

Світлана Доценко
Вікторія Ворожбіт-Горбатюк
Тетяна Собченко

ОНЛАЙН-БЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ В УМОВАХ ДИСТАНЦІЙНОГО І ЗМІШАНОГО НАВЧАННЯ

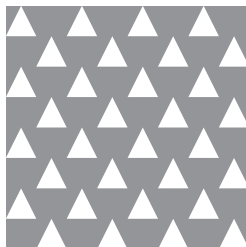
Світлана Доценко
Вікторія Ворожбіт-Горбатюк
Тетяна Собченко



ОНЛАЙН-БЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ В УМОВАХ ДИСТАНЦІЙНОГО І ЗМІШАНОГО НАВЧАННЯ

Схвалено
для використання в освітньому процесі

Харків
Видавництво «Ранок»
2021



УДК 37.018.43:004.056

Д71

Схвалено для використання в освітньому процесі
(Рішення експертної комісії з педагогіки та методики початкової освіти
від 07.10.2021 року (протокол № 8).
Зареєстровано у Каталозі надання грифів
навчальній літературі та навчальним програмам
за № 2.0344-2021)

Видано за рахунок державних коштів. Продаж заборонено

Доценко С. О.

Д71 **Онлайн-безпека учасників освітнього процесу в умовах дистанційного і змішаного навчання : навч.-метод. посіб. / С. О. Доценко, В. В. Ворожбіт-Горбатюк, Т. М. Собченко. — Харків : Вид-во «Ранок», 2021. — 192 с.**

ISBN 978-617-09-7625-3

Онлайн-безпека в інформаційному суспільстві є одним з основних напрямів фундаментальних досліджень у сфері інформаційних технологій, які використовуються під час вивчення практично всіх шкільних дисциплін. Сучасний учитель повинен знати основні принципи безпеки цифрових технологій у професійній діяльності, уміти користуватися засобами кібербезпеки електронних освітніх ресурсів для навчання з урахуванням психолого-педагогічних особливостей учнів.

Запропоновані в цьому посібнику теоретичні матеріали, інструкції, лайфхаки, практичні завдання допоможуть учителям захистити свою діяльність, свої персональні дані від кібератак.

Навчально-методичний посібник призначено для педагогічних працівників закладів загальної середньої освіти.

УДК 37.018.43:004.056



ISBN 978-617-09-7625-3

© Доценко С. О., Ворожбіт-Горбатюк В. В., Собченко Т. М., 2021
© ТОВ Видавництво «Ранок», 2021

РОЗДІЛ I. Організаційний аспект онлайн-безпеки учасників освітнього процесу в умовах дистанційного і змішаного навчання

1.	Нормативне забезпечення дистанційного і змішаного навчання	6
2.	Навчально-методичні посібники для вчителів з організації дистанційного та змішаного навчання в закладах загальної середньої освіти	7
3.	Надпрофесійні навички вчителя: hard skills і soft skills	8
4.	Пам'ятка педагогу щодо організації роботи з учнями в дистанційному та змішаному форматі	10
5.	Електронна шкільна документація	13
	Питання для самоконтролю	15
	Практичні завдання	16
	Рекомендовані джерела	16

РОЗДІЛ II. Онлайн-середовище та безпека

1.	Інтернет-залежність — вада сучасного цифрового суспільства	17
2.	Захист персональних даних	23
3.	Електронний цифровий підпис (ЕЦП)	38
4.	Надійний пароль	42
5.	Водяні знаки — захист авторських прав на світлини, рисунки, зображення	51
6.	Пароль на флешку, папку, файл	57
7.	Батьківський контроль	69
8.	Мобільні додатки батьківського контролю	76
9.	Екранний час. Цифровий добробут	83
	Питання для самоконтролю	84
	Практичні завдання	85
	Рекомендовані джерела	85

РОЗДІЛ III. Емоційний комфорт в онлайн-еdukаціях

1.	Принципи співпраці психологів і освітян щодо підтримки, збереження психічного здоров'я дитини	86
2.	Комунікативна активність як базис психологічного здоров'я	91
3.	Формування в підлітків безпечної поведінки в інтернет-мережі	95
4.	Мережевий етикет учасників форумів та чатів	101

5.	Безпека користування електронною поштою.....	105
6.	Етика електронного листування	115
7.	Корисні поради щодо використання соціальних мереж.....	116
8.	Інтернет-маркетинг.....	121
9.	Рекомендації для учасників освітнього процесу щодо організації роботи за комп'ютером без шкоди для здоров'я	123
10.	Кібербулінг — ідентифікація та запобігання	129
11.	Критичне мислення для оцінювання інформації.....	141
	Питання для самоконтролю.....	149
	Практичні завдання	149
	Рекомендовані джерела.....	150

РОЗДІЛ IV. Лайфхаки з онлайн-безпеки

1.	Дотримання етикету в месенджерах.....	152
2.	Telegram — це один із найпопулярніших месенджерів.....	152
3.	Інстаграм — це соціальна мережа для обміну фотографіями та відеозаписами.....	154
4.	Правила спілкування у Viber-чаті.....	162
5.	Захист від спаму.....	163
6.	Безпека у використанні ZOOM.....	163
7.	Як визначити, що на комп'ютері є вірус.....	164
8.	Як видалити комп'ютерний вірус.....	164
9.	Корисні поради для безпечної професійної комунікації.....	165
10.	Поради з безпечного з'єднання в публічних Wi-Fi мережах	165
11.	Уважність під час здійснення платежів.....	166
12.	Поради від Емі Макріді для батьків	167
13.	Конфіденційність та безпека веббраузера Google Chrome.....	167
14.	Що таке зумбомбінг та як від нього захиститися.....	168

ДОДАТКИ

1.	Перелік освітніх платформ для організації дистанційного та змішаного навчання в закладах загальної середньої освіти	172
2.	Сервіси та платформи для організації дистанційного та змішаного навчання: можливості, переваги, недоліки	173
3.	Навчальний захід у режимі вебконференції	177
4.	Школа в смартфоні. Освітня платформа HUMAN.....	182
5.	Короткий словник термінів	189

Хто володіє інформацією, той володіє світом.

Вінстон Черчилль

Інформація в сучасному світі — це стратегічний ресурс. Створення інформації може призвести до серйозних наслідків. Отже, забезпечення інформаційної безпеки держави є дуже актуальною задачею.

Закон України «Про основні засади забезпечення кібербезпеки України», прийнятий Верховною Радою України 5 жовтня 2017 року, визначає онлайн-безпеку (кібербезпеку) як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі.

Онлайн-безпека в інформаційному суспільстві є одним з основних напрямів фундаментальних досліджень у сфері інформаційних технологій, які використовуються під час вивчення практично всіх шкільних дисциплін уже з початкової школи. Отже, сучасний учитель повинен знати основні напрями кібербезпеки в Україні та світі, принципи безпеки цифрових технологій у професійній діяльності, засоби забезпечення кібербезпеки системи освіти; уміти безпечно використовувати ресурси інформаційних освітніх систем; інтегрувати засоби кібербезпеки, сучасні інформаційні технології в освітню діяльність; користуватися засобами кібербезпеки електронних освітніх ресурсів для навчання з урахуванням психолого-педагогічних особливостей учнів.

Запропоновані в цьому посібнику теоретичні матеріали, інструкції, лайфхаки, практичні завдання допоможуть учителям, батькам та учням захистити свою діяльність, свої персональні дані від кібератак.

Використовуйте цифрову самооборону!

1. НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ ДИСТАНЦІЙНОГО І ЗМІШАНОГО НАВЧАННЯ

Активне впровадження цифрових освітніх технологій, раціональне поєднання традиційного й дистанційного навчання здобувачів загальної середньої освіти висвітлено в таких нормативно-правових документах, що регулюють їх здійснення:

- Закон України «Про освіту» від 25 вересня 2017 року № 2145-VIII;
- Закон України «Про повну загальну середню освіту» від 16 січня 2020 року № 463-IX;
- Закон України «Про Національну програму інформатизації» від 24 лютого 1998 року № 74/98-ВР (редакція від 16.10.2020);
- Положення про дистанційне навчання, затверджене наказом Міністерства освіти і науки України від 25 квітня 2013 року № 466;
- Наказ Міністерства освіти і науки України від 26 квітня 2004 року № 335 «Про створення Координаційної ради з розвитку системи дистанційного навчання при Міністерстві освіти і науки»;
- Програма розвитку системи дистанційного навчання на 2004–2006 роки, затверджена постановою Кабінету Міністрів України від 23 вересня 2003 року № 1494;
- Розпорядження Кабінету Міністрів України від 3 березня 2021 року № 167-р «Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації»;
- Рамка цифрових компетентностей для громадян України (2021);
- Закон України «Про внесення змін до деяких законодавчих актів України, спрямованих на забезпечення додаткових соціальних та економічних гарантій у зв'язку з поширенням коронавірусної хвороби (COVID-19)» від 30 березня 2020 року № 540-IX;

2. Навчально-методичні посібники для вчителів

- Санітарний регламент для закладів загальної середньої освіти, затверджений наказом Міністерства охорони здоров'я України 25 вересня 2020 року № 2205;
- Наказ Міністерства освіти і науки України від 16 березня 2020 року № 406 «Про організаційні заходи для запобігання поширенню коронавірусу COVID-19»;
- Лист Міністерства освіти і науки України від 23 березня 2020 року № 1/9-173 «Щодо організації освітнього процесу в закладах загальної середньої освіти під час карантину».
- Концепція цифрової трансформації освіти і науки від 25 травня 2021 р.

Зміна парадигми освіти в останні роки висуває перед системою вищої освіти вимогу до вдосконалення підготовки вчителів, підвищення їхнього професіоналізму, педагогічної компетентності, здатності використовувати інноваційні форми, засоби й методи навчання.

Процеси, які відбуваються в суспільстві, освіті, призвели до розриву між інформаційно-інноваційними перетвореннями та рівнем використання наукових і технологічних досягнень у навчанні. Особливо відчутним це стало з упровадженням таких форм навчання, як змішане та дистанційне, що увійшли 2020 року в усі заклади освіти та стали випробовуванням для всіх учасників освітнього процесу.

2. НАВЧАЛЬНО-МЕТОДИЧНІ ПОСІБНИКИ ДЛЯ ВЧИТЕЛІВ З ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО ТА ЗМІШАНОГО НАВЧАННЯ В ЗАКЛАДАХ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ

- Дистанційне навчання: виклики, результати та перспективи. Порадник. З досвіду роботи освітян міста Києва: Навч.-метод. посіб. /упоряд. І. П. Воротнікова, Н. В. Чайковська. — Київ : Київ. ун-т ім. Бориса Грінченка, 2020. — [Електронний ресурс]. — Режим доступу: <https://don.kyivcity.gov.ua/files/2020/8/19/90.pdf> (дата звернення 15.07.2021).
- Дистанційне та змішане навчання у школі. Путівник /упоряд. І. П. Воротнікова. — Київ : Київ. ун-т

ім. Бориса Грінченка, 2020. — [Електронний ресурс]. — Режим доступу: <https://drive.google.com/file/d/1ZdbMMlyz8OTbmisaVmmqL23yqisRyTuC/view> (дата звернення 15.07.2021).

- Організація дистанційного навчання в школі: Метод. рек. / Алевтина Лотоцька, Оксана Пасічник; упоряд. Іванна Коберник, Зоя Звєняцьківська; Міжнародний фонд «Відродження»; ГО «Смарт освіта»; Міністерство освіти і науки України, 2020. — [Електронний ресурс]. — Режим доступу: https://nus.org.ua/wp-content/uploads/2020/06/GRYF_Metodychni_rekomendatsii_dystantsiy-na_osvita_razvoroty.pdf (дата звернення 15.07.2021).
- Організація освітнього процесу в школах України в умовах карантину: Аналітична записка / Л. Гриневич, Л. Ільч, Н. Морзе, В. Прошкін, І. Шемелинець, К. Линьов, Г. Рій. — Київ: Київ. ун-т ім. Бориса Грінченка, 2020. — [Електронний ресурс]. — Режим доступу: <http://elibrary.kubg.edu.ua/id/eprint/31739/> (дата звернення 15.07.2021).

3. НАДПРОФЕСІЙНІ НАВИЧКИ ВЧИТЕЛЯ: HARD SKILLS I SOFT SKILLS

Hard skills (з англ. «жорсткі» навички) — професійні навички, яких можна набути та які можна виміряти. Для набуття hard skills необхідно засвоїти знання та інструкції. Якість навчання можна перевірити за допомогою заліку або іспиту. Приклади hard skills: набирання тексту на комп'ютері, водіння автомобіля, читання, знання іноземної мови, використання комп'ютерних програм тощо.

Soft skills (з англ. «м'які» навички) — універсальні компетенції, які важко виміряти кількісними показниками. Іноді їх називають особистими якостями, тому що вони залежать від характеру людини та набуваються з особистим досвідом. Приклади soft skills: соціальні, інтелектуальні та вольові компетенції, такі як комунікабельність, уміння працювати в команді, креативність, пунктуальність, урівноваженість.

Терміни *hard skills* i *soft skills* уперше виникли у військовій справі. У 1959 році армія США почала розробляти науково обґрунтований підхід до підготовки військовослужбовців. У ході розробки дослідники виявили важливість для військовослужбовців не тільки професійних навичок (*hard skills*), а й універсальних компетенцій (*soft skills*), які не піддаються системному навчанню.

Розуміння відмінностей між *soft skills* i *hard skills* було виражено в доктрині «Системи проектування військової підготовки» у 1968 році таким чином: *hard skills* є навичками роботи переважно з машинами, а *soft skills* — навичками роботи з людьми й паперами. Після того як терміни прижилися у військовій науці й психології, їх почали використовувати у сфері бізнесу. Сьогодні в резюме можна зустріти замість розділів «професійні навички» i «особисті якості» — *hard skills* i *soft skills*.

Щоб розвивати *hard skills* необхідний інтелект (ліва півкуля мозку, IQ, логіка). Для розвитку *soft skills* потрібна «емоційність» (права півкуля мозку, EQ, емпатія).

Вимоги до *hard skills* залишаються незмінними незалежно від компанії, у якій ви працюєте, людей i корпоративної культури. *Soft skills*, навпаки, мінливі й ситуативні. Наприклад, програмування належить до професійних навичок (*hard skills*): правила створення гарного програмного коду будуть однакові для будь-якого програміста в будь-якій компанії. Комунікативні навички належать до універсальних компетентностей (*soft skills*): правила побудови промови залежатимуть від аудиторії, до якої звертається мовець, від мовної ситуації (розмова в метро або виступ на конференції).

