові аборигени» – це діти, які народилися в цифрову епоху, епоху інформаційних технологій. Це діти, які, потримавши планшет або смартфон лише кілька хвилин, не відчувають страху чи трепету під час роботи з ними. Вони гортають, стискають і тикають, не завжди розуміючи, що вони роблять, але з упевненістю, що щось відбувається на екрані. За словами Марка Пренскі, «сьогодні всі наші учні є «носіями» цифрової мови комп'ютерів, відеоігор та Інтернету» (Prensky, M. (2001) «Digital Natives, Digital Immigrants Part 1» [Пренскі, М. (2001) «Цифрові аборигени, цифрові іммігранти». Ч. 1] On the Horizon 9(5) pp. 1-6, 1. Доступно за адресою: *<http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>).*

«Цифрові іммігранти» – це люди, які народились до появи сучасних технологій. Ця фраза також була придумана Пренскі у 2001 році і використана для опису покоління людей, які виросли не в цифрову епоху. Пренскі зазначає: «Ті з нас, хто не народилися в цифровому світі, але в якийсь пізній момент свого життя захопилися новою технологією та прийняли багато або більшість аспектів нової технології, є і завжди будуть у порівнянні з ними цифровими іммігрантами» (Prensky

(2001), 1-2 *<http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>*).

«Цифрове батьківство» – це ідея допомоги «цифровим батькам-іммігрантам» у розумінні того, що роблять їхні «діти-цифрові аборигени» сьогодні. Єдиною метою цього є захистити дітей, розширити можливості батьків та підтримувати відкрите спілкування між обома сторонами.

Цифрове батьківство включає:

- відкрите спілкування з дитиною щодо ризиків та переваг Інтернету;
- регулярне залучення до інтернет-діяльності дитини;
- активний захист цифрової репутації та цифрової ідентичності дитини;
- вивчення разом із дитиною можливостей, які може запропонувати Інтернет;
- захист дитини від небезпек, які може становити Інтернет;
- перенесення навичок офлайн-батьківства у онлайн-світ.

Позитивне батьківство включає:

- забезпечення наявності позитивної дисципліни та позитивного керівництва в житті дитини;
- виховання дитини без суворості, але так, щоб вона гарно поводилась;
- навчання дітей з раннього віку, як поводитися належним чином, через демонстрацію їм негативних наслідків «поганої» поведінки та переваг від «добрих» учинків;
- ясність у вимогах до дітей;
- визначення конкретних та відповідних ситуації меж;
- послідовність у всьому.

Явно видно, що ці якості перетинаються, оскільки цифрові батьки та опікуни потребують усіх доступних інструментів, щоб бути ініціативними, позитивними та забезпечити відповідальне користування з боку дитини пристроями з підтримкою Інтернету та Wi-Fi.

ЗНАЧЕННЯ ДЛЯ РОЗУМІННЯ ПРОБЛЕМ

- Через всюдисущість Інтернету, мобільних телефонів та пристроїв, підключених до Wi-Fi, батьки можуть відчувати безпомічність через відсутність конкретних технічних знань та досвіду. А тих батьків, які «підковані в техніці», турбує швидкість, з якою їхні діти засвоюють Інтернет та інформаційні технології.
- Батьки можуть не розуміти, як поводитися з дітьми, які проводять години, граючи в Minecraft, коли проводять ніч у друзів, або як установити обмеження для 17-річного підлітка щодо текстових повідомлень вечорами, а також чи використовувати програму для навчання 2-річної дитини користуванню горщиком. Таких питань нескінченно багато, оскільки технологія рухається вперед, а пристрої стають більш оптимізованими та технічно складними.
- Враховуючи зміни сімейних структур батьки можуть відчувати труднощі з дотриманням однакових правил щодо інформаційних технологій у домі свого партнера, будинку бабусі чи в якомусь іншому сімейному середовищі.
- Із урахуванням розвитку технологій дослідження проблем розвитку дітей та наслідків користування онлайн-пристроями також просуваються, але довгострокові результати стануть доступні лише за кілька років.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Перші результати дослідження продемонстрували, що використання смартфона або пристрою для «заспокоєння» дітей може перешкоджати розвитку їхньої здатності до саморегуляції[1].
- Виховання дитини сьогодні одночасно включає виховання відповідального цифрового громадянина, оскільки діти повинні знати, як безпечно та розумно користуватися Інтернетом та сучасними технологіями.
- Батьки повинні допомогти своїй дитині засвоїти цифрову грамотність: вміння добре використовувати інформацію, вміння ефективно використовувати носії інформації й цифрові технології та розвиток цифрового громадянства.
- Цифровий світ та Інтернет також мають глибокий вплив на офлайнове батьківство. Уявлення про онлайновий світ як щось окреме від офлайнового є помилковим. Завдяки безмежним можливостям, що їх пропонує онлайн-світ, діти можуть зіткнутися з певним контентом або досвідом на більш ранній стадії, ніж це було б в офлайн-світі. Сюди входить «позитивний» контент: раннє навчання читати, навчання музиці, «контакт» із іноземною мовою тощо. У той же час діти можуть також зіткнутися з відвертим сексуальним контентом, насильством, страхом, цькуванням тощо.
- Остерігайтеся комерційної сторони Інтернету. Більшість «безкоштовних» онлайн-сервісів покладаються на непрозорі бізнес-моделі та структуру витрат або використання персональних даних для реклами. Наприклад, деякі умовно-безкоштовні ігри спонукають вашу дитину витрачати багато грошей на просування в грі, тоді як «рекламні ігри» стирають межу між грою та рекламою, приховано асоціюючи товар чи бренд із чимось всередині гри.
- Що стосується дев'яти елементів цифрового громадянства, див. «Цифрове громадянство: належне використання технологій»[2] і прочитайте Інформаційний матеріал 17 про цифрове громадянство.
- Результати нещодавніх досліджень Спільного дослідницького центру Європейської Комісії з питань використання сучасних технологій сім'ями з малими дітьми, допомагають зрозуміти проблеми та ризики[3].
- Сайт EU Kids Online тепер систематично повідомляє у своєму блозі з питань батьківства про те, що непокоїть батьків по всій Європі[4].

ЯК ЦЕ РОБИТИ

- Будьте взірцем для своїх дітей і обмежуйте власне використання сучасних технологій.
- Будьте в курсі останніх проблем онлайн-світу та обговорюйте онлайн-діяльність своїх дітей.
- Поговоріть із працівниками школою своїх дітей, щоб визначити, чи є там програма онлайн-безпеки.
- Будьте обережні, вилучаючи пристрої у вашого підлітка в якості дисциплінарного заходу, оскільки це може мати непередбачені наслідки, ізолюючи дитину від її соціальних зв'язків та мереж.
- Поговоріть з іншими батьками, щоб зібрати належні практики для кожного віку.
- Щоб навчити своїх дітей балансувати час, який проводиться онлайн, використовуйте обмеження онлайн-часу так само, як ви навчали б їх контролювати витрачання кишенькових грошей. Визначте для них певний час, який вони можуть «витратити» щотижня, і нехай вони самі управляють ним.
- Підкресліть важливість проведення сімейного часу офлайн та продовжуйте проводити щотижневі сімейні заходи.

1. http://web.archive.org/web/20160424230408/https://www.theguardian.com/technology/2015/feb/01/toddler-brains-research-smart phones-damage-so- cial-development
2. http://www.digitalcitizenship.net/Nine_Elements.html
3. http://publications.jrc.ec.europa.eu/repository/handle/JRC93239
4. http://web.archive.org/web/20160415215157/http://blogs.lse.ac.uk/parenting4digitalfuture/2015/06/26/svenjas-post-on-little-kids-european-comparison/

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Попросіть учнів написати короткий допис для своїх батьків із порадами щодо батьківства в цифрову епоху.
- Проведіть обговорення з учнями щодо використання інформаційних технологій у наш час. Які переваги воно надає? Які ризики? Чи можуть учні щось зробити для просування його переваг та протидії ризикам?
- Після обговорення належних практик користування Інтернетом попросіть учнів назвати найкращі поради, якими вони могли б поділитися зі своїми молодшими братами та сестрами, племінницями, племінниками чи молодшими сусідами. Чому діти молодшого віку можуть навчитися з досвіду учнів?
- Попросіть учнів розглянути технології 1960-х років та сучасні технології. Чи були причини занепокоєння батьків такими ж самими? Чому?

НАЛЕЖНА ПРАКТИКА

- Поговоріть зі своїми дітьми про те, з ким вони спілкуються онлайн, що вони роблять онлайн, які місця вони відвідують онлайн та коли вони це роблять.
- Підтримуйте діалог, навіть тоді, коли його тема може бути для вас незручною, оскільки це найкращий спосіб залишатися в курсі онлайн-діяльності вашої дитини.
- Разом із розмовами зі своїми дітьми про «безпечний секс» розгляньте можливість проведення з ними розмови про «безпечні технології» та «безпечний контент» у Інтернеті, а також поясніть недоречність та ризики сексуальних або екстремістських фотографій, розмов чи повідомлень.
- Будьте готові обговорити такі питання, як насильство, флеймінг, цькування, сексуальність, гендерні стереотипи та ролі, оскільки ваші діти можуть несподівано зіткнутися з ними онлайн, і їм знадобляться ваші вказівки для формування стійкості та реагування через позитивну онлайн-поведінку.
- Розберіться, як користуватися налаштуваннями конфіденційності, та поясніть дитині, як їх встановлювати та чому це корисно робити.
- Довідайтеся про бізнес-модель, яка лежить у основі ігор, сервісів чи вебсайтів, якими користується ваша дитина. Для дітей молодшого віку переконайтеся, що пропонований їм контент не містить реклами, прихованих витрат чи платних функцій. Краще внести невелику плату за гру або щомісячну підписку на якісний сервіс, ніж піддавати свою дитину спробам комерційної експлуатації.
- Переконайтесь, що ваші діти розуміють бізнес-моделі, що стоять за сервісами чи іграми, якими вони користуються, або за контентом, який вони читають.
- Переконайтеся, що ваша дитина не поширює того, що не варто поширювати (особиста інформація, характеристики, за якими можна ідентифікувати особу, неприйнятні фотографії тощо).
- Знайдіть здоровий баланс щодо користування Інтернетом і часу, який проводиться біля екранів, і будьте самі зразком правильної цифрової поведінки.
- Нагадуйте своїм дітям, що все, що вони пишуть, публікують або поширюють, буде існувати нескінченно довго в Інтернеті – і що його також можна змінювати та надсилати різним адресатам.
- Навчіть своїх дітей як користуватися інструментами повідомлення про порушення, щоб вони могли повідомити про будь-який неприйнятний контент.

Додаткова інформація

- Інформацію про вплив iPad на розвиток дитини див. у випуску новин: *<https://www.youtube.com/watch?v=VrQhmcPrhFw>*.
- Щоб прочитати статтю Марка Пренскі «Цифрові аборигени, цифрові іммігранти» (2001), див.: *<http://web.archive. org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20 Natives,%20Digital%20Immigrants%20-%20Part1.pdf>*.
- COFACE, Європейська конфедерація сімей, що надає корисну інформацію для сімей: *<http://www.coface-eu.org/>*.
- The Parent Zone – це британський вебсайт, який пропонує безліч інформації: *<http://www.theparentzone.co.uk/>*.
- Перегляньте це видання Інституту сімейної онлайн-безпеки: *<https://www.fosi.org/good-digital-parenting/>*.
- Vodafone випускає рекомендації для батьків, а також журнали з питань цифрового батьківства: *<https://www.vodafone.com/content/parents/howto-guides.html>*.
- Медичний центр Бостонського університету опублікував доповідь про використання мобільних пристроїв: *<http://web.archive.org/web/20160607121811/http://www.eurekalert.org/pub_releases/2015-01/bumc- mai013015.php>*.
- Спільний дослідницький центр Європейської комісії опублікував доповідь про маленьких дітей та цифрові технології: *<http://publications.jrc.ec.europa.eu/repository/handle/JRC93239>.*
- Програма «Грай і вчись: перебування онлайн» містить заходи для 4-8-річних дітей, які допоможуть батькам та вчителям у розмові з дітьми про відповідальне користування Інтернетом: *<https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=198308>*.
- Укажіть маленьким дітям дорогу на сайти, пристосовані до їх віку; таких сайтів досить багато, й до них належать, зокрема, Junior: safe search for kids *<https://www.juniorsafesearch.com/>* та YouTube Kids *<https://kids.youtube.com/>*.
- Відповідні документи Ради Європи розміщено на вебсторінці Ради Європи на тему «Діти в цифровому середовищі» *<http://www.coe.int/en/web/children/the-digital-environment>*.

5. Інтернет – реакція на виклик

> «Відмовляти людям у правах людини означає ставити під сумнів їх людський статус»
>
> *Нельсон Мандела, лауреат Нобелівської премії миру 1993 року, активіст боротьби проти апартеїду, Президент Південно-Африканської Республіки в 1994-1999 роках*

> «Права кожної людини зменшуються, коли під загрозою опиняються права хоч однієї людини»
>
> *Джон Кеннеді, Президент США в 1961-1963 роках*

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 19 – КІБЕРЗЛОЧИННІСТЬ: СПАМ, ШКІДЛИВІ ПРОГРАМИ, ШАХРАЙСТВО ТА БЕЗПЕКА

Чи встановили ви надійні різні паролі для своїх облікових записів та чи налаштували дворівневу систему безпеки? Чи вивчали ви налаштування безпеки своїх пристроїв/облікових записів?
Чи оновлені ваша операційна система та програми? Чи зробили ви резервну копію своїх найважливіших даних?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 20 – МАРКУВАННЯ ТА ФІЛЬТРУВАННЯ

Чи замислювались ви про культурні та моральні наслідки фільтрування? Чи знаєте ви про різницю між «чорним списком» і «білим списком»?
Чи знайомі ви з найчастіше використовуваними системами маркування дитячого контенту та тим, що вони означають?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 21 – ОНЛАЙН-ПЕРЕСЛІДУВАННЯ: ЦЬКУВАННЯ, СТЕЖЕННЯ ТА ТРОЛІНГ

Чи є у вас чітка сімейна чи шкільна політика, щоб діти розуміли наслідки своєї участі в онлайн-цькуванні?
Чи достатньо ви захищаєте свої персональні дані? Багато онлайн-проблем виникають через необдуманий обмін фотографіями та інформацією.
Чи вивчали ви, як розвинути кращі соціальні та емоційні навички (інакше їх називають соціальною грамотністю), щоб подолати анонімність та «безликість» онлайн-спілкування, що полегшує цькування, тролінг та загалом переслідування?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 22 – ЯК ОТРИМАТИ ДОПОМОГУ

Чи знаєте ви та ваші діти/учні, куди повідомляти про протизаконний контент?
Чи переглядаєте ви коли-небудь статистику, яку повідомляють служби довіри, щоб зрозуміти нові тенденції та ризики? Які п’ять цифрових навичок найкраще захистять вас онлайн?
Чи розумієте ви технології геолокації та Bluetooth достатньо, щоб комфортно та безпечно користуватися мобільними пристроями?
Мобільне навчання та мобільні гаманці – це сфери, в яких використання мобільних пристроїв змінює способи нашого навчання, роботи та покупок. Що ви знаєте про ці нещодавні зміни?

Інформаційний матеріал 19

Кіберзлочинність: спам, шкідливі програми, шахрайство, безпека

Хоча Інтернет є чудовим способом отримати доступ до якісного контенту та послуг, він також може служити цілям недоброзичливих людей, які розповсюджують через нього спам, віруси, шкідливі програми та шахрайські повідомлення.

- **Кіберзлочинність** включає злочини з незаконним використанням комп'ютерів та даних, наприклад, незаконний доступ до комп'ютера (також зване хакерство), перехоплення повідомлень, перешкоджання функціонуванню комп'ютера або пошкодження чи видалення даних, а також злочини, скоєні за допомогою комп'ютерів: шахрайство або сексуальне насильство проти дітей. Шкідливі програми, спам, фішинг та інші форми викрадення персональних даних – це лише деякі з інструментів, якими користуються кіберзлочинці.
- **Шкідливі програми**[1] – загальний термін, що використовується для позначення різноманітних форм ворожих чи інтрузивних програм, що включають віруси, трояни та інше. Цілі шкідливих програм бувають дуже різноманітні. Вони можуть ставити за мету просто порушити роботу вашого комп'ютера, пошкодивши програмне забезпечення чи зіпсувавши апаратне забезпечення, або вони можуть викрасти інформацію та дані, які якимось чином можуть бути монетизовані.

1. https://en.wikipedia.org/wiki/Malware

Ваш заражений комп'ютер також може стати «ботом» (роботом), яким без вашого відома керують злочинці; потім він може бути використаний разом із мільйонами інших заражених комп'ютерів як частина «бот-мережі» для розповсюдження спаму, вчинення шахрайства або здійснення атак на лікарні, аеропорти чи банки.

- **Спам**[2] означає масову розсилку незапитуваного повідомлення численним одержувачам. Його найчастіше пов'язують із електронною поштою, але він застосовується також у соціальних мережах, миттєвих повідомленнях, мобільних телефонах тощо. На щастя, більшість сервісів електронної пошти мають ефективні спам-фільтри. Спам може також служити каналом розповсюдження різних типів шкідливих програм, наприклад, коли одержувач відкриває вкладення або посилання, вказані в спам-листі.
- **Термін «Фішинг»**[3] походить від слів «виловлювання паролів (fishing for passwords)» і є однією з форм крадіжки персональних даних. Наприклад, одержувачі отримують спам, який маскується під справжні листи від відомої установи, наприклад, банку чи соціальної мережі. Ці листи часто містять посилання на підробні вебсайти, які використовуються для збору закритої інформації користувачів, наприклад, номерів кредитних карток або паролів. Потім вкрадена інформація про особу часто використовується для вчинення шахрайства.
- **Інтернет-шахрайство**[4] активно розвинулось за останні кілька років, оскільки можливості електронної комерції та здійснення платежів онлайн суттєво зросли. Інтернет-шахрайство охоплює різні типи шахрайства, такі як підробки, шахрайство з нерухомістю, мелодії дзвінків для СМС преміум-класу, шахрайство з грошовими переказами тощо.

ЯК ЖЕ ВАМ ЗАЛИШАТИСЯ В БЕЗПЕЦІ?

Вашу онлайн-безпеку можна порівняти з безпекою вдома. Ви захищаєте вміст, тримаючи вікна закритими, а двері зачиненими. Здоровий скептицизм, критичне мислення та навички ІКТ також допоможуть вам уникнути перетворення на жертву шахрайства, фішингу, шкідливих програм чи онлайн-шахрайства.

Багато питань, що стосуються безпеки, стосуються і конфіденційності (див. Інформаційний матеріал 9).

ПЕРСОНАЛЬНИЙ РОЗВИТОК ТА ОСВІТНЯ ЦІННІСТЬ

Зберігати безпеку однаково важливо як у ваших власних інтересах, так і в інтересах усіх інтернет-користувачів. Шкідливі програми, віруси та спам поширюються здебільшого через самих користувачів! Якщо ваш комп'ютер або пристрій не убезпечено, всі ваші друзі та контакти також можуть зіткнутися з безпековими ризиками!

Знання про інтернет-безпеку є дуже цінним для подальшого розвитку навичок цифрової грамотності, оскільки воно підштовхує користувачів заглибитися в параметри та налаштування своїх пристроїв та онлайн-сервісів, якими вони користуються, та отримати повніші технічні знання про те, як працюють їхні пристрої, операційні системи та Інтернет.

ПОТЕНЦІЙНІ РИЗИКИ

Спам

- Зазвичай спам є нешкідливим, і його наслідки зводяться здебільшого до великої втрати часу через необхідність пробиратися через нього або витрачати час клікаючи на посилання.
- Спам часто включає неправдиву або шахрайську інформацію. Оскільки відправник залишається анонімним, притягнення його до відповідальності за неправдиві заяви, як правило, неможливе.
- Спамери часто паразитують на добрій волі одержувачів, щоб зібрати поштові адреси для своїх баз даних. Наприклад, вони можуть надсилати листи з проханням до одержувачів додати свою особисту інформацію до списку для підтримки якоїсь петиції чи доброї справи. Часто посилаючись на добру справу, до прикладу, збір грошей для хворої дитини, яка потребує хірургічного втручання, спамер неправдиво стверджує, що якась компанія чи організація пообіцяла, що гроші будуть виплачуватися кожного разу, коли цей лист буде пересилатися.

2. https://en.wikipedia.org/wiki/Spamming
3. https://en.wikipedia.org/wiki/Phishing
4. https://en.wikipedia.org/wiki/internet_fraud

- Щодня з'являються нові прийоми спаму. Наприклад, у соціальних мережах спам може набирати вигляду «піднімання кліків (click jacking)»[5], в ході якого дописи поширюються друзями та містять такі приваблині заголовки, як «10 найкращих способів схуднути» або «Ви не повірите, що робить ця дівчина перед своєю вебкамерою». Як наслідок, ви можете відвідати вебсайт, який завалить вас масою реклами для отримання доходу, або змусить поставити «лайк» сторінці, яка потім надішле вам набагато більше спам-дописів.
- Існує багато видів онлайн-шахрайства, й нові з'являються щодня із розвитком технологій. Поширена шахрайська схема називається «419» на честь нігерійського закону, що забороняє цей вид віктимізації (тобто перетворення користувачів на жертв шахрайства). Зазвичай ця схема передбачає обіцянки виплатити частку від великої суми грошей в обмін на допомогу з банківськими переказами. Ще одна шахрайська схема полягає в тому, щоб попросити потерпілого надіслати гроші через Western Union як завдаток перед відвідуванням квартири, яка здається в оренду.

Фішинг і викрадення персональних даних

- Ризики стати жертвою фішингу та викрадення персональних даних набагато серйозніші. Залежно від того, яку інформацію ви надали під час спроби фішингу, ви можете зазнати найрізноманітнішої шкоди: від втрати контролю над відносно неважливим онлайновим обліковим записом, наприклад: профіль учасника інтернет-форуму, до втрати контролю над надзвичайно важливими обліковими записами, наприклад, вашій основній електронній адресі, що може скомпрометувати всі ваші онлайнові облікові записи!
- Як тільки ваші облікові записи будуть скомпрометовані, ваші дані можуть опинитися під загрозою. Наприклад, можна буде завантажити зміст усіх ваших електронних листів. Ці дані можуть виявитися дуже цінними для вимагання грошей у вас або у знайомих, використання ваших облікових записів онлайн для замовлення речей, використання кредитної картки, видавання себе за вас онлайн тощо.

Шкідливі програми

- Ризики встановлення шкідливих програм подібні до фішингу та навіть спаму, або є ще гіршими. Шкідливі програми можуть використовуватися для фішингових цілей для викрадення інформації про ваші облікові записи (наприклад, за допомогою програми-реєстратора ключів[6]), для спаму, щоб засипати вас спливаючими вікнами, сповіщеннями або головними екранами за замовчуванням у ваших браузерах, а також для інших цілей, наприклад, крадіжка інформації та даних безпосередньо з комп'ютера або порушення функціонування комп'ютера, взяття під контроль комп'ютера для вчинення злочинів, активація мікрофонів чи камер ваших пристроїв для шпигування за вами та потенційне остаточне знищення контенту.
- Методи, спрямовані на введення користувача в оману з тим, щоб спонукати його встановити шкідливі програми, також швидко розвиваються. Прикладом цього може бути фальшиве спливаюче вікно, яке реалістично імітує антивірусну перевірку вашого комп'ютера. Після закінчення фальшивої перевірки на вашому комп'ютері нібито виявлено небезпечні віруси, і щоб позбутися від них, ви повинні встановити якусь програму, яка насправді є шкідливою програмою чи вірусом!

5. https://en.wikipedia.org/wiki/Clickjacking
6. https://en.wikipedia.org/wiki/Keystroke_logging

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Попросіть дітей та молодь працювати в групах по три-чотири особи та запропонувати надійний пароль для умовного онлайнового облікового запису. Дайте ясно зрозуміти, що вони повинні придумати новий пароль, а не розкрити наявний, який вони вже використовують! Попросіть різні команди представити свої паролі і попросіть решту членів груп визначити особливості надійного пароля, переглянувши подані пропозиції.
- Надійний пароль:
  - складається з принаймні восьми знаків;
  - не містить слів, знайдених у словнику, не містить відсилок до вашого особистого життя або вашого імені користувача, справжнього імені чи назви компанії;
  - містить знаки з кожної із наступних категорій: великі і малі літери, цифри та інші символи.
- CERT (computer emergency response team, група реагування на надзвичайні ситуації, пов'язані з комп'ютерами), також відома як CSIRT (computer security incident response team, група реагування на інциденти, пов'язані з комп'ютерною безпекою) – це група експертів, яка ліквідує інциденти, пов'язані з комп'ютерною безпекою. Доручіть своїм учням знайти вашу національну CERT/CSIRT та дізнатися більше про роль і функціонування цих груп.
- Жертви кіберзлочинів часто не повідомляють про злочин поліції, і тому правопорушники продовжують свою справу та знаходять нових жертв.
  - Попросіть своїх учнів дізнатися про те, як повідомити про злочин у поліцію чи інші державні органи, в тому числі за допомогою гарячих ліній.
  - Попросіть своїх учнів з'ясувати, що вважається кіберзлочинами за законами вашої країни.

НАЛЕЖНА ПРАКТИКА

- Одним із наслідків того, що інтернет-користувачі сподіваються отримувати онлайн все безкоштовно, став постійний розвиток шкідливих програм чи спаму, вкладених у «безкоштовні» програми чи сервіси, які використовуються онлайн. Стан інтернет-середовища є предметом спільної відповідальності й результатом індивідуальної поведінки та актів вибору, які користувачі вчиняють онлайн. Надаючи фінансову підтримку якісним сервісам/контенту/програмам (за рахунок пожертв на проєкти розробки з відкритим вихідним кодом або придбання ліцензій чи передплати на продукти комерційних організацій), ви сприяєте підвищенню рівня безпеки онлайн-середовища.
- Зручність користування може бути ворогом безпеки. Наприклад, ви можете налаштувати свою операційну систему так, щоб вона вимагала пароль адміністратора, коли виконується важлива дія (наприклад, установка нового програмного забезпечення). Це може бути надзвичайно неприємно і нудно, але це ціна, яку потрібно заплатити за більшу безпеку! Майте це на увазі під час установлення параметрів безпеки операційної системи.
- Якщо ви керуєте кількома користувачами комп'ютера або мережі, переконайтесь, що кожен користувач має лише відповідні його статусу права. Обмеження непотрібних прав користувачів може допомогти уникнути випадкових або навмисних проблем із безпекою.

- Перш ніж завантажувати щось на свій комп'ютер, переконайтеся, що ви довіряєте джерелу. Будьте особливо обережні із програмним забезпеченням для однорангових мереж[7], що сприяють розповсюдженню шкідливих програм (див. Інформаційний матеріал 14 про музику та зображення). Установлюючи програмне забезпечення, щоразу обов'язково прочитайте всі кроки, перш ніж натискати кнопку «далі». Зверніть особливу увагу на заздалегідь встановлені галочки, які можуть запустити встановлення шкідливих програм на ваш комп'ютер!
- Установіть антивірус[8] та оновлюйте його за потреби.
- Установіть оновлення системи безпеки або оновлення операційної системи, як тільки вони стануть доступними. Ви можете розпорядитись, щоб деякі операційні системи та програми оновлювались автоматично або повідомляли вас, як тільки оновлення стане доступним для завантаження.
- Установіть брандмауер[9], щоб контролювати трафік до вашого комп'ютера та з нього.
- Використовуйте різні облікові записи електронної пошти для різних випадків, щоб уникнути повсякчасного розкриття своєї «особистої» адреси електронної пошти (наприклад, для реєстрації на форумах, заповнення форм тощо) та уникайте широкого розповсюдження своєї електронної адреси. Майте на увазі, що якщо ви вкажете свою адресу електронної пошти на вебсайті, пошукові роботи можуть її помітити та додати до списків розповсюдження спаму. Не слід також відповідати на спам. Таким чином спамер отримає підтвердження вашої адреси електронної пошти. Майте на увазі, що посилання, при натисканні на які вас обіцяють вилучити зі списку розсилки, можуть бути несправжніми.
- Якщо вам потрібно опублікувати свою адресу електронної пошти, ви можете замаскувати її, додавши символи, як-от Tom(крапка)Smith(собака)gmail(крапка)com, або опублікувавши її як зображення, щоб її не вдалося автоматично скопіювати.
- Зберігайте здоровий скептицизм щодо отримуваних вами електронних листів. Не відкривайте електронних листів, якщо ви не довіряєте джерелу. Завжди перевіряйте електронну адресу будь-якого отриманого сповіщення, щоб перевірити, чи справжнє воно.
- Будьте особливо обережні щодо вкладень. Отримавши щось підозріле або те, про що ви не просили, негайно видаліть його, не відкриваючи.
- Ніколи не клікайте на посилання від відправників, яким не довіряєте, а особливо на посилання, які використовують скорочені URL-адреси, де неможливо побачити «оригінальну» URL-адресу. Пам'ятайте, що навіть відправники, яким ви довіряєте, можуть надсилати вам заражені повідомлення, якщо їх обліковий запис або пристрій було скомпрометовано.
- Ніколи не надсилайте та не публікуйте електронною поштою конфіденційну інформацію, наприклад, ім'я користувача та пароль або номер кредитної картки. Жоден онлайн-сервіс ніколи не попросить вас надіслати своє ім'я користувача та пароль електронною поштою, а такими даними, як номер вашої кредитної картки, вас попросять поділитися лише в рідкісних випадках (наприклад, при бронюванні номера в готелі вам може знадобитися надіслати цю інформацію на офіційну електронну адресу готелю).
- Використовуйте різні паролі для своїх найважливіших облікових записів і обов'язково встановлюйте дворівневі заходи безпеки, коли це можливо (додаючи номер свого мобільного телефону або додаткову контрольну фразу/запитання). Переконайтеся, що ваші паролі не мають явного зв'язку з вами, складаються щонайменше з восьми знаків і використовують комбінацію літер (малих та великих), цифр та інших символів.
- Регулярно створюйте резервні копії всіх своїх даних на зовнішньому жорсткому диску. Існує багато програм для резервного копіювання, які автоматично та регулярно створюють резервні копії даних. Деякі з них навіть включені до вашої операційної системи (Windows, MacOS, Linux тощо). Обов'язково залишайтеся в курсі подій[10].

7. https://en.wikipedia.org/wiki/Peer-to-peer
8. https://en.wikipedia.org/wiki/Antivirus_software
9. https://en.wikipedia.org/wiki/Firewall_(computing)
10. ttps://en.wikipedia.org/wiki/List_of_backup_software

ДОДАТКОВА ІНФОРМАЦІЯ

- Truth or Fiction – це вебсайт, на якому інтернет-користувачі можуть перевірити достовірність тверджень, зроблених в електронних листах, що часто пересилаються: *<http://www.truthorfiction.com/>*.
- Більше інформації про боротьбу зі спамом можна отримати тут: <http://spam.abuse.net> та <http://www.spamhelp. org/>.
- Більше інформації про безпеку продуктів Microsoft можна отримати тут: *<http://www.microsoft.com/security/>.*
- Інформацію про безпеку продуктів Apple можна отримати тут: *<http://www.apple.com/support/security/>.*
- ENISA (European Union Agency for Network and Information Security, Агентство Європейського Союзу з питань мережевої та інформаційної безпеки) регулярно представляє оновлену інформацію з питань цифрової безпеки: *<http://enisa.europa.eu>.*
- Рада Європи має вебсторінку під назвою «Дії проти кіберзлочинності»: *<www.coe.int/cybercrime>*.
- TechTarget є журналом з питань інформаційної безпеки: *<http://informationsecurity.techtarget.com/>.*
- Корисну інформацію та тести для користувачів на теми від кукі-файлів до IP-адрес та перевірок браузера можна знайти за адресою: *<http://www.2privacy.com/>*.
- Поради уряду Великої Британії з питань онлайн-безпеки можна знайти за адресою: *<https://www.getsafeonline.org> та уряду США за адресою: <http://www.us-cert.gov/>*.
- Знайдіть свою національну групу реагування на надзвичайні ситуації, пов'язані з комп'ютерами за допомогою пошуку в мережі, вводячи абревіатуру CERT та назву вашої країни.
- Хоча керівні принципи інформаційної безпеки, запропоновані Асоціацією прямого маркетингу (*<http://www.the-dma.org/guidelines/informationsecurity.shtml>*) призначені для учасників ринку прямого маркетингу, вони також містять корисні поради для всіх, кого турбує онлайн-безпека.
- Відповідні статті Конвенції ООН про права дитини:
  Стаття 16 – Діти мають право на приватність. Закон повинен захищати їх від нападок на їхній спосіб життя, їхнє чесне ім'я, їхні сім'ї та їхні домівки.
  Стаття 17 – Діти мають право отримувати достовірну інформацію із засобів масової інформації. Телебачення, радіо та газети повинні надавати інформацію, яку діти можуть зрозуміти, і не повинні просувати матеріали, які можуть завдати шкоди дітям.
  Стаття 34 – Уряд повинен захищати дітей від сексуального насильства.
  Стаття 36 – Дітей слід захищати від будь-якої діяльності, яка може зашкодити їхньому розвитку.

Інформаційний матеріал 20

Маркування та фільтрування

МАРКУВАННЯ

Як маркування, так і фільтрування є методами обмеження доступу до інтернет-контенту: відео, зображень, вебсторінок та ігор. Незважаючи на те, що на ранньому етапі, близько десятиріччя тому, технічні відомства та служби захисту дітей сподівалися створити електронну систему маркування, яку можна було б вбудовувати на вебсайти з метою фільтрації, сьогодні маркування зазвичай має форму символу, видимого неозброєним оком, який означає, що певних конкретних правил або стандартів дотримано. Однак розробка критеріїв для систем знаків довіри та маркування, що дозволять дітям та їхнім сім'ям визначати відповідний віку онлайн-контент, та обмін міжнародною належною практикою у цій галузі продовжує залишатися пріоритетом для Ради Європи, зокрема через Форум із управління Інтернетом, який щороку організовується Організацією Об'єднаних Націй[1]. Маркування вебсайтів є не лише засобом захисту неповнолітніх та підвищення довіри громадськості до використання онлайн-транзакцій, але також заохочує дотримання правових стандартів постачальниками контенту.

1. www.intgovforum.org

PEGI – це європейська система онлайн-маркування, яку підтримує Європейська Комісія, оскільки вона надає вказівки щодо вікових обмежень та типів контенту, який може бути присутнім в іграх та застосунках (див. Інформаційний матеріал 16 про ігри). Вона містить указівки щодо вікових обмежень для ігор, застосунків та деяких видів онлайн-контенту, а також вказує на тип контенту, що міститься в них. Вона також показує, що постачальники контенту дотримуються стандартів якості, які включають, серед іншого, зобов'язання вживати заходів для захисту вебсайтів від протизаконного та образливого контенту, створеного користувачами, та небажаних посилань, захищати конфіденційність та мати незалежний механізм розгляду скарг.