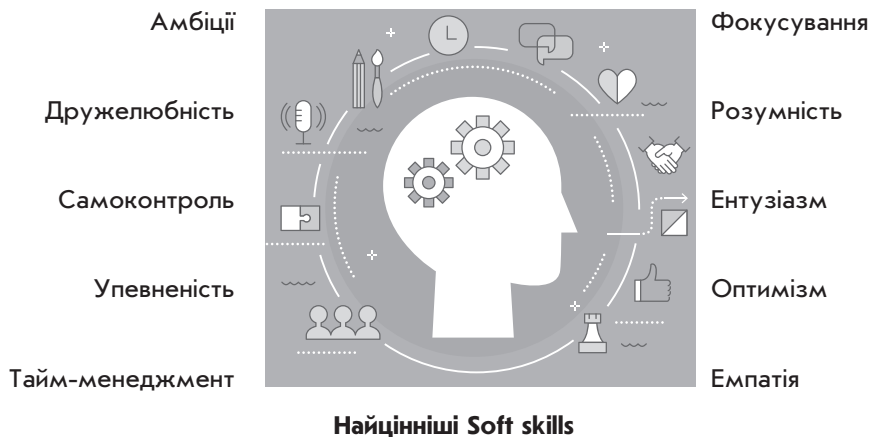
Опанувати *hard skills* можна в різних навчальних закладах (школах, університетах, на додаткових курсах). Зазвичай для них визначаються певні рівні складності, за якими можна поступово підніматися, як по сходах. Наприклад, володіння англійською мовою ділиться на рівні А, В та С. Щоб отримати новий рівень, необхідно скласти іспит. На відміну від *hard skills*, для засвоєння *soft skills* не існує легких покрокових інструкцій: людина або має будь-яку якість від народження (наприклад, дружелюбність, спокійний характер), або набуває його з досвідом, шляхом спроб i помилок

(наприклад, вміння працювати в команді, лідерські якості). Soft skills опановуються повільніше, ніж hard skills.

Hard skills підтверджуються сертифікатами й дипломами про те, що співробітник має необхідні професійні навички. Soft skills не мають сертифікації й довести їх наявність набагато важче.

Удосконалювати hard skills можна за допомогою навчальних центрів (курси підвищення кваліфікації, програми професійної перепідготовки). При цьому для таких навичок характерні кілька рівнів складності. Опанування кожного рівня закінчується складанням іспиту, атестацією, перевіркою. Доведенню hard skills до автоматизму сприяє щоденна практика під час роботи.

Soft skills формуються на особистому досвіді, шляхом спроб і помилок. Прискорити розвиток допоможуть особистісні тренінги, майстер-класи, спілкування, самонавчання та розвиток у процесі роботи, корпоративні програми навчання.



4. ПАМ'ЯТКА ПЕДАГОГУ ЩОДО ОРГАНІЗАЦІЇ РОБОТИ З УЧНЯМИ В ДИСТАНЦІЙНОМУ ТА ЗМІШАНОМУ ФОРМАТІ НАЛАШТУВАННЯ

- Слід налаштуватися на особливості навчання онлайн. Учні/учениці повинні виявляти старанність

4. Пам'ятка педагогу щодо організації роботи з учнями

у самостійному вивченні матеріалу, а вчитель / вчителька здійснюватиме контроль за виконанням завдань.

- Перегляньте навчальну програму та визначте теми, які потребують вивчення в обов'язковому порядку, повторення або перенесення на наступний навчальний рік.
- Відкоригуйте календарно-тематичний план з урахуванням використання дистанційних освітніх технологій

ВИБІР ПЛАТФОРМИ НАВЧАННЯ

- Оберіть онлайн-платформу для взаємодії з учнями / ученицями, яка містить навчальний контент, адже від цього залежатиме якість навчання.
- Створіть навчальний контент (презентації, відеоуроки, відеолекції, тести) із використанням сервісів мережі інтернет для комплексної організації навчання

ВИБІР ФОРМИ ТА МОДЕЛІ НАВЧАННЯ

- Якщо заняття проходитимуть у режимі онлайн (синхронно), скористайтесь безкоштовними сервісами.
- У разі асинхронного режиму оберіть платформу з онлайн-уроками.
- Виберіть модель дистанційного та змішаного навчання («Ротація за станціями», «Перевернутий клас», «Гнучка», «Самостійне змішування», «Поглиблена віртуальна модель»)

СКЛАДАННЯ РОЗКЛАДУ ЗАНЯТЬ

- Фіксуйте навчальний час (оптимально — перша половина дня).
- Узгодьте розклад із колегами.
- Не перевантажуйте дитину обсягом вивчення матеріалу (виконання завдання — не більше 45–60 хвилин).
- Дотримуйтесь санітарних норм відповідно до вікових категорій учнів / учениць.
- Робіть дні занурення в предмет учнів / учениць основної та старшої школи.
- Повідомте розклад дітям та батькам

ОРГАНІЗАЦІЯ ЗВОРОТНОГО ЗВ'ЯЗКУ

- Налагодьте комунікативний контакт з учнями / ученицями за допомогою сервісів, платформ, чатів, пошти.
- Надавайте роз'яснення, коментуйте, відповідайте на запитання

ОСОБЛИВОСТІ ПОБУДОВИ УРОКУ

- Використовуйте чергування теорії та практики, асинхронного та синхронного режимів.
- Слідкуйте за часом (5–10 хвилин на виконання одного завдання).
- Чітко визначайте час для виконання завдання та критерії оцінювання

ІНТЕРАКТИВНІСТЬ

- Залучайте до роботи кожного учня / ученицю.
- Організуйте групову, проєктну роботу за допомогою сучасних сервісів.
- Створюйте вебквести, вікторини, кросворди до тем уроку.
- Використовуйте інтерактивну дошку, наприклад Padlet

ЗВ'ЯЗОК ІЗ БАТЬКАМИ

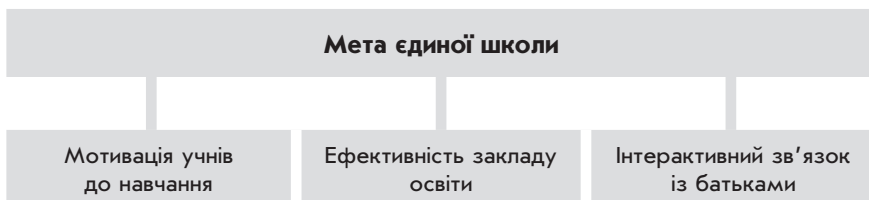
- Створіть чат із батьками (електронний щоденник, Viber, Twitter, WhatsApp, Telegram тощо).
- Допоможіть батькам зареєструватися на освітніх онлайн-платформах.
- Створіть пам'ятку для батьків із відповідями на запитання, що виникають найчастіше, і розмістіть у спільному чаті

НЕМАЄ ІНТЕРНЕТУ

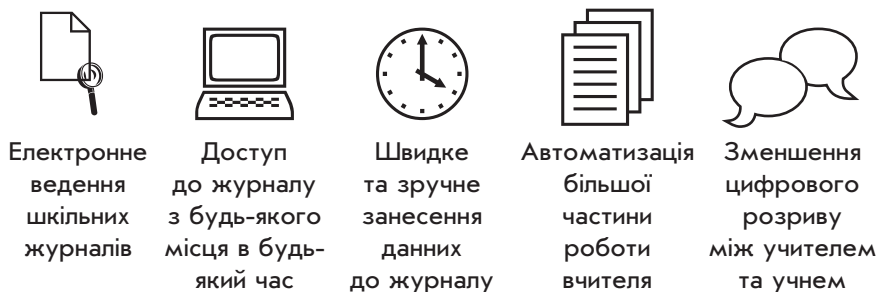
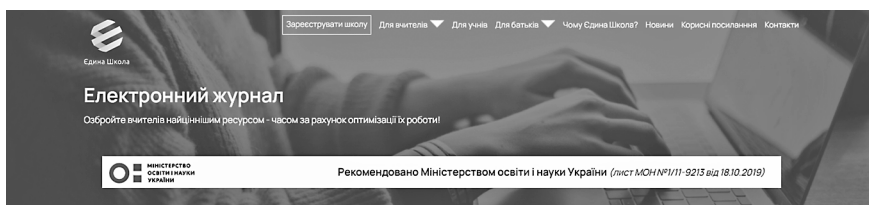
- Майте роздруковані завдання та матеріали.
- Складіть з учнями план дій на випадок відсутності інтернету.
- Продумайте систему своєчасного доставляння матеріалів від учителя до учня й навпаки

5. ЕЛЕКТРОННА ШКІЛЬНА ДОКУМЕНТАЦІЯ¹

Цифрові технології мають допомогти вчителю «автоматизувати більшу частину своєї роботи, вивільняючи час на пошук, спілкування, самовдосконалення, індивідуальну роботу з учнями, забезпечують зворотний зв'язок, підвищують ефективність управління навчальним процесом та освітою в цілому» (*З Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки*).