Маркування знаками якості та довіри можна знайти також на сайтах онлайн-покупок та інших онлайн-транзакцій, де вони вказують на дотримання норм і приписів щодо безпечних транзакцій (див. Інформаційний матеріал 13 про онлайн-покупки). Одним із найпоширеніших символів, які ви можете побачити, є значок замка, який вказує на те, що сторінка вебсайту, на якому ви перебуваєте, використовує протокол SSL (рівень захищених з'єднань, стандарт безпеки передачі даних, який шифрує дані та автентифікує сервер і цілісність повідомлення) або протокол TLS (захист транспортного рівня). Відтак ви можете обґрунтовано припустити, що ваші дані, зокрема банківські реквізити, захищені.

ФІЛЬТРУВАННЯ

Під фільтруванням зазвичай розуміють процес виявлення та блокування неприйнятних платформ та/або контенту в Інтернеті. Це можна зробити в браузерах та проксі-програмах, або встановивши програмні цензори, зокрема, батьківський контроль. Фільтри встановлюються відповідно до правил, створених батьками, школами, підприємствами, урядами тощо. Зазвичай вони функціонують як «чорні» списки (контент, який потрібно заблокувати), або «білі» списки (що забороняють доступ до всього інтернет-контенту, крім елементів, схвалених фільтром). Іноді білі списки об'єднуються в рамках програмної системи, в якій надавач комунікаційних послуг або постачальник сервісів контролює застосунки, контент і носії інформації та обмежує зручний доступ до несхвалених застосунків або контенту. Коли така система створена для дітей, її називають «огородженим садом» або «закритою платформою»[2] на відміну від відкритої платформи, де споживачі мають необмежений доступ до застосунків, контенту та багато чого іншого.

Інший метод фільтрування – це введення правил за допомогою ключових слів або термінів, що обмежує або повністю блокує доступ до будь-яких вебсторінок, що містять заборонені слова чи фрази. За допомогою пароля особа, яка встановила правила фільтрування, також може дозволити разовий доступ до сайтів[3].

Сьогодні існують фільтри, які можуть працювати з кількома пристроями одночасно. Фільтрувальну програму чи застосунок можна завантажувати на декілька пристроїв: ноутбук, планшет, смартфон, телевізор або електронну книгу, а також управляти ними централізовано, що можуть робити, наприклад, батьки. Для дітей різного віку можуть бути встановлені різні правила, які можуть автоматично змінюватися з дорослішанням дитини. Правила фільтрування можуть застосовуватися для обмеження часу перебування онлайн та доступу до контактів, а також для моніторингу геолокації та багато чого іншого.

ОСВІТА

- Білі списки особливо цінні, коли діти роблять перші кроки в Інтернеті, дозволяючи їм розпізнавати свої улюблені сайти та швидко отримувати доступ до них. Це не тільки допоможе розвинути в них візуальне розрізнення об'єктів, що є необхідним для підготовки до читання, але також допоможе діяльності в Інтернеті перетворитися на спільну сімейну діяльність, що є найважливішим елементом гарантування безпеки вашої дитини в Інтернеті.
- Фільтрування може бути дуже корисним доповненням до системи захисту неповнолітніх від неприйнятного контенту в Інтернеті або контролю за використанням екранного часу, але воно повинно використовуватися разом із відповідними рекомендаціями батьків, учителів та вихователів дітей.

2. https://en.wikipedia.org/wiki/Closed_platform
3. http://internet-filter-review.toptenreviews.com

- Під час класного заняття фільтри можуть бути корисними для зменшення ризику доступу учнів до неприйнятних або шкідливих матеріалів. Однак це не знімає необхідності перевіряти сайти, які пропонуються учням, перед тим, як давати завдання на основі Інтернету.
- Еталонне дослідження Програми безпечнішого Інтернету (SIP-Bench) показує, що сучасні засоби фільтрування здатні фільтрувати потенційно шкідливий контент без серйозного зменшення можливостей Інтернету для дітей і молоді. Більше можна дізнатися на вебсайті Програми безпечнішого Інтернету [4] .
- Проблеми, порушені під час вивчення методів маркування та фільтрування, багаті матеріалом для тем громадянського виховання та/або соціальних досліджень. Розпочніть дебати на тему онлайн-фільтрування. Чи є воно прийнятною та необхідною формою цензури?

ПРОБЛЕМИ

- Фільтрування контенту може заблокувати доступ до цінної інформації та ресурсів, наприклад, до історії світових війн чи статевого виховання через певні ключові слова, вміщені в них.
- Маркування та рейтингування вебсайтів залишається переважно добровільною практикою, за винятком випадків, коли країни мають закони, що вимагають дотримання певних стандартів. Ми живемо у глобальному світі, і на їх ефективність певною мірою впливає їх обмежене використання постачальниками платформ та контенту й відсутність загальноприйнятих систем маркування та рейтингування.
- Законодавство не встигає за технологічною еволюцією, і сервіси фільтрування все ще переважно позначають сторінки відповідно до своїх власних систем цінностей та суспільних цілей.
- Важко вирішити, який контент насправді шкідливий для дітей певного віку, хто повинен ухвалювати рішення щодо загальних правил, яких повинні дотримуватися постачальники контенту, а хто повинен ухвалювати рішення щодо застосування цих правил. Тому інструменти фільтрування повинні бути дуже гнучкими, щоб дозволити особам, які виховують дітей, формувати правила фільтрування відповідно до сімейних цінностей. Постачальники фільтрів повинні розробити методи, щоб забезпечити відповідність фільтрування цим критеріям.
- Фільтри також можуть стати інструментом цензури, використовуваним для формування громадської думки та придушення політичного інакодумства. Деякі країни блокують сайти опозиційних політичних партій чи ідеологій. Це може бути цікавою відправною точкою для обговорення прав людини та демократії на уроці.
- Деякі люди вважають фільтрування формою цензури і, отже, таким, що суперечить духу Інтернету. Інші стверджують, що якби не існувало програмного забезпечення для фільтрування, на уряди чинився б тиск, щоб змусити їх регулювати онлайн-контент.
- Постачальники програмного забезпечення для фільтрування намагаються не відставати від розвитку соціальних мереж, мобільних пристроїв та використання Інтернету дедалі молодшими дітьми.
- Тривають міжнародні дискусії щодо створення домену .kids для заміни .org, .com та подібних доменів для сайтів, пристосованих для дітей, щоб захистити їх від такого онлайн-контенту, який може бути потенційно шкідливим, зловмисним чи неприйнятним. Оскільки сайти, що використовуватимуть доменне ім'я .kids, муситимуть дотримуватися вказівок, отриманих під час реєстрації, пов'язані з цим численні проблеми включають встановлення міжнародно прийнятих стандартів, вибір міжнародного агентства з моніторингу тощо.

4. http://www.sipbench.eu

ЯК ЦЕ РОБИТИ

- Якщо ви розробник гри або застосунку й хочете отримати оцінку свого творіння відповідно до національних чи міжнародних стандартів, або один із батьків чи вихователів і просто хочете зрозуміти цей процес, перегляньте відео «Як це робити» на вебсайті Міжнародної коаліції вікових рейтингів (IARC) [5]. Більшість браузерів та операційних систем мають вбудований батьківський контроль, який ви можете налаштувати на фільтрування небажаного контенту. Блог «Як налаштувати недратівливий батьківський контроль на всіх своїх пристроях?» [6] містить інформацію про те, як це зробити в широкому діапазоні пристроїв та програмного забезпечення. У більшості програм фільтрування ви можете вказати, які типи контенту ви хочете фільтрувати чи дозволяти. Однак заздалегідь установлені фільтри можуть не задовольнити всі ваші вимоги, особливо якщо ви хочете встановити різні правила для двох або більше користувачів. Вам потрібно буде придбати спеціальну програму для більш просунутого підходу до фільтрування сайтів та контролю за використанням пристрою. Остання доповідь Програми безпечнішого Інтернету[7] та огляди програмного забезпечення для Інтернету[8] можуть бути корисними при здійсненні вибору з широкого спектру продуктів, доступних на ринку.

НАЛЕЖНА ПРАКТИКА

- Перш ніж встановлювати фільтр, подивіться уважно, як він працює. Чи ухвалює він при фільтруванні якісь ідеологічні чи культурні рішення, з якими ви не погоджуєтесь?
- Використовуйте електронні засоби розбірливо та не вірте рекламі. Оцінюйте заявлені характеристики продукту за власним досвідом. Жоден фільтр ніколи не зможе замінити «фільтр критичного мислення», якого потребують усі інтернет-користувачі незалежно від віку.
- Поговоріть з учнями, батьками та працівниками школи про те, як вони користуються пристроями, та про їхні потреби, й робіть це регулярно. Створення відкритого середовища для обговорень зробить для поліпшення якості перебування ваших учнів в Інтернеті більше, ніж цензура чи полювання на відьом. За рекомендаціями експертів, ключовим елементом сприяння відповідальному дитячому інтернет-користуванню має стати зацікавлення батьків онлайн-діяльністю своїх дітей та проведення з ними часу онлайн.
- Подумайте про використання «білого списку», який дозволяє доступ лише до схвалених сайтів, для наймолодших інтернет-користувачів. Зробіть закладки улюблених та інших дружніх до дітей вебсайтів у своєму браузері, щоб створити особистий список для ваших дітей, за яким вони могли б легко отримати доступ до безпечних сайтів, якими вони вже користувались.
- Слід заохочувати дітей та молодь говорити про неприйнятні матеріали, які вони знаходять в Інтернеті. Підлітки часто стверджують, що однією з головних проблем для них є неможливість поговорити з батьками про моральні проблеми, з якими вони стикаються онлайн. Повідомляйте про потенційно протизаконний контент на гарячу лінію[9].
- Стежте за діяльністю своїх дітей на ігрових вебсайтах та шукайте ярлик PEGI Online, щоб виділити безпечні сайти.
- Дедалі більше інтернет-спільнот покладаються на самих користувачів, які допомагають маркувати контент, особливо коли його створюють самі ж користувачі. Не забудьте промаркувати будь-який контент, який ви вивантажуєте, і допомогти позначити неправильно маркований контент.

5. https://www.globalratings.com
6. http://web.archive.org/web/20160528132556/http://lifehacker.com/5868750/how-do-i-set-up-non-annoying-parental-controls-on-all-my-devices
7. http://www.sipbench.eu/
8. http://internet-filter-review.toptenreviews.com
9. http://www.inhope.org

ДОДАТКОВА ІНФОРМАЦІЯ

- У Вікіпедії є стаття про цензуру в кіберпросторі: *<http://en.wikipedia.org/wiki/Censorship_in_cyberspace>*.
- Вебсайт відділу ЗМІ Ради Європи містить інформацію про його роботу, що сприяє саморегулюванню та розширенню можливостей користувачів: *<http://www.coe.int/media>*. NetNanny за адресою *<http://www.netnanny.com>* та Cyberpatrol за адресою: *<http://www.cyberpatrol.com>* належать до відомих комерційних фільтрів.
- Фонд електронного фронтиру (ФЕФ) має за мету захищати громадянські свободи в Інтернеті: *<http://www.eff.org/>*.
- Проєкт SIP-Bench, що фінансується ЄС, щороку публікує результати порівняльних досліджень фільтрувальних продуктів дев'ятьма мовами: *<http://www.sipbench.eu/>*.
- Дослідження Ради Європи щодо молоді, самопочуття та ризиків онлайн (2006) вивчає значення шкідливого контенту для роботи із захисту дітей та молоді в інформаційному суспільстві: *<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMCon- tent?documentId=0900001680483b30>*.
- Вебсайт системи маркування PEGI Online пропонує інформацію про онлайн-ігри, категорії, ризики, поради щодо безпеки та список маркованих вебсайтів: *<http://www.pegionline.eu>.*
- Рекомендація CM/Rec(2008)6 Комітету міністрів державам-членам про заходи з розвитку поваги до свободи слова та інформації у зв'язку з інтернет-фільтрами: *<https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec(2008)6&Language=lanEn- glish&Ver=original&direct=true>*.
- Відповідні документи Ради Європи для отримання додаткової інформації щодо маркування та фільтрування: *<www.coe.int/en/web/freedom-expression/internet-standard-setting>*.

Інформаційний матеріал 21

Онлайн-переслідування: цькування, стеження та тролінг

З розвитком Інтернету інформаційні технології все ширше проникають у наше життя, те саме роблять люди, які хочуть заподіяти шкоду іншим шляхом.

Згідно із дослідженням 2014 року, проведеним Дослідницьким центром П'ю серед дорослих американців, існує принаймні шість різних форм онлайн-переслідувань: обзивання, докладання зусиль, щоб когось навмисно поставити в незручну ситуацію, фізичні погрози, переслідування протягом тривалого періоду часу, сексуальні домагання або стеження. У цьому ж дослідженні науковці виявили п'ять ключових фактів про онлайн-переслідування:

1. З-поміж опитаних інтернет-користувачів 40% особисто зазнавали онлайн-переслідувань.
2. Із усіх демографічних груп саме молоді люди найчастіше стають жертвами онлайн-переслідування.
3. Чоловіки та жінки мають різний досвід онлайн-переслідування.
4. Половина тих, хто зазнає онлайн-переслідування, не знає, хто за цим стоїть.
5. Найчастіше для переслідування використовуються соцмережі.

Онлайн-переслідування передбачає неодноразове висловлювання зневажливих або образливих коментарів на адресу об'єктів переслідування. Це може набувати різних форм, наприклад: кіберцькування, кіберстеження, тролінг або поширення ненависті.

КІБЕРЦЬКУВАННЯ

- Всесвітня організація охорони здоров'я визнає цькуванням «навмисне використання фізичної та психологічної сили чи влади, як у вигляді погрози, так і насправді, проти самого себе, іншої особи або проти групи чи спільноти, що призводить або з високою ймовірністю може призвести до травмування, смерті, психологічної шкоди, порушень розвитку чи депривації» (Всесвітня організація охорони здоров'я – 2002) World report on violence and health: summary [Глобальна доповідь про насильство та здоров'я: резюме][1].
- Цькування – це дія, яка здійснюється проти іншої особи з метою заподіяння їй шкоди і повторюється у різних формах протягом певного періоду. Батьки та діти зазвичай по-різному уявляють собі масштаби цієї проблеми.
- Цькування може набувати різних форм: фізичне, словесне, сексуальне цькування, агресія у стосунках, цькування через упередження, вимагання та кіберцькування.
- Кіберцькування – це цькування через Інтернет або мобільний телефон, що включає образливі або зловмисні повідомлення, електронні листи, коментарі в чаті чи на форумі, або, в ще гірших випадках, вебсайти, створені з намірами завдати шкоду окремій людині або певним групам людей.
- Учасники кіберцькування використовують мобільні телефони також для того, щоб робити фотографії інших у незручні моменти або надсилати образливі СМС чи ММС-повідомлення. Всі форми онлайн-цькування мають набагато більший вплив, ніж звичайне цькування, оскільки їхні ініціатори відчувають себе сильнішими через почуття анонімності, а жертвам немає де сховатися від ініціатора цькування – вони можуть бути жертвами вдень і вночі практично будь-де.
- Кіберстеження – це використання Інтернету чи інших електронних засобів для стеження за особою, групою чи організацією або для їх переслідування[2].
- Тролінг – це створення проблем у Інтернеті через ініціювання суперечок або виведення людей з рівноваги шляхом публікації провокаційних, побічних або далеких від теми дописів у онлайн- спільноті: групі новин[3] або блозі.
- Тролінг здійснюється з прямим наміром спровокувати читачів на емоційну реакцію або іншим чином порушити нормальну дискусію за темою.[4]
- Оскільки кіберстеження, тролінг та цькування, як правило, розглядаються як складові ширшого явища – онлайн-переслідування, наведені нижче вказівки та інформація можуть бути застосовані до окремих випадків.

ЗНАЧЕННЯ СТІЙКОСТІ ТА СОЦІАЛЬНО-ЕМОЦІЙНОЇ ПІДГОТОВКИ

- Соціальна та емоційна стійкість та хороше самопочуття є вирішальними факторами, які допомагають молодим людям виробити захист від цькування та іншої агресивної онлайн-поведінки.
- Позитивний шкільний клімат або позитивна спільнота можуть пом'якшити наслідки онлайн- та офлайн-цькування, а також онлайн-переслідування у цілому.
- Батьки можуть допомогти своїм дітям розвинути стійкість, допомагаючи їм підвищити свою самосвідомість та самоповагу; показавши їм, що їх приймають і люблять саме такими, якими вони є; навчаючи їх пристосовуватись до складних ситуацій, справлятися з ними та долати їх; надихаючи їх на позитивні емоції, знаходячи задоволення та гумор у житті; шляхом розвитку навичок вирішення проблем; навчаючись бути гнучкими у своїх реакціях; і показуючи їм важливість співпереживання.