E-schools.info — сучасний сервіс електронних щоденників і журналів. За умови підключення закладу освіти до цієї платформи можна використовувати цей сервіс. Для цього потрібно залишити заявку на сторінці **Підключити школу**.



¹ «Нормативні документи під час карантину: журнали, заміни, взаємодія з педагогами» (див.: <https://osvitoria.media/experience/9-pytan-shchodo-klasno-gzurnal-na-dystantsijtsi/>).

Користувачами можуть бути адміністрація, учителі, батьки, учні, маючи певні права та доступ до інформації.

Уся електронна документація має паперовий прототип.

Користувачі сервісу мають можливість переглядати розклад уроків, тривалість семестрів, канікул.

Платформа забезпечує зручність ведення персональної сторінки кожного користувача й налагодження комунікативних зв'язків усередині школи.

Інформація надається в різному вигляді:

- Журнал.
- Щоденник.
- Таблиця успішності.
- Графіки успішності кожного класу й учня/учениці.
- Звіти для вчителя/вчительки після закінчення навчального періоду.

Класний журнал — це обов'язковий паперовий або електронний документ закладу загальної середньої освіти, у якому фіксуються результати навчальних досягнень учнів, відвідування ними занять, стан виконання навчальних програм тощо.

Батькам та учням журнал недоступний.

Можливості та переваги електронного журналу:

- сучасно, перехід на безпаперову форму;
- друк будь-якої сторінки;
- збереження в архівному файлі;
- імпортування / експортування даних;
- облік оцінок;
- контроль та відзначення відсутніх;
- автоматичний розрахунок середньої оцінки за чверть;
- вибір типу уроку;
- вибір оцінки (поточна, тематична, підсумкова, семестрова, річна);
- облік заміненних уроків;
- запис домашніх завдань (прикріплення файлів);
- коментарі до уроків;



- написання зауважень до записів;
- таблиця успішності учнів та рейтинг класу;
- статистика успішності в графічному вигляді (за предметами, класами тощо).

На підставі даних, унесених учителями до журналів, для кожного учня формується його електронний щоденник.

Можливості та переваги електронного щоденника:

- для кожного учня — окрема сторінка щоденника;
- запис розкладу уроків (кабінетів);
- оголошення шкільних новин та подій;
- інформація про записи, пропуски, зауваження, поведінку;
- залучення батьків до освітнього процесу;
- майданчик для зворотного зв'язку між учителями та батьками;
- можливість «підписати» щоденник (батьки мають доступ до всіх даних тільки своєї дитини);
- запис домашніх завдань та коментарів щодо їх виконання.



ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Які нормативно-правові документи визначають упровадження комп'ютерних освітніх технологій у закладах загальної середньої освіти?
2. Схарактеризуйте 6 сфер, компетентності та дескриптори, які визначені в «Рамці цифрових компетентностей громадян України».
3. Які фактори було враховано під час адаптації «Рамки цифрових компетентностей країн ЄС» в Україні?
4. Які вам відомі освітні платформи, що розкривають питання організації дистанційного та змішаного навчання в закладах загальної середньої освіти?
5. За допомогою яких сервісів можна створити навчальний відеоконтент?

ПРАКТИЧНІ ЗАВДАННЯ

1. Створити інфографіку за допомогою сервісу Canva на тему «Гейміфікація процесу навчання».
2. Виділити дидактичні можливості сервісу PlayPosit.
3. Розробити та презентувати логотип (сервіс на вибір) навчальної дисципліни.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА

1. Дистанційне навчання: виклики, результати та перспективи. Порадник. З досвіду роботи освітян міста Києва : Навч.-метод. посіб./упоряд. І. П. Воротнікова, Н. В. Чайковська — Київ : Київ. ун-т ім. Бориса Грінченка, 2020. [Електронний ресурс]. — Режим доступу : <https://don.kyivcity.gov.ua/files/2020/8/19/90.pdf> (дата звернення 15.07.2021).
2. Дистанційне та змішане навчання у школі. Путівник/упоряд. І. П. Воротнікова. — Київ : Київ. ун-т ім. Бориса Грінченка, 2020. [Електронний ресурс]. — Режим доступу : <https://drive.google.com/file/d/1ZdbMMlyz8OTbmisaVmmqL23yqisRyTuC/view> (дата звернення 15.07.2021).
3. Організація дистанційного навчання в школі : Метод. рекомендації/А. Лотоцька О. Пасічник. — ГО Смарт освіта, 2020. [Електронний ресурс]. — Режим доступу : https://nus.org.ua/wp-content/uploads/2020/06/GRYF_Metodychni_rekomendatsii_dystantsiy-na_osvita_razvoroty.pdf (дата звернення 15.07.2021).
4. Організація освітнього процесу в школах України в умовах карантину: аналітична записка/Л. Гриневич, Л. Ільїч, Н. Морзе, В. Прошкін, І. Шемелинець, К. Линьов, Г. Рій. — Київ : Київський університет імені Бориса Грінченка, 2020. [Електронний ресурс]. — Режим доступу : <http://elibrary.kubg.edu.ua/id/eprint/31739/> (дата звернення 15.07.2021).
5. Собченко Т. М. Змішане навчання як засіб активізації адаптивних процесів у вищій педагогічній освіті // Адаптивне управління: теорія і практика [Електронне видання]. — Серія «Педагогіка». — 2020. — Вип. 9 (17). [Електронний ресурс]. — Режим доступу : <https://amtp.org.ua/index.php/journal/article/view/340> (дата звернення 15.07.2021).

1. ІНТЕРНЕТ-ЗАЛЕЖНІСТЬ — ВАДА СУЧАСНОГО ЦИФРОВОГО СУСПІЛЬСТВА

Сучасна людина є своєрідним заручником високих технологій. Важко відволікти увагу дитини від смартфона чи монітора комп'ютера? Ваша дитина повсякчас щось шукає в мережі чи копіює з неї? Це може свідчити про інтернет-залежність. Ми порадимо, як цьому запобігти.



Інтернет-залежність (або **інтернет-адикція**) — нав'язливе й неконтрольоване бажання людини підключатися до мережі інтернет і нездатність свідомо відключитися, вийти з мережі.

Термін «інтернет-залежність» увів Айвен Голдберг у 1996 році для опису несвідомо довгого перебування людини в інтернеті.

На цей час до 38 % дорослого населення мають інтернет-залежність.

СИМПТОМИ ІНТЕРНЕТ-ЗАЛЕЖНОСТІ

Ознаки та симптоми інтернет-залежності можуть мати емоційні або фізичні прояви.

Емоційні	Фізичні
• Депресія • Нечесність • Почуття провини • Занепокоєння • Ейфорія від використання комп'ютера	• Синдром зап'ястного каналу • Головні болі • Безсоння • Збільшення або зменшення ваги

Емоційні	Фізичні
• Неможливість визначити пріоритети або дотримуватися розкладу • Ізоляція, самоізоляція • Утрата відчуття часу • Уникнення інших видів діяльності • Агітація • Перепади настрою • Страх • Самотність • Нудьга, рутинність • Прокрастинація	• Розлади харчування (відмова від їжі або переїдання, щоб не перебувати далеко від комп'ютера) - Погана особиста гігієна (наприклад, відмова від купання, щоб залишатися в мережі) • Біль у шиї • Відчуття сухого ока, інші проблеми із зором

МЕТОДИ ЛІКУВАННЯ ІНТЕРНЕТ-ЗАЛЕЖНОСТІ

- Індивідуальна, групова, сімейна терапія.
- Модифікація поведінки.
- Діалектична поведінкова терапія (ДПТ).
- Когнітивно-поведінкова терапія (КПТ).
- Кінна терапія.
- Арт-терапія.
- Рекреаційна терапія.
- Реалістична терапія.