1. http://www.who.int/violence_injury_prevention/violence/world_report/en/summary_en.pdf
2. https://en.wikipedia.org/wiki/Cyberstalking
3. https://en.wikipedia.org/wiki/Usenet_newsgroup>, forum, chat room <https://en.wikipedia.org/wiki/Chat_room
4. https://en.wikipedia.org/wiki/Internet_troll

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

- Цькування та переслідування в класі можуть знизити моральний дух усього класу, створюючи атмосферу страху й недовіри та роблячи навчання майже неможливим.
- Для тих, хто зазнає цькування або є жертвами переслідування, наслідки найчастіше включають депресію, тривогу, низьку самооцінку, труднощі соціальної адаптації та самотність.
- Для виконавців цих дій наслідки найчастіше включають підвищену тривожність, ризик невдач у школі, часто також протизаконну поведінку та підвищену ймовірність скоєння злочинів у дорослому віці.
- Одним із заходів запобігання перетворенню цькування чи переслідування на проблему є введення в навчальну програму таких тем: управління соціальними відносинами, управління гнівом та вирішення конфліктів. Добре підібрані програми такого типу дозволять дітям і підліткам розкрити власні таланти як потенційних посередників у конфліктах. Таким чином, ризик дрібних конфліктів, що переростають у загрозливу поведінку, буде зменшено як офлайн, так і онлайн.
- Ваша школа повинна проводити чітку політику – зазвичай її називають політикою прийнятного користування (ППК) або політикою відповідального користування (ПВК) 5 – щоб контролювати, коли і як учні та працівники школи використовують Інтернет, мобільні телефони в школі. Цей документ повинен чітко пояснювати, що вульгарні вислови, словесні залякування чи переслідування не допускаються. Прямі наслідки повинні бути чітко прописані для тих, хто використовує Інтернет або свої мобільні телефони неналежним чином.
- Повинна існувати процедура для документування користування Інтернетом, зокрема визначення хто перебуває онлайн, коли і де, хоча це може спричинити деякі проблеми у сфері захисту даних.
- Учнів слід проінструктувати припинити контакти з будь-ким, хто переслідує їх або робить їхнє онлайн-перебування якимось чином неприємним.
- Учні повинні негайно розповісти про те, що сталося, дорослому, якому вони довіряють, і за можливості показати йому образливий матеріал. Тоді дорослий повинен діяти за процедурою, прописаною в шкільній ППК або ПВК.
- Ця процедура така ж, як і та, яку застосували б у реальному житті, якби дитину хтось переслідував. Вона повинна припинити контакт із порушником та повідомити дорослому, якому довіряє, про інцидент. Вона не повинна почуватися так, ніби вона сам-на-сам із проблемою або повинна самостійно її подолати.

Таким чином, політика використання Інтернету та мобільних телефонів у школі повинна включати такі методи втручання, як вирішення конфліктів, навчання учнів та працівників тому, що вони мають робити в разі онлайн-переслідування, надання позитивної підтримки об'єктам жорстокого поводження та, де це можливо, допомоги для ініціаторів такого поводження, щоб змінити їхню поведінку. Якщо школи здійснюватимуть таку політику, вони без особливих проблем дадуть раду цькуванню чи переслідуванню.

ЯК ЦЕ РОБИТИ

Педагогам завжди доводилося стикатися з цькуванням та переслідуванням в класі та поза ним. Зараз же необхідно зрозуміти, як цей тип переслідування поширюється також і на Інтернет.

- Учні повинні вміти брати на себе відповідальність за власні дії, але цькування та переслідування підривають довіру і самоповагу. Коли людину переслідують або знущаються з неї, її спроможність до навчання знижується, оскільки вона не може зосередитися, відчуває загрозу та втрачає впевненість у собі.
- Учні, які почуваються у загрозі (як онлайн, так і офлайн), потребують допомоги дорослого, якому довіряють. Слід також пам'ятати, що особа, яка здійснює цькування чи переслідування, також потребує порад, щоб така поведінка не повторювалась у майбутньому.
- Боротьба з цькуванням та переслідуванням вимагає глобального підходу шляхом відкритого обговорення в сім'ї чи в класі природи та потенційної причини неприйнятної поведінки та кроків щодо виправлення ситуації, які можуть бути вжиті колективно.

5. https://en.wikipedia.org/wiki/Acceptable_use_policy

- Цькування та переслідування є соціальними проблемами. Учителі та батьки зобов'язані розслідувати будь-які твердження про таку поведінку та працювати в сім'ї чи в класі, щоб забезпечити найкраще з можливих середовище для навчання чи то в класі, на ігровому майданчику чи під час роботи онлайн.
- Давайте вчителям знання про динаміку процесу цькування й переслідування та способи використання Інтернету та мобільних телефонів із цією метою. Навчайте їх зчитувати сигнали, які надходять від жертв, а також від особи, відповідальної за образливу поведінку, і як реагувати, коли вони помічають такі сигнали.
- Школи повинні розробити конкретні керівні вказівки. Було б непогано включити запобіжні заходи в політику вашої школи щодо Інтернету для боротьби з цькуванням та переслідуванням.
- Учнів слід навчати чотирьом золотим правилам боротьби з кіберцькуванням чи кіберпереслідуванням:
    1. За можливості скопіюйте образливий матеріал.
    2. Не пересилайте його іншим.
    3. Відключіть пристрій, на який ви його отримали (комп'ютер чи мобільний телефон).
    4. Повідомте про інцидент дорослому, якому ви довіряєте.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Рольова гра: учні беруть участь в ігровому процесі вирішення конфлікту. Учитель розподіляє ролі та організовує групи, в яких учні відповідають за врегулювання суперечки. Наступним кроком є зміна ролей, що дозволяє поглянути на проблему з іншої точки зору.
- Дискусійні групи: учні беруть участь у дискусійних групах, щоб оцінити свою участь у груповій роботі та свої враження щодо таких тем, як цькування в цілому, рекомендовані та заборонені дії в Інтернеті та обов'язки.

НАЛЕЖНА ПРАКТИКА

Ось кілька ідей щодо того, як діяти при зіткненні з онлайн-цькуванням та електронними листами чи повідомленнями будь-якого типу, які використовуються для переслідування:

- Учнів слід проінструктувати не відкривати електронні листи з невідомих джерел.
- Якщо електронний лист чи текстове повідомлення відкрито та визнано образливим, зробіть копію образливого матеріалу, щоб показати її дорослому, якому довіряєте. Жертва ніколи не повинна реагувати на образливі повідомлення, оскільки це лише заохочує іншу особу продовжувати образливу поведінку.
- Якщо якась особа продовжує надсилати образливі або використовувані для переслідування електронні листи або повідомлення, і ви можете (за допомогою електронної адреси) з'ясувати, звідки такі повідомлення надсилають, негайно зв'яжіться з провайдером цього сервісу[6] або оператором мобільного зв'язку, щоб повідомити про переслідування.
- Шкільна політика щодо цькування та/або політика прийнятного користування повинна містити положення про те, як боротися з онлайн-переслідуванням з боку учнів.
- Учні повинні знати, що вони можуть звернутися до когось із батьків, учителя чи іншого дорослого, якому вони довіряють, у будь-який час, якщо їх переслідують онлайн або за допомогою мобільного телефону. Такий довірений дорослий повинен сприйняти розповідь всерйоз і заспокоїти жертву.
- Працюйте з відповідальними за цькування або винними у домаганнях, пояснюючи їм, що їх поведінку не можна терпіти та слід негайно припинити, але також з'ясуйте їхні мотиви, наскільки це можливо. Чи наважаться вони сказати ті самі слова чи вчинити ті самі дії в реальному житті?

6. https://en.wikipedia.org/wiki/Internet_service_provider

- Завжди намагайтеся зробити так, щоб батьки були в курсі, якщо їхню дитину цькують чи вона сама когось цькує. Коли особа, відповідальна за цькування, використовує для цього Інтернет або мобільний телефон, її образлива поведінка зазвичай не припиняється за воротами школи і, ймовірно, вона продовжуватиме її з дому.
- ENABLE[7] (European Network Against Bullying in Learning and Leisure Environments, Європейська мережа проти цькування в навчальному та дозвіллєвому середовищі) – це проєкт, що фінансується Європейською Комісією та надає детальну інформацію про найбільш успішні підходи до боротьби з цькуванням, а також соціальну та емоційну підготовку; він також надає інформаційні пакети для батьків та набори для однорангового навчання для шкіл.

ДОДАТКОВА ІНФОРМАЦІЯ

- Вебсторінка Ради Європи «Подолати цькування» пропонує інструменти проти цькування: *<www.coe.int/en/ web/edc/beat-bullying>*.
- Сайт NoBullying.com пропонує ресурси на тему цькування та кіберцькування: *<http://nobullying.com/>*.
- Вебсайт Smile of the Child пропонує допомогу у вирішенні щоденних проблем, з якими стикаються діти: *<http://www.hamogelo.gr/1.2/home>*.
- «Stomp Out Bullying»: *<http://www.stompoutbullying.org>* «Stop bullying now!» є американським вебсайтом, метою існування якого є зменшення поширеності цькування: *<http://www.stopbullyingnow.com/>*.
- «#DeleteCyberbullying» є інтерактивним застосунком для Android, що дає поради щодо кіберцькування: *<https://deletecyberbullying.wordpress.com/app/>*.
- Цільовою аудиторією сайту «Know the risks: challenging cyber bullying» є батьки та вчителі: *<http://web.archive.org/web/20100923133231/http://www.media-awareness.ca/english/teachers/wa_teachers/ safe_passage_teachers/risks_bullying.cfm>.*
- «What is cyber bullying?» – це вебсайт австралійського уряду, який дає поради сім'ям: *<http://web.archive.org/web/20090703064421/http://www.netalert.gov.au/advice/risks/cyber- bullying/What_is_cyber_bullying.html>*.
- Повідомляйте про цькування та шкідливий контент мережі Insafe: *<http://www.betterinternetforkids.eu>*.
- 2014 року Дослідницький центр П'ю опублікував резюме результатів своїх досліджень на тему онлайн-переслідування: *<http://web.archive.org/web/20160703044152/http://www.pewinternet.org/2014/10/22/on- line-harassment/>*.
- The No Hate Speech Movement (Рух проти мови ненависті) є молодіжною кампанією під егідою Ради Європи: *<http://www.nohatespeechmovement.org/>*.
- Дізнайтеся більше про цькування та завантажте плани уроків, інформаційні пакети для батьків і набори для однорангового навчання: *<http://enable.eun.org>*.

7. http://enable.eun.org

Інформаційний матеріал 22

Як отримати допомогу

Інтернет – це глобальна система взаємопов'язаних комп'ютерних мереж, які використовують пакет протоколів Інтернету (TCP/IP) для встановлення зв'язку між мільярдами пристроїв у всьому світі[1]. Тому він значно відрізняється від інших інформаційних каналів тим, що це найбільш децентралізований з наявних засобів спілкування. У нього немає єдиної точки управління через те, що ці мільярди вільно підключених пристроїв мають багато різних шляхів для забезпечення роботи зв'язку та передачі інформації. Крім того, користувачі онлайн-мереж є не лише глядачами, а й виробниками інформації з моменту появи Web 2.0 (див. Інформаційний матеріал 1 про підключення). У наш час, оскільки кожен може публікувати майже будь-що онлайн, і багато наших даних зберігаються в місцях, відомих як «хмарні сховища», ставиться багато питань про майбутнє Інтернету та про те, як можна контролювати хоча б невеликі частини цього потоку інформації. Ми часто запитуємо самих себе, хто може визначити, яка мова та інформація є образливими чи небезпечними для наших дітей, членів наших сімей та нас самих. І що ще важливіше, як ми можемо захистити від цього себе та своїх близьких?

1. https://en.wikipedia.org/wiki/Internet

ПРОТИЗАКОННИЙ КОНТЕНТ

Кожна країна сама визначає, який контент та які дії є законними та протизаконними згідно з її національним законодавством. Відповідно, Інтернет як засіб спілкування функціонує як регульована сфера діяльності. Будь-які дії, які вважаються протизаконними в «реальному житті», також повинні вважатися протизаконними в Інтернеті. Однак величезні можливості поширення інформації через Інтернет можуть посилити наслідки порушення поваги до прав інших людей і помножити негативний вплив цього; наприклад, онлайн-«дражніння» може перерости в дискредитацію чи щось іще гірше.

Протизаконним контентом у широкому сенсі слова може бути будь-яка діяльність, матеріал, інформація тощо, що суперечить законодавству та може завдати шкоди фізичній особі чи організації та/або викликати упередження проти неї.

Протизаконний контент охоплює зображення та вебсайти, що демонструють насильство й жорстоке поводження щодо дітей, незаконну діяльність у чатах (наприклад, зваблювання дітей), онлайн-пропаганду ненависті, ксенофобські повідомлення та вебсайти тощо. Ці та інші форми протизаконної поведінки регулюються Конвенцією Ради Європи про кіберзлочинність[2], яка є першим міжнародним договором про злочини, вчинені через Інтернет та інші комп'ютерні мережі, та Додатковим протоколом до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи[3]. Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (також відома як Лансаротська Конвенція)[4] охоплює також несанкціонований збір і зберігання даних та пошук інформації. Ця Конвенція є першим міжнародним договором, який передбачає кримінальне покарання за всі форми сексуального насильства проти дітей, включаючи зваблювання.

ОТРИМАННЯ ДОПОМОГИ Є ОДНИМ ІЗ ОСНОВНИХ ПРАВ!

Інтернет – це інструмент, до якого легко отримати доступ звідусіль і будь-кому, і тому контент, який вважається шкідливим або неприйнятним, може легко дістатися дітей, молоді та інших вразливих верств населення. Право на захист від шкоди та відшкодування втрат через дискримінацію чи будь-яке порушення прав є основним правом людини згідно із Загальною декларацією прав людини[5]. До того ж Конвенція ООН про права дитини підкреслює обов'язок дорослих діяти в інтересах дитини, захищаючи її від шкідливого контенту та дій, і покладає на уряди та сім'ї обов'язок ужити всіх заходів для забезпечення дотримання, захисту та здійснення прав дітей. Це включає надання соціальних послуг, а також створення правових, медичних та освітніх систем для підтримки дітей та створення середовища, в якому вони можуть зростати та розкривати свій потенціал. Служби довіри та інші механізми повідомлення про інциденти є важливим елементом у цих системах.

Поруч із іншими міжнародними організаціями, особливо в рамках діяльності в складі Міжнародного форуму з управління Інтернетом, Рада Європи прагне підвищувати суспільну та сімейну обізнаність щодо захисту дітей та молоді в Інтернеті. Це включає надання легкодоступної інформації про інструменти та процедури, які є в наявності для отримання відповідної допомоги.

ЯК ЦЕ РОБИТИ

- Про протизаконний контент будь-якого характеру, знайдений в Інтернеті, можна повідомляти на гарячу лінію. Гаряча лінія[6] – це сервіс, за допомогою якого кожен може подати повідомлення про будь-який імовірно протизаконний контент у Інтернеті. INHOPE – це асоціація, яка координує роботу гарячих ліній із проблем Інтернету в багатьох країнах світу[7]. Додаткову інформацію про тип протизаконного контенту, яким займається INHOPE, можна знайти на їх вебсайті[8].
- Щоб повідомити про протизаконний контент, відвідайте сайт *<http://www.inhope.org/tns/contact-us/details.aspx>* і дотримуйтесь указаних там кроків. Гаряча лінія вивчить повідомлення[9], щоб перевірити, чи є контент справді незаконним, і, якщо так, простежити його походжен-

2. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185
3. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189
4. http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=12/18/2008&CL=ENG; http://www.coe.int/en/web/children/lanzarote-convention
5. http://www.un.org/en/universal-declaration-human-rights/index.html
6. http://en.wikipedia.org/wiki/Hotline
7. http://inhope.org/gns/who-we-are/at-a-glance.aspx
8. http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/illegal-content.aspx
9. http://www.inhope.org/en/about/faq.html

ня та зв'язатися з правоохоронними органами країни перебування, а також з інтернет-провайдером для видалення цього контенту.

Запит про допомогу служби довіри

- Діти та молодь можуть звернутися за допомогою, зателефонувавши на телефон довіри[10], тобто сервіс, що пропонує підтримку в телефонному режимі та/або консультування за допомогою електронної пошти, Інтернету або СМС.
- У багатьох країнах центри обізнаності Insafe[11] співпрацюють з національними службами довіри, реагуючи на питання та занепокоєння молодих людей, пов'язані з їхнім онлайн-досвідом, або шкідливим чи протизаконним онлайн-контентом, з яким вони стикаються. Багато служб довіри, які займаються проблемами, пов'язаними з Інтернетом, також можуть допомогти молодим людям із широким колом інших питань «реального світу».
- Child Helpline International (Міжнародна дитяча служба довіри)[12] є важливим контактним пунктом у багатьох європейських та неєвропейських країнах. Ця глобальна мережа дитячих служб довіри працює майже в 150 країнах для захисту прав дитини.
- Зазвичай служби довіри працюють 24 години на добу та 7 днів на тиждень. Всі їх послуги є безкоштовними та конфіденційними, і вони не відстежують походження дзвінків, електронних листів та текстових повідомлень. Діти та підлітки можуть писати до них про багато різних речей, і є засоби, що дозволяють молодим людям спілкуватися за допомогою чату, електронної пошти та форумів, а також і більш традиційними методами. Співробітники служби довіри готові вислухати їх та допомогти їм розробити власні рішення.
- Щоб знайти службу довіри у своїй країні, ви можете здійснити пошук у мережі за назвою країни та словами «повідомлення» та «служба довіри».

Використання спеціальних сервісів для повідомлень на платформах соціальних мереж

- У більшості платформ соціальних мереж, наприклад, Facebook, Twitter, Instagram або Google, є центр безпеки, який пропонує поради користувачам, і онлайн-сервіс повідомлень, через який можна повідомити про неприйнятний контент або діяльність. Як правило, їх можна знайти в меню «Підтримка» чи «Допомога». Повідомлення про випадки цькування, наприклад, на сайтах соціальних мереж, може призвести до видалення образливого контенту і навіть до видалення облікових записів людей, які порушили умови використання. Більшість сайтів працюють подібним чином: наприклад, на Facebook кожен елемент контенту має спадне меню, яке дозволяє користувачам повідомити про допис чи фотографію та сказати, чому вони не хочуть їх бачити. Ця сторінка містить інформацію про процедуру повідомлення[13].
- Усі оператори мобільного зв'язку надають допомогу по телефону, через мережевий чат чи електронну пошту, а багато хто з них також надає поради, спрямовані на сім'ї та дітей. Наприклад, Vodafone надає доступ до вебсайту «Digital parenting»[14], який дає поради батькам та дітям та інструкції щодо налаштування батьківського контролю, а також пропонує встановити батьківський контроль та інші заходи безпеки через SecureNet[15]. Застосунок Vodafone Guardian на пристроях Android також дозволяє блокувати небажані контакти.

ДОДАТКОВА ІНФОРМАЦІЯ

- Перегляньте Конвенцію ООН про права дитини *<http://www.ohchr.org/en/professionalinterest/pages/crc.aspx>* та/або оглядовий документ, укладений UNICEF *<http://www.unicef.org/crc/fiights_overview. pdf>*, і отримайте додаткову інформацію про право дітей на захист і допомогу.
- Детальну інформацію про захист від насильства та повідомлення про нього можна отримати з Інтегрованої стратегії Ради Європи проти насильства, яка надає корисну інформацію за адресою: *<http://www.coe.int/en/web/children/integrated-strategies>.*
- Щоб повідомити про протизаконний контент, можна зв'язатися з INHOPE: *<https://www.inhope.org/>*.

10. http://en.wikipedia.org/wiki/Helpline
11. http://www.betterinternetforkids.eu
12. http://www.childhelplineinternational.org
13. https://www.facebook.com/help/181495968648557/
14. http://www.vodafone.com/content/digital-parenting.html
15. https://securenet.vodafone.com/

- Портал Insafe, європейської мережі центрів інтернет-безпеки *<http://www.betterinternetforkids.eu/>* пропонує інформацію про національні контактні пункти та служби довіри по всій Європі.
- Щоб повідомити про кіберцькування або отримати допомогу, можна зв'язатися з Childline *<http://www.childline.org. uk/>* , безкоштовною цілодобовою службою довіри для дітей та молоді (Телефон: 0800 1111).
- Befrienders.org *<http://www.befrienders.org>* – це вебсайт, де можна знайти службу довіри для тих, хто хоче вчинити самогубство, коли ви потребуєте допомоги.
- Europe Direct *<http://ec.europa.eu/europedirect/index_en.htm>* є безкоштовним сервісом, за допомогою якого ви можете негайно отримати відповіді на загальні запитання про діяльність ЄС та контактні дані відповідних організацій, зокрема національних служб довіри.

6. Інтернет – погляд у майбутнє

> «Вільне вираження поглядів є основою прав людини, джерелом людської природи та матір'ю правди. Вбити свободу слова означає посягнути на права людини, задушити людську природу та приховати правду».
>
> *Лю Сяобо, лауреат Нобелівської премії миру 2010 року та правозахисник*

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 23 – ІНТЕРНЕТ РЕЧЕЙ

Так само, як ви вже захищаєте свій комп'ютер та інші пристрої від порушень їх безпеки, обов'язково застосовуйте ці заходи до своїх пристроїв у «Інтернеті речей».
Майте на увазі, що важко захистити кожен окремий пристрій, але ви можете захистити свою мережу та зменшити зони вразливості.
Добре подумайте, перш ніж ввести до свого дому та в життя дитини будь-які предмети «Інтернету іграшок». Перевірте параметри безпеки та конфіденційності іграшки і запитайте себе: «Наскільки ця іграшка необхідна?»

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 24 – ШТУЧНИЙ ІНТЕЛЕКТ, АВТОМАТИЗАЦІЯ ТА РЕВОЛЮЦІЙНІ ТЕХНОЛОГІЇ

Чи знайшли ви інформацію про останні розробки в галузі штучного інтелекту та автоматизації? Чи доклали ви зусиль до вдосконалення своїх міжособистісних, соціальних та емоційних навичок?
Чи налаштували ви свої «розумні» пристрої так, щоб забезпечити належний рівень безпеки та захисту користувачів?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 25 – ВІРТУАЛЬНА ТА ДОПОВНЕНА РЕАЛЬНІСТЬ

Чи обговорили ви зі своєю дитиною/учнем такі ключові теми, як сексизм, сексуальність, расизм, цькування, стереотипи та інші форми дискримінації?
Чи переконались ви, що пристрої, якими користується ваша дитина/учень, налаштовані правильно, із високим рівнем конфіденційності та захисту безпеки?
Чи перевірили ви, чи підтримує ваша дитина/учень здоровий баланс у житті під час використання технологій віртуальної або доповненої реальності?

КОНТРОЛЬНИЙ СПИСОК ДО ІНФОРМАЦІЙНОГО МАТЕРІАЛУ 26 – ЧИ Є ВИ ПРОДУКТОМ? ВЕЛИКІ ДАНІ, ЗДОБУВАННЯ ДАНИХ І КОНФІДЕНЦІЙНІСТЬ

Чи витратили ви час на те, щоб переглянути спосіб, яким ваші приватні дані обробляються онлайн-сервісами, якими ви користуєтесь, і встановити адекватні налаштування конфіденційності?
Чи переглядали ви нещодавно контент, який ви розмістили онлайн, щоб переконатись, що він все ще відповідає дійсності і ви все ще готові ним ділитися?
Чи залишаєтесь ви в курсі останніх подій у сфері «великих даних», щоб зрозуміти, як ці зміни можуть вплинути на вас і що ви можете з цим зробити?

Інформаційний матеріал 23

Інтернет речей

Технологічний прогрес, про який свідчить нещодавній розвиток Інтернету та бездротового підключення до пристроїв, що підтримують передачу даних, викликає ажіотаж у багатьох сферах. Ця перспективна сфера розвитку відома як «Інтернет речей», де пристрої, пов'язані з мережею, підвищують ефективність компаній та роблять життя зручнішим, але можуть також викликати величезне занепокоєння як у батьків, так і у окремих осіб.

Занепокоєння щодо безпеки, конфіденційності та збору даних – це лише декілька з тих питань, які намагаються вирішити експерти та політики, оскільки розробляється та продається дедалі більше пристроїв. Однак Інтернет речей становить особливу проблему через те, що експерти та політики повинні знайти унікальні способи просувати переваги цієї нової технології, одночасно обмежуючи та навіть зменшуючи її ризики.

Споживачі не тільки починають замислюватися, коли «речі починають думати», але вони також мусять турбуватися про те, щоб хакери не отримали доступ до їхніх речей. Прочитайте статтю «Хакери віддалено вбивають джип на трасі»[1], у якій розповідається про те, як два хакери дистанційно граються з кондиціонером, радіо та склоочисниками,

1. http://web.archive.org/web/20160703222843/https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

а потім вимикають двигун транспортного засобу. Дії двох хакерів викликали дискусію щодо цифрової безпеки для легкових та вантажних автомобілів.

Ще один предмет дискусій – це ідея, що Інтернет речей стане наступною промисловою революцією. На сьогоднішній день існує близько 10 мільярдів підключених до мережі пристроїв, але очікуване зростання в межах цієї нової тенденції на ринку, як очікується, виведе цей показник на рівень від 26 до 30 мільярдів пристроїв до 2020 року, при цьому обсяг ринку оцінюється від 6 до 9 трильйонів доларів[2].

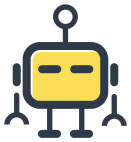
Це призведе до вибухоподібного зростання кількості підключених пристроїв та відповідного зростання кількості даних. Загальний регламент про захист даних зіткнеться з новими проблемами у захисті приватного життя, коли дані стануть присутніми всюди.

ІНТЕРНЕТ РЕЧЕЙ

- Термін «Інтернет речей» вперше з'явився у 1999 році, але лише за кілька років ми реально побачили об'єкти, підключені до Інтернету.
- Інтернет речей[3] – це мережа фізичних об'єктів або речей, до яких вбудовано електроніку, програмне забезпечення, датчики та засоби підключення, що дозволяє їм збирати дані та обмінюватися ними.
- Поняття Інтернету речей використовується для опису всього: від інтелектуальних термостатів, які підсилюють опалення перед тим, як ви прийдете додому, до холодильників, які замовляють апельсиновий сік, коли він закінчується. Люди носять браслети для відстеження стану здоров'я та фізичної форми, а на тварин вдягають пристрої, що відстежують їх стан здоров'я та місце перебування[4].
- Інтернет речей просто означає таке підключення до Інтернету, з яким пристрої можуть взаємодіяти між собою, полегшуючи контроль і автоматизацію завдань, а також збір даних.
- Дослідницький центр П'ю вважає, що Інтернет речей та «носимі пристрої» матимуть широкий та позитивний ефект[5] уже до 2025 року.

НОСИМІ ПРИСТРОЇ

- Носимі пристрої – це одяг та аксесуари, що включають елементи комп'ютерних та передових електронних технологій.
- Носимі пристрої також називають модними пристроями, технічним одягом або модною електронікою[6].
- Ці засоби надають користувачеві миттєві дані, і користувач може миттєво відстежувати технологію, завантажувати її для подальшого використання або надсилати роздруківку.



ІНТЕРНЕТ ІГРАШОК

- Інтернет речей поширюється також і на дитячі іграшки. Бездротове підключення дозволить іграшці взаємодіяти з іншими пристроями, що підтримують передачу даних, або іншими іграшками.
- Інтернет іграшок представляє нові способи ознайомити молоде покоління з технологіями та часто заохочує їх до взаємодії з іграшкою.
- Створений у 2015 році проєкт компанії Mattel зі сфери Інтернету іграшок Hello Barbie, в межах якого Барбі може слухати дітей, викликав занепокоєння у батьків та експертів з питань конфіденційності, а також провідних психологів, які задаються питанням, чи не можуть такі типи іграшок викликати проблеми у розвитку дітей, впливаючи на їх здатність творити, уявляти та вчитися самостійно. Створена 2011 року компанія ToyTalk висловлює іншу думку та стверджує, що іграшки, які говорять, та іграшки з підтримкою Wi-Fi можуть запропонувати дітям можливості для навчання[7].

2. https://securityintelligence.com/data-protection-in-the-internet-of-things/
3. https://en.wikipedia.org/wiki/Internet_of_Things
4. http://web.archive.org/web/20160310125239/http://www.theguardian.com/technology/2015/mar/30/internet-of-things-convenience-price-privacy-security
5. http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf
6. https://en.wikipedia.org/wiki/Wearable_technology
7. http://web.archive.org/web/20150604014333/http://www.nytimes.com/2015/03/29/technology/a-wi-fi-barbie-doll-with-the-soul-of-siri.html?_r=0

- Незважаючи на зручності, пропоновані Інтернетом речей та носимими пристроями, і незважаючи на розваги та веселощі, які пропонує Інтернет іграшок, користувачі можуть недостатньо усвідомлювати, що Інтернет речей та іграшкові пристрої, як і смартфони та комп'ютери, можуть створювати ризики для безпеки та конфіденційності. У випадку іграшок можуть виникати навіть ризики для розвитку дітей.

ВАЖЛИВІСТЬ РОЗУМІННЯ ПРОБЛЕМ

Інтернет речей включає носимі пристрої, які багато користувачів можуть не вважати «обчислювальним пристроями»; через це вони можуть проігнорувати проблеми у сфері конфіденційності.

Техно-футуристичне бачення Інтернету речей та носимих пристроїв є привабливим для багатьох. Однак позиціонування Інтернету речей на початковому рівні означає, що потрібно провести більше досліджень. Як показує минулий досвід фірм кібербезпеки, люди, що мають злочинні наміри, працюють дедалі активніше й швидше, щоб створити нові способи досягнення своєї кінцевої мети.

Просування іграшкових компаній у сферу Інтернету речей означає нові прекрасні іграшки для дітей, але батьки повинні розуміти ризики наявності в руках дітей пристроїв із відкритим мікрофоном та появи відкритих каналів передачі даних у їхніх домівках.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

Кінцевою метою Інтернету речей є підвищення ефективності, але взаємні зв'язки, що супроводжують цю підвищену ефективність, можуть становити значні ризики.

- Думка про те, що люди можуть віддалено отримати доступ до ваших пристроїв і ваших даних, просто лякає.
- Більшість пристроїв та носимих пристроїв не розроблені з урахуванням оптимальної безпеки та конфіденційності.
- Під час останніх проникнень у мережі хакери дивилися на людей у їхніх домівках за допомогою радіонянь і вебкамер[8].
- Споживачі можуть стикатися з таким самим високим ризиком кіберпроникнення, яким раніше був для них ризик фізичного вторгнення до їхніх домівок.
- Споживачі повинні знати, що Загальний регламент про захист даних надає їм контроль над своїми даними, і вони повинні знайти інформацію про те, як це буде працювати на практиці.

ЯК ЦЕ РОБИТИ

- Пристрої Інтернету речей відрізняються за конструкцією та функціями. Найважливіша порада щодо правильного використання пристрою – це ознайомитися з інструкцією та розуміти його функціональні можливості.
- Необхідно переглянути функції налаштувань, щоб вимкнути або увімкнути потрібні налаштування, які забезпечують конфіденційність там, де ви цього хочете.
- Подумайте про те, щоб вивчити пристрій перед покупкою, оскільки деякі носимі пристрої були відкликані або не функціонують, як заявлялося.
- Пам'ятайте, що це сфера, що розвивається, і, якщо почекати кілька тижнів або місяців, на ринку завжди з'явиться щось нове, краще, а часто ще й дешевше.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Доручіть учням скласти список усіх можливих пристроїв, які можна підключити вдома. Потім попросіть їх перерахувати потенційні ризики для безпеки або конфіденційності. Що може зробити користувач, щоб зменшити ці ризики? Що може зробити постачальник пристроїв? Що може зробити інтернет-провайдер?

8. http://web.archive.org/web/20160406200102/http://www.bbc.com/news/technology-30121159

- Після обговорення Інтернету речей попросіть учнів скласти тексти, які могли б виступити інструкціями для споживачів, щоб допомогти споживачам зрозуміти проблеми безпеки.
- Прочитайте резюме Загального регламенту пр захист даних і попросіть учнів перерахувати всі пункти, що стосуються Інтернету речей[9].
- Завантажте відеокліп про кампанію з інформування про права споживачів[10] та залучіть учнів до дискусії про права споживачів та Інтернет речей.
- Попросіть дітей «розробити» нові іграшки для Інтернету іграшок. Якими є переваги такої іграшки? Які ризики? Як вони можуть захистити юних користувачів? Як вони можуть переконати батьків у безпечності іграшки?

НАЛЕЖНА ПРАКТИКА

Важливо бути відкритим для прийняття цієї нової технології, але ви повинні бути впевнені, що вживаєте відповідних заходів безпеки, щоб захистити свої дані та конфіденційність.

- Обмежте присутність особистої інформації на пристроях із підтримкою даних.
- Посильте безпеку своєї домашньої бездротової мережі.
- Оберіть надійні паролі.
- Де це можливо, тримайте певні пристрої окремо один від одного.
- Обмежте взаємодію Інтернету іграшок із іншими пристроями та обов'язково контролюйте їх можливості.

При виборі пристрою, що належить до Інтернету речей, споживачі повинні бути уважними до кількох питань:

- Сумісність: цей пристрій сумісний з пристроями інших виробників, чи вам потрібно залишатися в тій самій «екосистемі», щоб мати можливість користуватися цим пристроєм? Це надзвичайно важливо, оскільки в іншому випадку ви будете «прикуті» до цього виробника, не маючи можливості переключитися на інші пристрої інших виробників або інтегрувати їх.
- Підключення: чи покладається пристрій Інтернету речей лише на підключення до Інтернету, щоб нормально функціонувати? В ідеалі ви повинні мати змогу отримати доступ до пристрою без необхідності підключатися до Інтернету. Це особливо важливо, оскільки в іншому випадку, якщо виробник вашого пристрою закриє онлайн-платформу, через яку здійснюється доступ до вашого пристрою, він фактично стане непридатним для роботи.

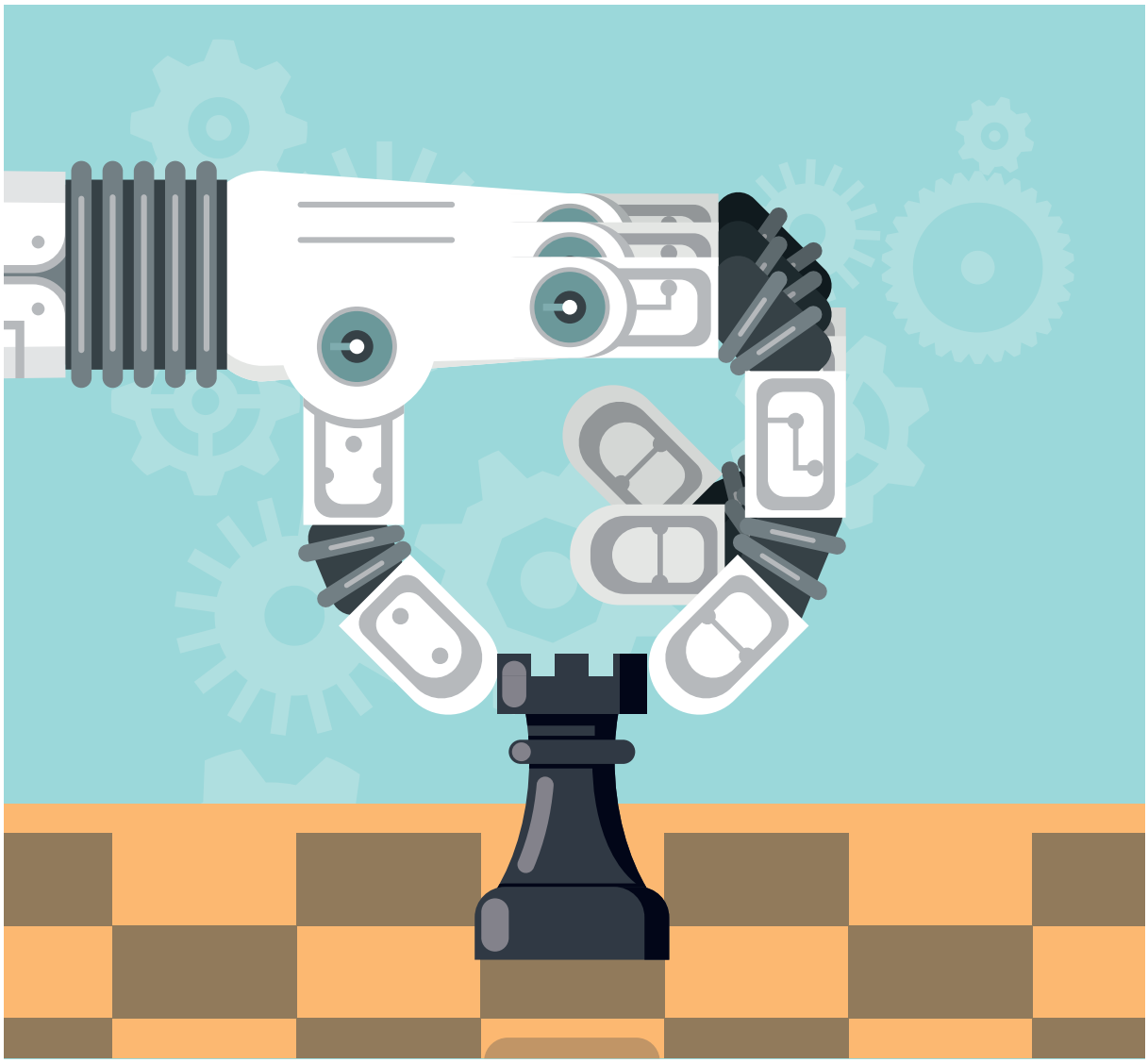
ДОДАТКОВА ІНФОРМАЦІЯ

- Додаткова інформація про "Законодавство про захист прав споживачів" ЄС доступна за посиланням: *<http://ec.europa.eu/consumers/consumer_rights/index_en.htm>*.
- Публікації The Guardian про Інтернет речей: *<http://www.theguardian.com/technology/internet-of-things>*.
- Додаткова інформація про Інтернет речей доступна в інфографіці Intel: *<www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html>*.
- Компанія Disney провела дослідження про Інтернет іграшок: *<http://www.disneyresearch.com/project/calipso-internet-of-things/>*.
- Посібник про Інтернет іграшок доступний за посиланням: *<http://www.mutualmobile.com/posts/iot-internet-toys>*.
- Додаткова детальна інформація з Дитячого центру цифрових медіа: *<http://cdmc.georgetown.edu/publications-and-papers/textbooks/>*.
- Відповідні документи Ради Європи: «Права людини для користувачів Інтернету – діти та молодь» *<http://www.coe.int/en/web/internet-users-rights/children-and-young-people)>*.