ЧИМ НЕБЕЗПЕЧНА ІНТЕРНЕТ-ЗАЛЕЖНІСТЬ

Формується пасивне мислення. Проведені дослідження щодо інтернет-залежності свідчать про те, що тривале й неконтрольоване перебування в мережі формує пасивне мислення в людини, сприяє зниженню рівня інтелекту та погіршення пам'яті.

Втрачаються комунікативні навички. Людина, яка звикла до спілкування через чати та відеозв'язок, не потребує реального спілкування. Така людина втрачає комунікативні навички, стає відлюдною та неуважною, може зазнати депресії. Можуть виникнути труднощі в реальному спілкуванні, у комунікації з новими людьми, а перебування в незнайомій компанії для інтернет-залежної людини є стресом.

Поступово така людина заглиблюється в себе, що негативно відбивається на роботі чи навчанні. Виникають проблеми зі сном (позбутися безсоння без допомоги фахівця для інтернет-залежної людини фактично неможливо) і розлади харчової поведінки.

Порушуються взаємини в сім'ї. Інтернет-залежність може стати причиною порушення стосунків у сім'ї між батьками і дітьми, між подружжям. Поступово інтернет-залежність віддаляє членів родини духовно, втрачаються родинні традиції, посилюється непорозуміння між різними поколіннями в родині. Інтернет-залежність часто свідчить про співзалежність батьків і дітей у сім'ях.

Погіршується стан здоров'я. Постійне перебування перед монітором комп'ютера викликає додаткову напругу очей, що призводить до погіршення зору. Довге сидіння може викликати остеохондроз, артроз, сколіоз, стати причиною захворювань серцево-судинної системи, варикозу.

КЛАСИФІКАЦІЯ ЗАЛЕЖНОСТІ ВІД ІНТЕРНЕТУ

Нав'язливий вебсерфінг:	• нескінченні подорожі по всесвітній павутині, пошук інформації.
Пристрасть до віртуального спілкування та знайомств:	• постійне листування, участь у чатах, веб-форумах, надмірна кількість віртуальних знайомих і друзів.
Нав'язлива фінансова потреба:	• непотрібні покупки в інтернет-магазинах (оніоманія) або постійна участь в інтернет-аукціонах.
Емоційна залежність:	• відчуття залежності від людей, низька самооцінка; потреба у постійному схваленні й підтримці з боку інших, щоб відчувати, що у вас усе йде добре.
Ігрова залежність:	• неконтрольована пристрасть до ігор, потреба в зовнішніх стимуляторах для відволікання від особистих переживань.

ОЗНАКИ ІНТЕРНЕТ-ЗАЛЕЖНОСТІ В ДИТИНИ

Якщо ви, спостерігаючи за дитиною, побачили деякі з перелічених нижче ознак, варто приділити більшу увагу цій проблемі.

- Дитина проводить у глобальній мережі більше вільного часу, ніж зазвичай. Її важко відволікти від цього заняття.
- Дитина неспокійно спить уночі.
- У дитини знижується успішність у навчанні, вона стає розсіяною та неуважною.
- Віртуальне спілкування витісняє реальне. Дитина не спілкується з однолітками, пропускає школу й секції, не цікавиться прогулянками.
- У дитини спостерігаються порушення режиму дня, харчові розлади.
- Нестабільний емоційний стан у дитини, часта зміна настрою, нещирість.
- У дитини з'явилася потреба бути онлайн постійно. Прагнення регулярно перевіряти соціальні мережі й онлайн ігри. Якщо дитина залишається без інтернету якийсь час, то стає агресивною, дратівливою, може із цього приводу влаштувати істеричку.

ТЕСТ НА ВІЯВЛЕННЯ ІНТЕРНЕТ-ЗАЛЕЖНОСТІ ДІТЕЙ

(за С. Кулаковим)

Інструкція. Оцініть кожен вислів за п'ятибальною шкалою: 1 — дуже рідко, 2 — іноді, 3 — часто, 4 — дуже часто, 5 — завжди.

1. Як часто Ваша дитина порушує тимчасові рамки, встановлені Вами для користування мережею?
2. Як часто Ваша дитина забуває про свої домашні обов'язки для того, щоб провести більше часу в мережі?
3. Як часто Ваша дитина бажає проводити час у мережі замість того, щоб провести його в колі сім'ї?
4. Як часто Ваша дитина формує нові відносини з друзями по мережі?
5. Як часто Ви скаржитеся на кількість часу, що проводиться Вашою дитиною в мережі?

6. Як часто навчання Вашої дитини страждає через кількість часу, проведеного нею в мережі?
7. Як часто Ваша дитина перевіряє електронну пошту, перш ніж зайнятися чимось іншим?
8. Як часто Ваша дитина віддає перевагу спілкуванню в мережі?
9. Як часто Ваша дитина чинить опір, коли Ви запитуєте про те, що вона робить в інтернеті?
10. Як часто Ви помічали, що Ваша дитина виходить у мережу проти Вашої волі?
11. Як часто Ваша дитина проводить час у своїй кімнаті, граючи за комп'ютером?
12. Як часто Ваша дитина отримує дивні дзвінки від віртуальних друзів?
13. Як часто Ваша дитина реагує агресивно чи кричить, дратується, якщо її потурбували з приводу перебування в мережі?
14. Як часто Ваша дитина виглядає більш стомленою, ніж коли не було інтернету?
15. Як часто Ваша дитина виглядає закритою, зануреною в себе, коли знаходиться поза мережею?
16. Як часто Ваша дитина лається й гнівається, коли Ви робите зауваження з приводу часу, проведеного в мережі?
17. Як часто Ваша дитина замінює улюблене заняття, хобі на інтернет розваги?
18. Як часто Ваша дитина стає агресивною, коли Ви накладаєте обмеження на час, який вона проводить у мережі?
19. Як часто Ваша дитина бажає замість прогулянок із друзями проводити час у мережі?
20. Як часто Ви помічаєте в дитини пригніченість, поганий настрій, нервування, коли вона знаходиться поза мережею, а після повернення в мережу все це зникає?

Якщо сума балів 50–79, батькам потрібно усвідомлювати серйозний вплив інтернету на життя дитини та всієї родини.

Якщо сума балів 80 і вище, у дитини є висока інтернет-залежність і їй потрібна допомога фахівця.

ЯК ПОЗБУТИСЯ ІНТЕРНЕТ-ЗАЛЕЖНОСТІ (ПОРАДИ БАТЬКАМ)

Батьки можуть позбавити свою дитину від інтернет-залежності. Фахівцями різних країн і різного профілю встановлено, що для цього необхідно.

- 1) Якомога більше спілкуватися з дитиною.

Діти, не обділені батьківською увагою, не стануть шукати розради в знищенні монстрів, оскільки не будуть відчувати себе самотніми.

- 2) Залучати дитину до культури і спорту, щоб вона не прагнула заповнити вільний час комп'ютерними іграми.

Якщо в дитини не залишиться часу на комп'ютерні ігри, то й залежності не буде. Цікаво, що 90 % дітей, що займаються спортом чи мистецтвом, не захоплюються комп'ютерними іграми.

- 3) Не сердьтеся на дитину за захоплення іграми. У жодному разі не забороняйте їх. Виняток становлять ігри з насильством і жорстокістю.

Дитяча психологія така: чим більше «не можна», тим сильніше бажання. Тому загострювати увагу на тому, що «комп'ютерні ігри — зло» не варто. Краще знайти їм альтернативу.