9. <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>
10. <http://ec.europa.eu/justice/newsroom/consumer-marketing/events/140317_en.htm>

Інформаційний матеріал 24

Штучний інтелект, автоматизація та революційні технології



«Автоматизація»[1] – це процес, за допомогою якого будь-яка дія чи функція, що виконуються людиною, передається машині, а «штучний інтелект»[2] – це інтелект, який демонструють машини або програмне забезпечення.

В історії технологічні стрибки багато разів знищували старі робочі місця та створювали нові. Візьмімо, наприклад, телефоністок, які повністю зникли через розвиток телекомунікаційних технологій. Дестабілізації на ринку праці, спричинені технологічними революціями, не є новим явищем, але щоразу суспільство побоюється, що нових робочих місць не буде достатньо, щоб компенсувати втрачені.

1. https://en.wikipedia.org/wiki/Automation
2. https://en.wikipedia.org/wiki/Artificial_intelligence

Досі такі побоювання були в основному невиправданими, оскільки робочі місця, які раніше ніхто не міг уявити, створювалися в достатній кількості, щоб компенсувати втрачені робочі місця. Наприклад, два десятиліття тому ніхто не передбачав, що існуватиме така робота, як «менеджер соціальних мереж» або «оптимізатор пошукових систем».

У той же час сучасні технологічні тенденції в галузях штучного інтелекту (ШІ), машинного навчання та автоматизації загрожують набагато більшій частині ринку праці, а не лише низькокваліфікованим робочим місцям.

НОВІ ТЕНДЕНЦІЇ

Безпілотні автомобілі

Незважаючи на те, що безпілотні автомобілі ще не скоро стануть доступними та готовими до масового виробництва, поступ у цій галузі є незаперечним. Наприклад, Tesla вже виробляє автомобілі, які можуть автономно їздити по шосе. Заходи, вжиті після найпершої смертельної аварії через помилку програмного забезпечення в машині Tesla у травні 2016 року, вплинуть на майбутнє технології безпілотних автомобілів. Найбільшою перешкодою є не сама технологія, а проблема визначення відповідальності у випадку аварії та необхідне застосування закону до ситуацій, коли машини самі ухвалюють рішення у критичних ситуаціях. Але як тільки ці перешкоди буде усунуто, таксисти, водії вантажівок та громадського транспорту (метро, автобус, трамвай) зникнуть. В ЄС транспортна галузь складає 4,5% загальної зайнятості.

Автоматично згенеровані вебсайти, застосунки, ігри

Професія вебдизайнера з'явилася нещодавно, але вона може зникнути навіть швидше, ніж професія телефоністки. На сьогоднішній день створення вебсайту за допомогою програм-конструкторів вебсайтів стає дедалі простішим, вимагаючи від користувача лише маніпулювання контентом шляхом перетягування його на екран. Складні алгоритми тепер можуть автоматично згенерувати ваш вебсайт на основі ваших уподобань. «The Grid»[3] – це перший сервіс, який пропонує автоматичне створення вебсайтів на основі ваших уподобань. Для створення повністю масштабованого вебсайту (сумісного з усіма екранами від комп'ютерів до смартфонів) йому потрібні лише зображення, контент та деяка інформація щодо призначення вашого вебсайту та ваших уподобань. І це лише початок. Із вдосконаленням штучного інтелекту, алгоритмів та машинного навчання багато робочих місць, для яких потрібні навички програмування, будуть автоматизовані, залишаючи лише ті робочі місця, які вимагають багато творчих зусиль, індивідуального підходу чи інновацій.

Випадково згенеровані твори мистецтва

Завдяки успіхам машинного навчання комп'ютери тепер можуть створювати художні твори, починаючи від зображень та картин і закінчуючи музикою. Генератор компанії Google «Deep dream»[4] аналізує ваше зображення та показує вам уявні об'єкти всередині, подібно до того, як ви дивитесь на хмари та бачите собаку чи квітку. Інші програми здатні наслідувати стиль художника, наприклад, Ван Гога або Пікассо, і застосувати його до будь-якої зробленої вами фотографії[5]. У музиці програма Emily Howell[6] здатна аналізувати музичні партитури, робити висновки про «правила» чи «закономірності» всередині музики та складати музику в подібному жанрі. Хоча це не означає кінець професії митця, це, безумовно, вплине на мистецтво.

Роботи та самообслуговування

Величезні інтернет-магазини, такі як Amazon, інвестують значні кошти в роботів, щоб виконувати такі завдання, як сортування та впорядкування товарів для доставки. Перший готель, яким повністю управляють роботи, вже відкрив свої двері в Японії. Існують станції самостійного сканування в супермаркетах, самообслуговування в ресторанах, наповнені роботами виробничі складальні лінії, роботи-помічники в закладах охорони здоров'я та догляду за літніми людьми, автоматизовані процеси доставки для онлайн-покупок, а такі послуги, як готельна справа, починають управлятися роботами. Дедалі більше прикладів автоматизації з'являтиметься по всьому світу. Навіть будівельні роботи можна автоматизувати з приходом тривимірного друку!

3. https://thegrid.io/
4. http://deepdreamgenerator.com/
5. http://web.archive.org/web/20160114142911/http://arxiv.org/pdf/1508.06576v2.pdf
6. http://artsites.ucsc.edu/faculty/cope/Emily-howell.htm

Точні алгоритми з великою прогностичною силою

Завдяки поєднанню великих даних, суперкомп'ютерів та потужних алгоритмів багато галузей, наприклад, охорона здоров'я, зазнають нової революції. Завдяки величезному обсягу даних, пов'язаних зі здоров'ям, алгоритми стають кращими діагностами, ніж лікарі, у постановці діагнозу на основі симптомів, датчиків реального часу та даних минулих медичних записів.

ШІ та машинне навчання

Завдяки вдосконаленому програмному забезпеченню та комп'ютерам машини сьогодні можуть вчитися, спостерігаючи за діями людей та виводячи певні «правила» чи «зразки», які вони потім наслідують, або просто навчаються на практиці та виводять «правила» шляхом дослідження результатів певних дій. Наприклад, комп'ютерні програми змогли успішно закінчити сеанси відеоігор, «навчившись» перемагати ворогів, перестрибувати через перешкоди тощо. Неможливо спрогнозувати, чому машини зможуть «навчитися» у майбутньому, але в даний час вже ясно, що повторювані завдання перебувають в межах досяжного для них.

КОРИСТЬ ДЛЯ ОСВІТИ

- Навчання кодуванню прокладає шлях до глибшого розуміння робототехніки та програмного забезпечення, включаючи базові параметри ШІ та автоматизацію. Це є надзвичайно важливим для виявлення та вдосконалення навичок, які все ще перебувають поза межами досяжності комп'ютерів та машин, для розвитку тих навичок, які знадобляться для подальшого розвитку цих технологій. Коли робочі місця, які вимагають низької кваліфікації та рутинної праці, буде зайнято машинами, людям нічого не залишиться, як здобувати кращу освіту.
- У той же час вивчення автоматизації та ШІ допоможе сформувати погляди щодо політики, яка забезпечить користь для суспільства в цілому від їхнього впливу. Наприклад, багато авторів, що пишуть про автоматизацію та ШІ, виступають за універсальні виплати гарантованого доходу та зменшення робочого дня. Низка вчених, дослідників та видатних діячів, таких як Стівен Гокінг, підписали відкритий лист із закликом чітко визначити напрямок розвитку ШІ, щоб одного дня не потрапити в рабство до машин[7].

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

Безробіття

Найбільш очевидним ризиком розвитку ШІ та автоматизації є створення меншої кількості робочих місць, ніж вони замінять. Незважаючи на те, що неможливо передбачити робочі місця, які можуть бути створені у зв'язку з розвитком цих технологій, для цих нових робочих місць буде потрібна висококваліфікована робоча сила, і буде мало можливостей для працевлаштування людей, які мають лише середню освіту.

Зростання нерівності

Враховуючи те, що низькокваліфікованих робочих місць стає менше, зростатиме нерівність між тими, хто має популярні на ринку праці навички, і тими, чиї навички поступово замінюються машинами. Інша форма нерівності стосуватиметься країн, одні з яких мають технологічні ноу-хау для переходу до автоматизації та інновацій ШІ, тоді як інші покладаються на ручну працю. Без належної соціальної політики, політики зайнятості та політики освіти й професійного навчання, нерівність може спричинити соціальні заворушення.

Покладання надмірних надій на машини

Автоматизація та ШІ не є панацеєю. Наразі вони все ще вимагають людського нагляду і лише допомагають виконати більш складне завдання. Наприклад, хоча програмне забезпечення легко керує польотом літака на автопілоті на крейсерській висоті, посадка та зліт досі повинні здійснюватися людьми вручну. Однак, оскільки пілоти-люди отримують дедалі менше підготовки та практики, вони можуть бути менш здатними дати раду «критичній» ситуації, з якою не може впоратися автопілот. Те саме можна сказати про безпілотні автомобілі. Що станеться в майбутньому, де транспорт є автоматичним, якщо програмне забезпечення вийде з ладу,

7. http://futureoflife.org/AI/open_letter

а жодна людина вже не вміє керувати автомобілем? Якщо машини в кінцевому підсумку робитимуть все за нас і навіть будуть здатні самі себе створювати та ремонтувати, що залишиться робити нам, людям? Це може спричинити значний регрес частини населення, яка просто шукатиме розваг замість підвищення кваліфікації та знань, що, у свою чергу, сприятиме подальшому зростанню нерівності та соціальній напрузі.

Повільне або невідповідне ситуації пристосування до нових умов і розвиток навичок

Невідомо, чого автоматизація та ШІ досягнуть у майбутньому, а відтак дуже складно уявити, які навички слід розвивати, оскільки вони «витримають випробування майбутнім». Наприклад, світ освіти повільно починає підтримувати ідею викладання програмування та кодування в школах, але останні розробки в галузі ШІ показують, що можна автоматизувати саме програмування, оскільки воно ґрунтується на логіці та чітких правилах. Автоматична генерація вебдизайну є лише одним із прикладів.

Безпека

Як і будь-який пристрій, що підключений до Інтернету або використовує програмне забезпечення, ШІ та автоматизація також вразливі до злому. Але наслідки цього можуть бути набагато серйознішими, ніж викрадення або знищення ваших персональних даних. Команда спеціалістів з безпеки показала, що можна атакувати й узяти під контроль підключений до Інтернету автомобіль і виконати з ним такі дії, як вимкнення двигуна або навіть перехоплення управління кермом на низькій швидкості. Уявіть собі наслідки, якби було атаковано безпілотний автомобіль без керма.

Кінець нудної роботи, початок нудного світу

Можливо, що найбільші виклики з тих, які ставлять ШІ та автоматизація, мають філософський характер. Що робить наш світ цікавим? Чи можуть люди бути щасливими у світі, який є цілком зрозумілим, передбачуваним та оптимізованим, у якому все працює «за планом»? Що станеться з людською спонтанністю, навмисним рішенням зробити помилку і навчитися на ній або навіть правом ухвалити нерозумне рішення просто тому, що ми можемо це зробити? Впровадження «автоматизованих» рішень є логічним продовженням розвитку нашого суспільства, керованого наукою, фактами та розумом, але чи добре це для людей? Хоча століття тому багато вчених та інтелектуалів передбачали кінець релігії завдяки просвітницькій ролі науки, зараз ми спостерігаємо повернення інтересу до духовності та релігії. Можливо, це симптом світу, який не в змозі запропонувати людям сенс життя і воює з тим, що робить нас людьми: емоціями, почуттями, імпульсивністю та ірраціональністю.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Хорошим вступним заняттям у класі для презентації штучного інтелекту є так званий захід «розумний папірець». Він полягає в представленні аркуша паперу з надрукованими інструкціями, який може перемогти будь-яку дитину чи молоду людину у грі хрестики-нулики. Див. детальні інструкції тут: *<http://web.archive.org/web/20160326100226/http://csunplugged.org/artificial-intelligence/>*.
- Продовжуючи роботу після цього базового заходу, поцікавтеся у своїх дітей чи учнів, чи знають вони про якийсь штучний інтелект, який вони використовують у своєму повсякденному житті.
- Найімовірніше, ваші учні матимуть смартфони, а більшість смартфонів постачаються із власними «цифровими помічниками», а саме Siri для iOS/Apple, Google Now для Android/Google та Cortana для Windows/Microsoft. Усі три мають ознаки штучного інтелекту: вони мають функцію розпізнавання голосу, яка стає кращою, дослухаючись до мільйонів людських голосів, у них є алгоритм відповіді на запитання, які ви задаєте, і вони персоналізують інформацію, яку показують, на основі даних, які ви їм надаєте (дані пошуку, контактні дані, дані про місцезнаходження тощо). Те саме стосується основних функцій, таких як предиктивне введення тексту. Це теж технологія ШІ.

НАЛЕЖНА ПРАКТИКА

- Штучний інтелект, автоматизація та машинне навчання можуть бути дуже корисними, але ніколи не забувайте про необхідність підтримувати певні навички роботи вручну на випадок відключення цих функцій. Наприклад, навіть якщо застосунки GPS зараз часто зустрічаються на смартфонах, навчитися читати карту та розвинути відчуття орієнтації все одно корисно.
- Тримайте все під контролем. Існує багато рівнів автоматизації, та найекстремальніший з них – це машина, яка ухвалює рішення без участі людей чи перевірки з боку людей. Подібно до того, як робиться при предиктивному введенні тексту, де користувач завжди має вибір – прийняти чи відхилити пропозицію, внесену програмним забезпеченням, так само слід налаштувати будь-який автоматизований чи заснований на ШІ пристрій чи програмне забезпечення, щоб їхні рішення вимагали перевірки з вашого боку.
- Будьте готові до змін і універсальними при формуванні багатьох різних навичок. Оскільки ці революційні технології вже виходять на ринок, адаптуватись зможуть найбільш універсальні та гнучкі працівники. Дуже ймовірно, що в майбутньому працівникам доведеться часто проходити «перекваліфікацію» або повертатися до закладу освіти, щоб розвинути нові набори навичок. Навчання впродовж життя буде нормою.
- Удосконаліть свої міжособистісні, соціальні та емоційні навички, оскільки вони захищені від будь-якої форми автоматизації. Хоча роботи та алгоритми зможуть замінити багато низькокваліфікованих працівників, вони ніколи не зможуть замінити якість та взаємодію між людьми.
- ШІ та автоматизація спираються на програмне забезпечення. Переконайтеся, що всі «розумні» пристрої, якими ви володієте, мають найновішу версію програмного забезпечення, регулярно перевіряючи наявність оновлень та пристосовуючи ці пристрої до налаштувань безпеки високого рівня. Якщо для роботи вашого пристрою непотрібне постійне з'єднання з Інтернетом, переконайтеся, що його відключено, щоб зменшити ймовірність злому.
- Для того, щоб скласти для себе повну картину та отримати загальне уявлення про те, що може принести майбутнє, перевірте, чи прочитали ви Інформаційні матеріали про великі дані, доповнену та віртуальну реальність та Інтернет речей. Зрозумійте, що великі дані – це те, що живить розвиток штучного інтелекту та автоматизації, що доповнена та віртуальна реальність – це нові способи взаємодії з ШІ та машинами, що Інтернет речей буде не лише ще одним способом взаємодії з ШІ та машинами, але й механізмом забезпечення їх цінними даними, які сприятимуть їх подальшому розвитку. Тільки зрозумівши загальну картину, громадяни зможуть ухвалювати свідомі та обґрунтовані рішення щодо використання цих змін для поліпшення стану суспільства.

ДОДАТКОВА ІНФОРМАЦІЯ

- Стаття про штучний інтелект на сайті Бі-Бі-Сі: *<http://web.archive.org/web/20160509115227/http://www.bbc.com/news/technology-34224406>*.
- Google пропонує сторінку з дослідженнями про штучний інтелект та машинне навчання: *<http://research.google.com/pubs/ArtificialIntelligenceandMachineLearning.html>*.
- Тут можна прочитати новини автоматизації: *<http://www.automationworld.com/>*.
- Це офіційна вебсторінка Виставки побутової електроніки, яка часто демонструє останні новинки в галузі інформаційних технологій : *<https://www.cesweb.org/>*.
- Новини про останні дослідження та інновації в галузі ІКТ доступні в Research and Innovation Magazine Комісії ЄС: *<http://horizon-magazine.eu/topics/ict>*.

Інформаційний матеріал 25

Віртуальна та доповнена реальність

Віртуальна реальність[1] – це мультимедійний досвід із зануренням, який відтворює середовище, що імітує фізичну присутність у реальному світі. Створювані при цьому сенсорні відчуття можуть включати зір, слух, дотик, запах і смак, причому перші два найбільш поширені.

Доповнена реальність[2] – це додавання сенсорної ввідної інформації, створеної комп'ютером – звуку чи зображення до реальних середовищ.

Хоча ідея віртуальної та доповненої реальності виникла кілька десятиліть тому, лише недавно технологія зайшла достатньо далеко, щоб можна було собі уявити комерціалізацію пристроїв, послуг та програмного забезпечення віртуальної та доповненої реальності. Популярність застосунків доповненої реальності швидко зросла завдяки смартфонам, мобільному Інтернету та технологіям геолокації.

1. https://en.wikipedia.org/wiki/Virtual_reality
2. https://en.wikipedia.org/wiki/Augmented_reality

Деякі приклади останніх подій у сфері віртуальної та доповненої реальності:

- краща доступність гарнітур віртуальної реальності, наприклад, Oculus Rift, Samsung Gear VR, HTC Vive або Sony Playstation VR, причому для них запускається низка ігор, зокрема через мобільні платформи Android та iOS, PlayStation 4, Xbox One та традиційні комп'ютерні ігри для ПК або Mac;
- краща доступність гарнітур або окулярів доповненої реальності, наприклад, Google Glass та Microsoft HoloLens; Microsoft планує запустити версію Minecraft з доповненою реальністю, в яку можна буде грати у своїй вітальні;
- випуск мейнстримних ігор з доповненою реальністю, наприклад, Pokemon Go, що дозволяє ловити покемонів у реальному світі за допомогою смартфона (iOS та Android).

КОРИСТЬ ДЛЯ ОСВІТИ

- Завдяки тому, що віртуальна реальність може імітувати відчуття реального світу, це відкриває багато можливостей для навчання. Наприклад, навчання керуванню автомобілем можна точно змоделювати.
- З огляду на рівень занурення, який забезпечує віртуальна реальність, досвід вже показав перспективність використання віртуальної реальності в терапевтичних цілях: позбавлення від арахнофобії або подолання посттравматичних стресових розладів (ПТСР). Вона також успішно застосовується для підвищення рівня співпереживання та розуміння інших, дозволяючи користувачеві відчути себе в ролі іншого: людини з обмеженими можливостями (сліпої людини, людини в інвалідному візку) або члена меншини, яка страждає від дискримінації.
- Хоча ніщо не може замінити реальності, але не кожен має можливість подорожувати. Віртуальна реальність може імітувати відвідування пам'ятника чи будь-якого іншого місця, як ніби ви фізично там побували. Але вона може піти ще далі і дозволити вам відвідати місця, куди ви ніколи не змогли б поїхати насправді, наприклад, Місяць або космічний простір, або внутрішня порожнина вулкана, або навіть може повернути вас назад у часі, щоб імітувати перебування на полі бою XVIII століття або прогулянку поряд з динозаврами.
- У доповненої реальності забагато корисних застосувань, щоб їх можна було перерахувати. Оскільки вона полягає у накладанні додаткової інформації чи предметів на реальний світ, її можливості безмежні. З доповненою реальністю немає необхідності в екскурсоводі, оскільки коли ви дивитесь на пам'ятник, статую чи щось інше, корисна інформація може бути накладена на цей об'єкт. Для накладання інформації немає меж. Це може бути меню або огляд ресторану, нагадування про імена людей або інформація про них, котра спливає, коли ви їх бачите, тощо. З точки зору навчання, для нього теж існують безмежні можливості: доповнена реальність може показати вам, як відремонтувати/замінити деталь автомобіля, накладаючи кроки, які вам потрібно зробити; допомогти хірургу під час операції; показати вам, як приготувати страву, імітуючи, як ви повинні нарізати та змішати інгредієнти. Все, на що ви дивитесь, можна доповнити додатковою інформацією. Таким чином, клас можна перетворити на сцену, до якої можна додавати віртуальні об'єкти, наприклад, демонструючи напівпрозору модель людського тіла.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

Поведінковий ризик

У ряді досліджень вивчався зв'язок між захопленням відеоіграми та реальною поведінкою, зокрема підвищення рівня насильства та агресивності. Утім, ці висновки досі є предметом суперечок. Деякі дослідження вказують на «короткочасну» агресивність та буйну поведінку після сеансу відеоігри з високим рівнем насильства, інші дослідження підкреслюють ефект «розрядки напруги», який ці ігри мають на дітей. Інші деталі, наприклад, чи була гра багатокористувацькою (з елементом співпраці), також впливають на результати. Правда полягає в тому, що ми ще далекі від розуміння тривалого ефекту відеоігор для дітей та молоді. Віртуальна реальність та доповнена

реальність додадуть ще один шар реалістичності до відеоігор, роблячи їх дедалі ближчими до «реальності», і мало що відомо (якщо взагалі щось відомо) про те, як це вплине на дітей. Нещодавно бурхливу полеміку викликали такі відеоігри, як GTA V, де сторонній додаток, розроблений приватними особами, дозволяв гравцям імітувати зґвалтування віртуального жіночого персонажа. Сексизм у відеоіграх – це добре відоме явище, і гравчині часто прикидаються «чоловіками», щоб уникнути домагань. І справа не лише у формальному контенті відеоігор. Онлайн-чат відеоігор використовується для поширення екстремістського контенту, сексизму, цькування, мови ненависті тощо. Відеоігри з використанням віртуальної та доповненої реальності стануть частиною носіїв інформації, які діти споживатимуть у майбутньому, і певною мірою сприятимуть формуванню їхніх світоглядів і поведінки. Якщо безвідповідальні розробники включають надзвичайно жорстокий, екстремістський, сексистський, расистський, гомофобський контент до своїх ігор, це може негативно вплинути на користувачів.

Конфіденційність

Доповнена реальність спирається на постійний аналіз фізичного світу в режимі реального часу, щоб точно «доповнити» його за допомогою віртуальних елементів. Це означає, що вашу локалізацію та те, на що ви дивитесь, треба надсилати на суперкомп'ютери, як правило, онлайн, щоб точно розрахувати, що має відображатися. Без належного захисту конфіденційності доповнена реальність може стати способом набагато проникливішого шпигування за людьми в режимі реального часу.

Безпека

Завдяки постійному підключенню пристроїв до Інтернету, атакувати підключений пристрій на відстані стало значно простіше. Коли ми почнемо використовувати пристрої з доповненою та віртуальною реальністю – окуляри або навіть контактні лінзи – можуть виникнути нові сприятливі для злому ситуації, які будуть дуже небезпечними. Наприклад, якщо водій використовує дисплей доповненої реальності для отримання дороговказів, можна буде здійснити злом дисплея, щоб відволікти водія від дороги.

Маніпуляція та споживацтво

Доповнена та віртуальна реальність також принесуть із собою нові рекламні стратегії. Оскільки немає жодних норм, які б визначали, що є дозволеним, можна робити все що завгодно, і ми можемо легко припустити, що будуть використовуватися такі методи, як «доповнення» вашого дому за допомогою реклами. Наприклад, ви можете відкрити свій холодильник, і рекламний пристрій буде «доповнювати» вміст вашого холодильника, щоб відображати товари, які ви «повинні» мати всередині. У супермаркеті під час сканування товару за допомогою смартфона вам може прийти сповіщення, яке запропонує придбати інший товар.

Залежність і здатність викликати звикання

Неврологія за останні роки розвинулась, і було зроблено багато відкриттів стосовно роботи мозку. Мозок отримує велике задоволення від швидких подразників, до прикладу, швидких дій, рухів тощо. Саме це робить відеоігри та бойовики зі швидким розвитком сюжету такими успішними. На жаль, «реальний» світ вимагає набуття та відпрацювання таких навичок, як стриманість, самоконтроль, терпіння, наполегливість та ініціативність. Не все можна «перетворити на гру» або зробити «приємним» за допомогою сучасних технологій. Навчання грі на скрипці є лише одним із прикладів. Оскільки діти зростатимуть, бачачи віртуальну та доповнену реальність, існує ризик того, що вони не зможуть дати собі раду в світі, який не є «доповненим» або є не таким «багатим» та повним стимулів, як їхня «віртуальна» реальність. Хорошим прикладом цього є MMORPG (масові багатокористувацькі онлайн-рольові ігри). Хоча вони допомагають розвинути велику кількість навичок: відчуття організації, планування, керівництво та співпраця, вони мають дуже «приємну» криву навчання, яка є рівно настільки складною, щоб зацікавити гравців, але не надто складною, щоб не знеохочувати їх. Доповнена та віртуальна реальність посилить цю проблему і може створити звикання та залежність від світу, з яким легше дати собі раду, який менше розчаровує та набагато більше стимулює, ніж реальний світ.

Утрата міжособистісних навичок та асоціальна поведінка

Хоча масштаби цього явища все ще обмежені, в деяких країнах, наприклад, у Японії, спостерігається зростання такого явища, як відхід від суспільного життя підлітків та дорослих, яких називають «хікікоморі». Хоча це безпосередньо не пов'язано із медіа, телебаченням чи Інтернетом, ці носії інформації роблять відхід від суспільного життя більш стерпним, оскільки вони відволікають людину від труднощів «реального» життя. Віртуальна та доповнена реальність може ще більше посилити це явище, оскільки з віртуальною реальністю може бути легше дати раду, і від неї можна отримати більше задоволення, ніж від «невпорядкованої» людської взаємодії. Навіть секс та сексуальні стосунки пов'язані з негативними емоціями, тиском для досягнення успіху, соромом за своє тіло, але всі такі емоції зникають у віртуальному світі, де користувач повністю контролює все.

Фізичне здоров'я

Доповнена реальність та віртуальна реальність також дають можливість вирішити проблеми фізичної неактивності, наприклад, серед користувачів, які пасивно сидять за екранами по багато годин за раз. Наприклад, ігри, що базуються на локаціях, можуть відбуватися в реальному світі з доповненою реальністю, а проєкти можуть створювати спеціальні кімнати для середовищ віртуальної реальності. У той же час досвід занурення в нову реальність створює нові проблеми: ігнорування ознак болю або надмірного перебування біля екрана завдяки здатності віртуального або доповненого контенту привернути нашу повну увагу. Повторювані рухи всередині гри можуть призвести до тендиніту, як це спостерігається у деяких іграх Wii. Крім того, хвороба руху і нудота можуть бути сильним побічним ефектом досвіду доповненої реальності із зануренням, оскільки зображення, які подаються в мозок через монітор на голові, стикаються із вхідною інформацією від датчиків руху у внутрішньому вусі. Нарешті, багато бета-тестерів повідомляють, що вони постраждали внаслідок падіння або зіткнення з об'єктом, коли були занурені у віртуальну реальність або навіть доповнену реальність, оскільки вони дивилися на екрани смартфонів, граючи в ігри доповненої реальності в реальному світі.

Переслідування, кіберцькування та пов'язані з контактами ризики

Оскільки межа між тим, що є реальним, і тим, що є віртуальним, змінюється, віртуальна, і особливо доповнена реальність може бути використана як миттєвий спосіб приниження когось, наприклад, шляхом програмування накладання голови щура при розпізнаванні обличчя людини або транслювання відео когось, хто перебуває у принизливій ситуації.

Доповнена реальність і, в меншій мірі, віртуальна реальність несуть ризики, пов'язані з «контактами». Масові ігри з доповненою реальністю спираються на те, що люди грають в реальному світі проти реальних незнайомців. Проблемні ситуації можуть включати пограбування або напад у реальному житті.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

- Розширена та віртуальна реальність дуже залежні від апаратного забезпечення. Якщо ваша школа чи навчальний заклад не оснащені, наприклад, належною кількістю планшетів, ви не зможете повністю скористатися цими технологіями. У деяких випадках можна використовувати пристрої самих дітей та молоді (наприклад, їхні смартфони), але це створює проблеми щодо дотримання шкільної політики, оскільки деякі школи забороняють використовувати смартфони в навчальний час, і це може також призвести до дискримінації, оскільки деякі учні можуть не мати мобільного телефона, достатньо потужного для заходу із застосуванням доповненої чи віртуальної реальності, або навіть не мати мобільного телефона взагалі.
- Утім, в онлайн-просторі доступно багато ресурсів, які допоможуть вам використовувати доповнену та віртуальну реальність у класі. Доповнену реальність використовувати легше, оскільки вона не вимагає «наголовного спорядження», яке забезпечує відчуття повного занурення, і буде працювати з наявними пристроями: смартфонами та планшетами.

3. http://web.archive.org/web/20160318145342/http://www.schrockguide.net/augmented-reality.html; OnlineUniversities.com
4. http://www.onlineuniversities.com/blog/2012/09/20-coolest-augmented-reality-experiments-education-so-far/

НАЛЕЖНА ПРАКТИКА

- Оскільки нам мало відомо про наслідки тривалого використання або впливу цих нових технологій, підтримка здорового балансу життя є обов'язковою умовою. Переконайтеся, що ви та/або ваша дитина збалансуєте свої «мережеві», віртуальні чи доповнені заходи із «традиційними» заняттями спортом чи іншими захопленнями. Це стосується також і роботи в класі. Доповнена та віртуальна реальність є успішним бізнесом, і хоча багато тверджень про переваги їх використання в освіті можуть бути правдивими, не існує жодної чарівної палички для надання якісної освіти. Слід дотримуватися здорового балансу між традиційними та новими методами навчання, за цим майбутнє.
- Ретельно обирайте контент, який ви купуєте для своїх дітей, якщо вони користуються пристроями віртуальної або доповненої реальності, і контролюйте, до чого вони мають доступ. Прочитайте вікові обмеження та маркування, наприклад, маркування PEGI (див. Інформаційний матеріал 20 щодо маркування та фільтрування та Інформаційний матеріал 16 щодо ігор), а також увімкніть інструменти батьківського контролю на пристроях, що використовуються дітьми молодшого віку, щоб вони напевно не змогли отримати вільний доступ до контенту. Для дітей молодшого віку використовуйте якісні білі списки, якщо вони доступні у вашій країні/вашою мовою, оскільки це найкращий спосіб як захистити їх, так і гарантувати, що вони споживають позитивний контент, який перевірили професіонали.
- У наш час як ніколи важливо відверто говорити з дітьми та молоддю про насильство, кіберцькування, сексуальність і права та обов'язки. Установлення жорстких етичних стандартів із наймолодшого віку є найефективнішим способом нейтралізації сексистських, расистських чи будь-яких інших дискримінаційних чи негативних ідей, з якими ваші діти можуть зіткнутися в певний момент онлайн або за допомогою своїх пристроїв віртуальної та доповненої реальності.
- Установіть налаштування конфіденційності та безпеки для дітей молодшого віку на найвищому рівні. Див. Інформаційний матеріал 9. Пам'ятайте, що ці пристрої можуть стати об'єктами злому.
- Обов'язково ознайомтесь із бізнес-моделлю, яка стоїть за контентом або пристроєм, який ви використовуєте для віртуальної та/або доповненої реальності, оскільки ви або ваша дитина можете зазнати впливу нав'язливої реклами.

ДОДАТКОВА ІНФОРМАЦІЯ

- Новини про останні події у світі віртуальної реальності доступні на сайті Venture Beat: *<http://venturebeat.com/tag/virtual-reality/>*.
- Стенфордський університет опублікував статтю про віртуальну реальність та освіту: <https://teachingcommons.stanford.edu/teaching-talk/virtual-reality-and-education>.
- Новини про останні події у світі доповненої реальності також доступні на сайті Venture Beat: *<http://venturebeat.com/tag/augmented-reality/>*.
- Загальна інформація про доповнену реальність доступна в Посібниках для дослідників Бібліотеки Дартмутського коледжу: *<http://researchguides.dartmouth.edu/AR>*.

Інформаційний матеріал 26

Чи є ви продуктом? Великі дані, здобування даних і конфіденційність

Великі дані[1] – це широкий термін, який позначає дані настільки великі, що їх неможливо проаналізувати або обробити традиційними методами (наприклад, за допомогою одного комп'ютера або простого застосунку).

Великі дані виникли через поєднання таких чинників:

- надзвичайне зростання ємності цифрових сховищ, яке триває;
- збільшення обсягів даних, що генеруються нашими суспільствами (дедалі частіше все, що ми робимо, залишає цифровий слід);
- світ, взаємопов'язаний через Інтернет, що дозволяє з'єднати всі ці дані разом;
- дедалі більша здатність аналізувати та осмислювати всі згенеровані дані.

1. https://en.wikipedia.org/wiki/Big_data

Як приклади онлайн-сервісів, що використовують великі дані, можна навести такі соціальні мережі, як Facebook, пошукові системи Google або Bing та такі інтернет-магазини, як Amazon. Але великі дані – це щось набагато більше, ніж онлайнове явище; вони присутні і в нашому повсякденному офлайновому житті.