- 4) Пояснюйте дитині відмінність між грою та реальністю.

Реалістична комп'ютерна графіка, програми доповненої реальності нівелюють відмінність між віртуальним та реальним світом. Важливо дати зрозуміти, що в реальному житті частіше вчинки і дії незворотні, смерть — це назавжди.

- 5) Акцентуйте увагу дитини на цінності спілкування з батьками, іншими родичами, друзями, на успіху розумової праці й навчання.

Якщо вірити статистиці, 80 % дітей починають захоплюватися комп'ютерними іграми через нестачу спілкування в реальному житті. Допоможіть своїй дитині знайти спільну мову з однолітками, і це стане корисним моментом соціалізації.

- 6) Організуйте дозвілля і відпочинок дитини без комп'ютера.

Знайдіть для своєї дитини заміну комп'ютерній грі з огляду на її особисті здібності, уподобання. Не існує дітей, яких би не цікавило нічого, крім комп'ютера.

- 7) Дитині обов'язково потрібно відчувати вашу любов і турботу, щоб бути впевненою, що її обов'язково зрозуміють і підтримають. Тоді в неї не буде потреби віддалятися від рідних людей, реалізовуватися у віртуальному світі.

Більше половини юних користувачів інтернету шукають у ньому ігри та розваги, яких не вистачає в реальному житті. Вони прагнуть заповнити цю прогалину віртуальними радощами. Якщо ж у дитини буде достатньо захоплень і друзів у реальному житті, у неї не виникне бажання витрачати час на спілкування в мережі.

2. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Одним із головних правових питань в еру цифрових технологій є захист персональних даних.

Персональні дані — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Розпорядник персональних даних — фізична чи юридична особа, яка володіє персональними даними або за законом має право обробляти ці дані від імені власника (Закон України «Про захист персональних даних»).

28 січня — день захисту персональних даних (міжнародне свято).



ЩО ТАКЕ ПЕРСОНАЛЬНІ ДАНІ

Персональні дані: ім'я, по батькові, прізвище, адреса, номери телефонів, паспортні дані, національність, освіта, сімейний стан, релігійні та світоглядні переконання, стан здоров'я, матеріальний стан, дата й місце народження, місце проживання та перебування тощо. Також це дані про особисті майнові та немайнові відносини цієї особи з іншими

особами, зокрема членами сім'ї. До персональних даних належать відомості про події та явища, що відбувалися або відбуваються в побутовому, інтимному, товариському, професійному, діловому житті особи (за винятком даних стосовно виконання повноважень особою, яка обіймає посаду, пов'язану зі здійсненням функцій держави або органу місцевого самоврядування) тощо.

ЩО ТАКЕ «БАЗА ПЕРСОНАЛЬНИХ ДАНИХ»

База персональних даних є впорядкованою сукупністю логічно пов'язаних даних про фізичних осіб:

- що зберігаються та обробляються відповідним програмним забезпеченням, є базою персональних даних в електронній формі;
- що зберігаються та обробляються на паперових носіях інформації, є базою персональних даних у формі картотек.

Виходячи з положень статті 2 Закону, персональні дані одночасно можуть бути упорядковані і в електронній формі, і у формі картотек.

ПІДСТАВИ ДЛЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Підставами для обробки персональних даних є:

- згода суб'єкта персональних даних на обробку його персональних даних;
- дозвіл на обробку персональних даних, наданий власнику персональних даних відповідно до Закону виключно для здійснення його повноважень;
- укладання та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;
- захист життєво важливих інтересів суб'єкта персональних даних;
- необхідність виконання обов'язку власника персональних даних, який передбачений Законом;

- необхідність захисту законних інтересів власників персональних даних, третіх осіб, крім випадків, коли суб'єкт персональних даних вимагає припинити обробку його персональних даних та потреби захисту персональних даних переважають такий інтерес.

ЯК ЗАХИСТИТИ ПЕРСОНАЛЬНІ ДАНІ

- 1) Не зберігати відскановані копії документів (паспорт, ідентифікаційний код, свідоцтво про народження тощо) у хмарних сховищах (Dropbox, Google Drive тощо), на пошті чи у відкритих мережесхрощеннях папках на комп'ютері.
- 2) Не залишати оригінали чи копії таких документів без нагляду, зберігати їх удома в надійному місці.
- 3) Надаючи особисті дані в мережі інтернет, звернути увагу на символ замку в лівій частині адресного рядка: якщо він не зелений, а червоний чи жовтий, це може означати, що сайт ненадійний, тому подумайте, перш ніж залишати важливу інформацію на такому сайті.

ЩО ТАКЕ ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

Згідно із Законом України «Про захист персональних даних» при зарахуванні дитини до школи необхідно отримати обов'язкову задокументовану згоду суб'єктів персональних даних (ст. 2).

Оскільки суб'єктами персональних даних є неповнолітні особи, то згідно з нормами Сімейного та Цивільного кодексів України, згоду на обробку персональних даних дитини мають надати батьки або особи, які їх замінюють. Також батьки повинні подати згоду на обробку власних персональних даних. Це також означає, що заяву про зарахування дитини до школи можуть подати тільки батьки або особи, які їх замінюють. Ніякі інші члени родини, близькі та далекі родичі цього робити не мають права. Із настанням повноліття особа надає таку згоду самостійно, і батьки вже не мають права визначати межі обігу персональних даних їхніх дітей.

Зразок

ЗГОДА

на обробку персональних даних

Я, _____,

(прізвище, ім'я, по батькові)

народився ____ . ____ . ____ року, документ, що посвідчує особу
(серія № _____), виданий _____

_____, відповідно до Закону України «Про захист
персональних даних» даю згоду на:

- обробку моїх персональних даних із первинних джерел у такому обсязі: відомості про освіту, професію, спеціальність та кваліфікацію, трудову діяльність, науковий ступінь, учене звання, паспортні дані, дані про зареєстроване або фактичне місце проживання, біографічні довідки, номери телефонів, дані про мою участь у міжнародних та європейських проєктах;
- використання персональних даних, що передбачає дії власника бази щодо обробки цих даних, у тому числі використання персональних даних відповідно до їх професійних чи службових або трудових обов'язків, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними (стаття 10 Закону);
- поширення персональних даних, що передбачає дії власника бази персональних даних щодо передачі відомостей про фізичну особу з бази персональних даних (стаття 14 Закону);
- доступ до персональних даних третіх осіб, що визначає дії власника бази персональних даних у разі отримання запиту від третьої особи щодо доступу до персональних даних, у тому числі порядок доступу суб'єкта персональних даних до відомостей про себе (стаття 16 Закону).

Зобов'язуюсь у разі зміни моїх персональних даних надавати в найкоротший строк уточнену, достовірну інформацію та оригінали відповідних документів для оновлення моїх персональних даних.

_____ 20__ р. _____ (Підпис)

Після закінчення школи учень отримує документ про освіту — свідоцтво про базову середню освіту та атестат про повну загальну середню освіту.

Згідно з Порядком замовлення, видачі та обліку документів про освіту державного зразка, зареєстрованого в Міністерстві юстиції України 17 вересня 2001 року за № 822/6013, документ про освіту — це персонально-інформаційні дані про освітній чи освітньо-кваліфікаційний рівень випускника навчального закладу України, відтворений у пластиковій картці (п. 1.3). Для замовлення документа про освіту державного зразка навчальний заклад подає зведене замовлення до Державного центру прикладних інформаційних технологій Міністерства освіти і науки України, у якому містяться персональні дані кожного випускника навчального закладу.

Контроль за додержанням законодавства про захист персональних даних відповідно до статті 23 Закону покладено на Державну службу України з питань захисту персональних даних.

ЧИ ПОТРІБЕН ДОЗВІЛ НА РОЗМІЩЕННЯ ФОТО/ВІДЕО З ДИТИНОЮ В ІНТЕРНЕТІ

«Я не хочу, щоби фотографували або знімали на відеокamera мою дитину в школі, дитячому садочку або на вулиці» — такі вислови лунають практично на кожному заході, присвяченому темі захисту персональних даних. Людям не подобається, що світлина їхніх дітей поширюють у мережі без їхнього дозволу, і вони не знають, як цього запобігти.



Відео- або фотозйомка (збір інформації) — це один із видів обробки персональних даних, що регулюється Законом України «Про захист персональних даних». Наприклад, підставою для обробки даних може бути згода, дозвіл, договір або ж інший правочин (стаття 11 Закону).

На відміну від дитини, доросла людина здатна оцінити ризики та самостійно вирішити, чи хоче вона, щоб про неї збирали інформацію, чи ні (у статті 8 Закону визначено права суб'єкта даних). Тому законодавство приділяє окрему

увагу питанням обробки даних малолітніх або недієздатних осіб. У таких випадках необхідно отримувати згоду від батьків, опікунів чи усиновителів, які повністю усвідомлюють значення дій та наслідків, що можуть статися в результаті обробки даних.

ЯК ЗАХИСТИТИ ОСОБИСТУ ІНФОРМАЦІЮ ТА ФОТОГРАФІЇ ДІТЕЙ У МЕРЕЖЕВОМУ ПРОСТОРІ

Зважте на таке спостереження: у мережевому просторі майже кожна сучасна людина формує певний контент про себе. Можливо, краще, якщо сама людина подбає про створення свого образу в мережі. Ваша дитина подорослішає, і з вашою мудрою підтримкою і порадами сформує свій образ самостійно. Якщо ж цей процес почали ви, то і відповідальність за наслідки лежить на вас.



Якщо прагнення розмістити в мережі інформацію про свою дитину велике, то корисно звернути увагу на таке:

- визначте, з якою метою і якого змісту інформацію ви хочете розмістити в мережі, у який спосіб ви контролюватимете безпечність вебресурсу з наданою вами інформацією, хто матиме відкритий доступ до цієї інформації;
- погодьте з дитиною, яку інформацію ви надасте про неї широкій аудиторії, які можуть бути наслідки.

Краще презентувати особисту інформацію на сайтах із високим ступенем захисту. Політика конфіденційності користувачів дає правила й послідовність використання інформації про дитину, період і мету використання такої інформації.

Краще, якщо інформація про дитину буде мінімальною і в межах обсягу обов'язковою. Наприклад, коли реєструєтеся на нову послугу, її постачальник запитує, чи хочете отримувати повідомлення прямого маркетингу, ви можете сказати «Ні» на початку. Якщо випадково дали згоду, то маєте право скасувати, зв'язавшись із постачальником послуги.

Не варто публікувати матеріали із зазначенням номера телефону вашої дитини, адреси проживання чи реєстрації.

Заборонено публікувати матеріали, які містять інформацію про місце знаходження дитини в точний період часу, окрім перебування її в закладі освіти.

Якщо ви оприлюдните фото своєї дитини в мережевому просторі, фактично неможливо запобігти його поширенню. Копії таких фото можуть потрапити до рук недоброчесних людей. Подумайте й робіть такі вчинки розважливо. Не рекомендується виставляти фото неповнолітніх дітей крупним планом, коли в кадрі одна дитина. Коли в кадрі декілька дітей, то не можна виставляти фото без згоди батьків цих дітей.

Перш ніж виставляти фото свого малюка, подумайте, чи не образить це вашу дитину, коли вона стане дорослою. У світовій практиці є випадки, коли з дорослішанням діти знаходили свої дитячі світлини в інтернеті, і це як мінімум їх шокувало, а як максимум — шкодило їхній репутації та можливостям у навчанні та роботі. Зважте також на те, що не завжди люди керуються добрими намірами, шукаючи фото дітей у мережі. Захистіть свою дитину від залучення в сексуальну експлуатацію, від маніпуляторів. Зберігайте фото офлайн.

Розміщення чиеїсь фотографії або особистої інформації, наприклад, на вебсайті школи, вважається розкриттям особистої інформації, яке завжди вимагає згоди від особи, інформацію якої розміщують.

Не потрібно отримувати згоду батьків на фото-, відеозйомку дитини в публічних місцях. Згідно із цивільним законодавством України, «згода особи на знімання її на фото-, кіно-, теле- чи відеоплівку допускається, якщо зйомки проводяться відкрито на вулиці, на зборах, конференціях, мітингах та інших заходах публічного характеру».

Якщо ж для здійснення зйомки (не в публічному місці) потрібно отримати згоду, тоді таку згоду за неповнолітню чи малолітню дитину дають батьки. Якщо повнолітня особа чи батьки малолітньої / неповнолітньої дитини проти зйомки — її потрібно припинити.

У законодавстві немає чітких вимог до форми, у якій може бути виражена згода, тобто вона може бути як усна,

так і письмова. Згода на зйомку особи може виявлятися в конклюдентних діях (які свідчать про згоду особи на таку зйомку), таких як кивок голови чи усмішка в кадр, але треба мати на увазі, що таку згоду може бути важко довести у випадку судового спору. Більше того, дитина ще не розуміє довгострокових наслідків поширення власного зображення, тому її дії не означатимуть згоди на її зйомку.

У таблиці нижче наведено витяги із Цивільного кодексу України (ЦКУ) та приклади реалізації цих положень у контексті фото- чи іншої зйомки дітей (<https://childrenrights.info/photo-dytyny/>).

Стаття 307. Захист інтересів фізичної особи при проведенні фото-, кіно-, теле- та відеозйомок (Ця стаття стосується дозволу на зйомку)	
1. Фізична особа може бути знята на фото-, кіно-, теле- чи відеоплівку лише за її згодою. Згода особи на знімання її на фото-, кіно-, теле- чи відеоплівку припускається, якщо зйомки проводяться відкрито на вулиці, на зборах, конференціях, мітингах та інших заходах публічного характеру	Щодо згоди дитини на фото- чи іншу зйомку існує два правових аспекти: 1) згідно із чинним ЦКУ, до досягнення повноліття батьки або інші законні представники дитини (наприклад, опікуни), приймають рішення щодо здійснення більшості правочинів своєї дитини. Тобто фото- чи інша зйомка дитини може відбуватись тільки за їх згоди; 2) згідно з Конвенцією ООН про права дитини, кожна дитина є суб'єктом, а не об'єктом правовідносин. І провідним принципом Конвенції є право дитини на участь у вирішенні питань, які її стосуються. Це означає, що бажано питати згоду дитини на фото- чи іншу зйомку й у неї самої, а також ураховувати її думку.

2. Захист персональних даних

	Щодо заходів публічного характеру: у законодавстві не існує чіткого та універсального визначення «заходів публічного характеру». Однак переважно вони трактуються як такі, що: а) є вільні для відвідування будь-ким (наприклад, фестиваль вуличної їжі в містах, виставка квітів тощо), б) організатором або співорганізатором є орган публічної влади (тобто державної влади чи місцевого самоврядування)
2. Фізична особа, яка погодилася на знімання її на фото-, кіно-, теле- чи відеоплівку, може вимагати припинення їх публічного показу в тій частині, яка стосується її особистого життя. Витрати, пов'язані з демонтажем виставки чи запису, відшкодовуються цією фізичною особою	Наприклад, якщо під час запису заходів публічного характеру в кадр потрапив фрагмент, який стосується особистого життя, ви можете звернутись до власника запису, і за ваш кошт цей фрагмент буде вирізано
3. Знімання фізичної особи на фото-, кіно-, теле- чи відеоплівку, у тому числі таємне, без згоди особи може бути проведене лише у випадках, установлених законом	Наприклад, у рамках оперативно-розшукової діяльності
Стаття 308. Охорона інтересів фізичної особи, яка зображена на фотографіях та в інших художніх творах (Ця стаття стосується прав тих, хто вже зображений у кадрі)	
1. Фотографія, інші художні твори, на яких зображено фізичну особу, можуть бути публічно показані, відтворені,	Мати фотографію своєї дитини та розповсюджувати її — різні поняття. Те, що ви зберігаєте фото своєї дитини в сімейному

розповсюджені лише за згодою цієї особи	альбомі чи у своєму телефоні, не означає ваш дозвіл чи дозвіл дитини на розповсюдження цієї фотографії через журнали чи соціальні мережі
2. Якщо фізична особа позувала авторові за плату, фотографія, інший художній твір може бути публічно показаний, відтворений або розповсюджений без її згоди	Наприклад, якщо ваша дитина з вашого дозволу брала участь у професійній фотозйомці для журналу в ролі оплачуваної моделі, подальше розповсюдження цих фотографій відбуватиметься без узгодження з вами
3. Фотографія може бути розповсюджена без дозволу фізичної особи, яка зображена на ній, якщо це викликано необхідністю захисту її інтересів або інтересів інших осіб	Окрім посилань на додаткові правові норми, це положення може застосовуватися для пошуку зниклих дітей та для пошуку сімей для дітей-сиріт

Зразок

ДОЗВІЛ БАТЬКІВ

Я, _____
надаю дозвіл публікувати матеріали мого сина (доньки) _____
_____ учня (учениці) _____ класу
(назва закладу освіти повністю) в мережі інтернет на офіційному
сайті закладу, офіційній сторінці фейсбук _____ відповідно
до чинного законодавства.

Небажані для публікації в мережі інтернет:

_____ Ім'я дитини

_____ Особисті фотографії дитини

_____ Фотографії дитини (із занять та заходів закладу освіти)

_____ Групові фотографії із закладу освіти

Підпис батька / опікуна: _____

Дата: _____

ЯК ЗАХИСТИТИ ПЕРСОНАЛЬНІ ДАНІ ПІД ЧАС ДИСТАНЦІЙНОГО НАВЧАННЯ (ПОРАДИ ДЛЯ ПЕДАГОГІВ, БАТЬКІВ ТА УЧНІВ)

У листі МОН України № 1/9-609 від 2 листопада 2020 року «Щодо організації дистанційного навчання» наголошується, що всі учасники освітнього процесу мають дотримуватися вимог щодо захисту персональних даних учасників освітнього процесу в електронному освітньому середовищі.

Заклад освіти має:

- забезпечити захищену та надійну шкільну мережу, а для цього потрібно використовувати послуги офіційного інтернет-провайдера. Під час дистанційного навчання вчителі та учні використовують особисті домашні пристрої, які зазвичай не охоплюються мережевим захистом. У такому випадку вчителям та батькам учнів варто перевірити офіційність та надійність свого інтернет-провайдера, щоб оцінити можливі ризики. Якщо провайдер неофіційний — посилити захист за допомогою програмного забезпечення. Також ключове значення мають проведення для учнів навчання про безпеку в інтернеті, обговорення різних практичних випадків та діалог;
- використовувати програмне забезпечення для фільтрації та моніторингу безпеки пристроїв;
- встановлювати в межах школи політику, що регулює, де і як можуть використовувати технології різні учасники навчального процесу, а також порядок реагування на інциденти, пов'язані з безпекою дітей, зокрема в цифровому середовищі;
- організовувати для учнів навчання з питань онлайнової безпеки;
- забезпечувати достатній рівень підготовки всіх співробітників (зокрема технічного персоналу), а також регулярне підвищення їхньої кваліфікації;
- призначити в школі спеціального координатора й створити можливості для обліку та реєстрації інцидентів, пов'язаних з онлайновою безпекою, щоб сформулювати

цілісне уявлення про наявні в школі проблеми та тенденції, що вимагають уваги;

- ужити заходів для того, щоб адміністративно-управлінський персонал та керівники були достатньо обізнані в питаннях онлайн-безпеки в школі;
- узяти до уваги потенційний вплив інтернету та онлайн-нових технологій на навчання та психіку учнів.

Учителі повинні:

- переконатися в тому, що всі пристрої надійно захищені та на них встановлено пароль. Учителі також уразливі перед кібератаками, шкідливими програмами, вірусами та зламами. Важливо, щоб усі пристрої, які ви використовуєте, захищалися надійним паролем;
- блокувати пристрої, завершувати сеанс і виходити з облікового запису, коли не використовують їх (наприклад, якщо виходять із кімнати або класу);
- встановити антивірусне програмне забезпечення та брандмауер й регулярно їх оновлювати.

Батьки повинні:

- насамперед спілкуватися зі своїми дітьми, цікавитись, що вони люблять переглядати в інтернеті, спробувати організувати спільно з ними будь-яку онлайн-діяльність;
- визначити, які технології, пристрої та послуги використовуються у вас удома;
- установити на всіх пристроях брандмауер та антивірусну програму. Поміркувати над тим, чи будуть корисними та чи підходять для вашої родини програми фільтрації, блокування або відстеження. Розглянути можливість використання контент-фільтрів, що досить часто називаються системами батьківського контролю, і безпечних пошукових систем або обмежень доступу, щоб фільтрувати контент, який діти можуть переглядати в інтернеті;



- у колі родини домовитись про умови використання інтернету й особистих пристроїв, приділяючи особливу увагу питанням конфіденційності, вікової відповідності змісту сайтів, додатків та ігор, булінгу, кількості проведеного перед екраном часу та небезпеки з боку незнайомців;
- пояснити дітям, що перш ніж публікувати світлини або відео в мережі, слід отримати згоду людей, які там зображені. Батькам також варто звертати увагу на те, якою інформацією про своїх дітей вони діляться в соціальних мережах і в інтернеті загалом, зокрема, це стосується особистих історій про дітей або їхніх світлин. Пам'ятати про недоторканність приватного життя дитини;
- пояснити дітям, що не можна повідомляти свої паролі доступу друзям або братам і сестрам. Звертати їхню увагу на те, коли і де вони повідомляють свою персональну інформацію;
- звернути увагу на вік «цифрової згоди». У деяких країнах діють закони, що встановлюють мінімальний вік, починаючи з якого компанії або вебсайти можуть просити дітей повідомити персональну інформацію без попереднього отримання підтвердженої згоди батьків. Вік «цифрової згоди» зазвичай варіюється в межах 13–16 років. На багатьох вебсайтах, призначених для дітей молодшого віку, потрібна згода батьків для реєстрації нового користувача;
- дізнатися, як повідомити про проблему на платформах, якими користуються ваші діти, і як видалити профіль або змінити зазначену в ньому інформацію;
- розказати про важливість персональної інформації. Пояснити дітям, що їм слід ділитися тільки тією інформацією, яку, на вашу і на їхню думку, дозволено побачити стороннім (їм не слід ділитися інформацією, що дозволяє встановити їхню особистість або особистість інших). Нагадати дітям, що в них є онлайн-репутація, за якою необхідно стежити, а після того, як контент опубліковано, його може бути складно змінити або скоригувати;

- переконатися, що діти розуміють, що означає публікація світлин та відео в інтернеті, у тому числі їхніх власних та їхніх друзів. Пояснити дітям, що фотографії та відео можуть розкривати безліч персональної інформації (діти повинні розуміти ризики, пов'язані з використанням камер та опублікуванням контенту).

КУДИ ЗВЕРТАТИСЯ В РАЗІ НЕЗАКОННОЇ ОБРОБКИ ДАНИХ ТА ВТРУЧАННЯ В ОСОБИСТЕ ЖИТТЯ ЛЮДИНИ

У разі незаконної обробки персональних