- Супермаркети використовують картки складського обліку для аналізу моделей покупок та коригування своїх товарних запасів в режимі реального часу або програмування якоїсь спеціальної поді\ в магазині (маркетинговий захід, розпродаж тощо).
- Дані, отримані від водіїв, датчиків їхніх автомобілів та GPS-пристроїв, допомагають надавати інформацію про дорожній рух у режимі реального часу.
- У лікарнях аналіз даних із датчиків, наприклад, частоти серцебиття, в режимі реального часу може допомогти виявити інфекції або інші проблеми зі здоров'ям до появи зовнішніх ознак і симптомів.

Дані також стали однією з найпопулярніших онлайн-валют. Замість того, щоб платити реальними грошима за онлайн-сервіси, якими ви користуєтесь, чи то соціальні мережі, чи то пошукові системи, ви «платите» даними, які ви надаєте цим сервісам. Ці дані дозволяють сервісам адаптувати рекламу та маркетинг до ваших уподобань, роблячи їх більш ефективними. Однак порівняння даних із грішми є неточним. Порівняно з грошима, дані набагато делікатніші. Їх можна повторно використати кілька разів і перепродати. Більш справедливим порівнянням було б надання ключа від вашого будинку в обмін на доступ до сервісу!

Ця революція лише розпочинається, оскільки обсяг даних зростає ще більше, наприклад, через Інтернет речей (див. Інформаційний матеріал 23 про Інтернет речей), а аналіз даних стає більш ефективним завдяки збільшенню обчислювальної потужності, а також досягненням у техніці аналізу даних (штучний інтелект тощо).

КОРИСТЬ ДЛЯ ОСВІТИ

- Великі дані містять потужний потенціал оптимізації та полегшення багатьох елементів вашого життя: уточнення ваших пошукових запитів, гарантування, що ваша поїздка на роботу або з роботи чи школи займає мінімум часу та що ви завжди знайдете потрібні вам продукти у вашому місцевому магазині тощо.
- Дізнатися про великі дані та про те, як вони працюють, важливо для того, щоб використати їх силу та гарантувати, що вони працюють на вас, а не проти вас. Це передбачає ретельний вибір типу даних, якими ви готові ділитися, та вибір сервісів і продуктів на основі характеру використання ними даних.
- Великі дані також можуть слугувати для того, щоб допомогти зрозуміти наші суспільства, даючи можливість вперше в історії людства аналізувати та осмислювати великі маси даних, що генеруються людьми. Для соціальних наук, психології, поведінкових наук, охорони здоров'я, маркетингу та багатьох інших областей досліджень великі дані є справжнім проривом. Висновки, зроблені в цих областях знання, можуть бути використані вчителями для ілюстрування певних соціологічних концепцій реальними прикладами та цифрами.
- Поширеність онлайн-бізнес-моделей, що покладаються на дані, а не на реальні гроші як основне джерело доходу також створює потребу в нових навичках, як-от: управління персональними даними та навички захисту конфіденційності. Отже, подібно до відповідального управління особистим бюджетом і фінансами та уникання надмірного витрачання коштів, людям також доведеться вчитися відповідально керувати своїми персональними даними та не поширювати їх надмірно.

ЕТИЧНІ МІРКУВАННЯ ТА РИЗИКИ

Конфіденційність та захист даних

Хоча багато законів захищають дані та конфіденційність фізичних осіб, насправді їх важко реалізувати. Загальний регламент про захист даних вимагає, щоб сервіси запитували явну згоду користувача, але це, швидше за все, лише розширить масштаб вправи із проставляння «галочок», подібно до згоди з «умовами надання послуг»: клієнт або приймає їх, або відмовляється від послуги. Користувачі часто не мають детального контролю над своїми даними і стикаються з вибором: ділитися усім або нічим. Навіть якщо Загальний регламент про захист даних намагається вирішити проблему згоди споживачів, вводячи принцип пропорційності (тобто сервіс, що вимагає доступу до даних споживачів, може це робити, лише якщо він реально потребує таких даних для надання послуги), тлумачення та застосування Регламенту на практиці може бути недостатньо для захисту користувачів. Наприклад, чи потребують соціальні мережі ваших даних для сортування стрічки новин?

Самі поняття конфіденційності та захисту даних потребуватимуть подальшого розвитку в найближчі роки. Що означає конфіденційність? Чи можна використовувати ваші дані доти, доки їх неможливо простежити до вас? Як ви можете більш детально контролювати ступінь поширення та використання ваших даних, враховуючи величезний обсяг даних, що створюються користувачами щодня?

Стандартизація, конформізм та стагнація

Великі дані – це благо для оптимізації. Громадський транспорт, охорона здоров'я та лікарні, міське планування – всі ці сектори можуть отримати користь від аналізу даних, згенерованих користувачами, пацієнтами та громадянами, щоб бути більш ефективними. А що, якщо ви не такі, як усі? Що робити, якщо ви дістаєтесь до роботи в незвичні години, якщо у вас унікальна хвороба, чи якщо ви не хочете дотримуватися «нормального» способу життя? Якщо всі послуги навколо вас організовані більш ефективно на основі великих даних, ви як особа, разом із вашими унікальними прагненнями та потребами, можете залишитися поза увагою.

Але великі дані також можна використовувати для пристосування послуги до ваших потреб: наприклад, пошукові системи налаштовують результати пошуку на основі попередніх пошукових запитів та будь-яких інших даних про вас; соціальні мережі показують вам дописи, які можуть вам сподобатися. Однак показ вам лише того, що ви хочете побачити, або того, що вам подобається бачити, може мати негативний ефект і викликати особисту стагнацію. Наприклад, якщо ваші політичні уподобання та переконання будуть правими чи лівими, то подача лише таких інформації та контенту, що підтримують ваші погляди, може бути приємною для вашого его, але матиме потужний негативний вплив на формування таких основних цінностей, як демократія, дебати та особистісний ріст – замість цього вас буде «замкнено у своєму колі».

Дискримінація

Щоразу, коли ви підписуєтесь на страхування життя, подаєтесь на вакансію, просите про позику або отримуєте страховку на автомобіль, люди оцінюють вашу компетенцію або ризик, який ви становите. Це може робитися через опитувальник щодо стану здоров'я, в якому запитують, курите ви чи займаєтесь спортом, через співбесіду при прийомі на роботу, під час якої перевіряються ваші вміння, або через перевірку того, як ви останнім часом розпоряджаєтесь своїм бюджетом та чи повернули ви всі взяті кредити. Але де межа між «справедливою» оцінкою та прямим порушенням вашої конфіденційності? Багато роботодавців вже використовують онлайн-інформацію про кандидатів на роботу для ухвалення рішень про прийом, й існує багато натяків на те, що страхові компанії та банки переходять до аналізу онлайн-даних, щоб оцінити ймовірність невиконання Вами зобов'язань за кредитом або серйозних проблем зі здоров'ям. Хоча великі дані можуть врятувати життя завдяки своїм прогностичним можливостям, вони також можуть перешкодити деяким людям отримати доступ до базових фінансових послуг або охорони здоров'я.

Продаж анти-дискримінації

У Інтернеті почали виникати компанії з управління онлайн-репутацією. Підприємства та фізичні особи можуть платити цим компаніям за управління своєю репутацією та отримати гарантію, що їхні дані не позбавляють їх доступу до певних послуг, наприклад, кредитування/інвестиції, страхування чи працевлаштування. Це приклад комерційної експлуатації циклу зовнішніх чинників, подібного до ситуації із забрудненням річки, продажем ліків отруєним громадянам та найманням підприємства для очищення річки.

Маніпуляція та споживацтво

Враховуючи, що найпопулярнішою бізнес-моделлю як для застосунків, так і для онлайн-послуг є «безкоштовна» реклама, часто заснована на експлуатації даних користувачів, існує ризик того, що споживачі будуть отримувати дедалі більшу кількість повідомлень, що заохочують їх споживати. Ринок онлайн-реклами зростає з кожним роком, і нові методи, які змушують споживачів дивитись або клікати на рекламу, швидко розвиваються. Наприклад, заздалегідь записані відеоінтерв'ю з'явилися лише кілька років тому. Великі дані сприяють зростанню ринку реклами, роблячи її більш ефективною та пристосовуючи її до звичок та інтересів людей, а також визначаючи на основі масових даних найефективніший дизайн, місце та метод для перегляду рекламного оголошення та взаємодії з ним.

Політичні переслідування

Хоча деякі уряди поважають приватність і не шпигують за своїми громадянами, багато інших урядів її не поважають. Викриття Едварда Сноудена показали, що уряди з усього світу шпигують за інтернет-користувачами. У деяких випадках це виправдано з міркувань безпеки, наприклад, для боротьби з тероризмом та запобігання терактам, але пропорційність таких дій завжди має ставитися під сумнів. Наприклад, поліція може вивчати профілі в соціальних мережах, щоб ідентифікувати громадян, присутніх на марші протесту.

Права споживачів

Великі дані – це нова онлайн-валюта, але що користувачі отримують натомість? Право на користування онлайн-сервісом, на якому учасників переслідують та закидають нав'язливою рекламою? Коли користувачі вносять щомісячну плату за користування сервісом, вони захищені законодавством про права споживачів і мають право на компенсацію, якщо сервіс чи контент не відповідає їхнім очікуванням або має серйозні недоліки. Користувач може отримати свої гроші назад від онлайн-платформи для зберігання відео, якщо він не може переглядати фільм, але що, якщо ваша улюблена соціальна мережа працює з помилками або непридатна для використання? На яку компенсацію ви матимете право? Зрештою, соціальна мережа використовувала ваші дані, щоб спонукати вас переглядати рекламу, та заробила на цьому гроші. Нова бізнес-модель, що спирається на дані як на валюту, створює багато проблем для прав споживачів; оскільки ця модель нібито «безкоштовна», користувачі часто не мають права на компенсацію, а їхні права дуже обмежені.

Кінець анонімності

Хоча псевдоніми та прізвиська ще не зникли, анонімність перебуває під серйозною загрозою після появи великих даних. Установивши зв'язки між кількома фрагментами анонімних даних, можна ідентифікувати особу за іменем, яке вона використовує онлайн. Навіть дуже обережно ставлячись до інформації, яку ми розміщуємо, найближчим часом будь-кому буде важко залишатися анонімним онлайн, як би там не було.

Інтернет ніколи не забуває

«Право на забуття» набуло популярності з тих пір, як Європейський Союз вжив правових заходів для його реалізації. Утім, це все ще складно зробити на практиці. Цифровий контент можна легко розмістити повторно (у трохи зміненому вигляді, щоб його не впізнали автоматизовані інтернет-боти чи модератори), або розмістити на онлайнових серверах чи сервісах, які не підпадають під дію законодавства ЄС. Тепер кожен може в будь-який час легко знімати фотографії чи відео за допомогою свого смартфона, і це означає, що ви більше не можете грати дурня й діяти безвід-

повідально, перебуваючи на фестивалі, не ризикуючи побачити відео з собою вивантаженим в Інтернет, щоб весь світ із вас посміявся. І все одно треба підтримувати хистку рівновагу між правом на підзвітність та правом на забуття.

Низькоякісні контент і сервіси

Оскільки творці онлайн-сервісів та контенту дедалі більше покладаються на рекламу для отримання доходу, вони намагатимуться оптимізувати привабливість свого сервісу чи контенту. Великі дані допомагають визначити, що робить статтю, фотографію чи відео привабливими, але чи буде це працювати на користь чи проти якісного контенту чи сервісів? Дедалі більше статей, опублікованих онлайн, покладаються на «приманку», щоб спонукати користувачів клікнути на посилання чи допис, а відтак перейти на їхні переповнені рекламою сторінки. Такі заголовки, як «Три найкращі секретні рецепти схуднення», «Ти не повіриш, що робить ця дівчина перед своєю камерою» або «10 найсимпатичніших котів в Інтернеті» дедалі частіше з'являються онлайн. Хоча в розвагах та несистематичному контенті немає нічого поганого, бізнес-модель, що спирається на рекламу, створює сильний стимул створювати лише такий тип контенту на шкоду достовірному контенту чи освітньому контенту.

ІДЕЇ ДЛЯ РОБОТИ В КЛАСІ

Для молоді віком від 14 років: запросіть молодих людей провести пошук за своїм іменем та/або переглянути дані, що вже є про них онлайн, а потім проаналізувати їх з точки зору роботодавця, страховика та державного правоохоронного органу. Спонукайте їх обговорити, як би їх сприймали ці організації, якби проаналізували наявні дані про них. Наприклад, дописи, автори яких діляться статтями про переваги зволікання, або оновлення статусу, що містять багато орфографічних помилок, можуть виглядати дуже погано з точки зору роботодавця. Фотографії, на яких ви зображені в момент, коли курите, п'єте алкоголь або вчиняєте небезпечні дії, будуть виглядати погано для страховика. І нарешті, дописи з критикою вашого уряду та закликами до радикальних змін можуть виглядати підозрілими для правоохоронних органів.

НАЛЕЖНА ПРАКТИКА

- Зрештою, Інтернет та великі дані є лише дальшими кроками технічної революції. Чи будуть кінцеві результати хорошими чи поганими для людства та суспільства, залежить від того, як ми їх застосуємо. Як громадянин та інтернет-користувач ви можете впливати на спосіб використання великих даних, заохочувати ініціативи, що працюють на благо суспільства, і ліквідувати ті, що суперечать суспільним інтересам. Наприклад, як громадянин, ви можете проголосувати за тих творців політики, які просувають суворі етичні стандарти щодо використання даних; як інтернет-користувач, ви можете підтримати сервіси та компанії, які обробляють ваші дані етично та відповідально.
- Будьте в курсі останніх розробок у сфері великих даних, оскільки вони будуть суттєво впливати на ваше повсякденне життя. Це не тільки допоможе вам визначитися з даними, якими ви бажаєте поділитися і які ви обрали для цього, але також допоможе вам визначити та підтримати творців політики та компанії, які відповідають вашим етичним стандартам щодо того, як слід обробляти ваші конфіденційні дані.
- Стежте за всіма сервісами, якими ви користувались, і за всім контентом, який ви розмістили онлайн з самого початку вашої онлайн-присутності, особливо якщо ви починали це робити в молодості! Коментарі чи дописи, які ви опублікували, будучи дитиною чи підлітком, можуть бути легко знайдені, щоб використовуватися проти вас у дорослому житті. Витратьте трохи часу, щоб переглянути те, що ви опублікували, і заархівувати або видалити контент, який більше не відображає вашу нинішню позицію.
- Витратьте необхідний час, щоб продивитися спосіб використання онлайн-сервісами ваших персональних даних, і обирайте їх відповідно. Завжди перевіряйте всі доступні налаштування конфіденційності, щоб установити правильний рівень захисту ваших даних.

ДОДАТКОВА ІНФОРМАЦІЯ

- Приклади великих даних, що використовуються на благо суспільства, можна знайти на вебсайті Комісії ЄС: *<https://ec.europa.eu/digital-agenda/en/what-big-data-can-do-you>.*
- Є також інформація про нормативний акт ЄС про право на забуття: *<http:// ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>*.
- Data & Society (Дані і суспільство) – це американський аналітичний центр, що зосереджує свою увагу на соціальних, етичних і культурних проблемах, що виникають внаслідок технологічного розвитку, в центрі якого перебувають дані: *<http://www.datasociety.net/>*.
- Складено доповідь на тему «Громадянські права, великі дані та наше алгоритмічне майбутнє»: *<https://bigdata.fairness.io/>*.
- Фонд електронного фронтиру пропонує інформацію про захист ваших прав у цифровому світі: *<http://www.eff.org>*.
- Сайт The European Digital Rights (Європейські цифрові права) також пропонує інформацію про захист прав і свобод у цифровому середовищі: *<http://www.edri.org>*.

Для нотаток

Для нотаток

ПОСІБНИК З ІНТЕРНЕТ-ГРАМОТНОСТІ

Підтримка користувачів в онлайн-світі

Посібник українською мовою перекладено та надруковано
за підтримки проекту Ради Європи
«Боротьба з насильством щодо дітей в Україні, Фаза II»

Комп’ютерна верстка:
Н. Тілікіна

Формат 60x90/8
Ум. друк. арк. 17,21
Замовлення №20/10
Тираж 1000 прим.

ТОВ «Агентство «Україна»

Свідоцтво про реєстрацію серії ДК №265 від 30.11.2000 р.

Батьківство у XXI столітті – складне завдання навіть у найкращі часи. Сьогодні діти ростуть у швидкозмінну цифрову епоху та в новому світі, коли батьки можуть не мати достатньо механізмів контролю або взагалі не встигати за інноваціями.

Ця брошура, яку можна читати паралельно з переглядом шести коротких відео (www.coe. int/children), має на меті надати батькам і піклувальникам корисні інструменти й поради щодо захисту дітей в Інтернеті.

У цих матеріалах тренерка з питань цифрового батьківства Елізабет Міловідов, докторка права, дає чіткі практичні поради на особливо делікатну тему захисту дітей від сексуальної експлуатації та насильства в Інтернеті, пояснює терміни та пропонує обґрунтовані рекомендації щодо того, на що батькам потрібно звертати увагу, як поводитися в різних ситуаціях і уникати пасток. Шість тем, які описано в цих рекомендаціях: захист дітей в Інтернеті, сексуальний шантаж, секстинг, сексчатинг, грумінг, порно-реванш.

PREMS 134017

UKR

www.coe.lnt

Рада Європи є провідною правозахисною організацією на континенті. До неї належать 47 держав-членів, 28 із яких є членами Європейського Союзу. Усі держави-члени Ради Європи підписали Європейську конвенцію з прав людини – угоду, покликану захищати права людини, демократію та верховенство права. Європейський суд з прав людини контролює імплементацію Конвенції в державах-членах.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE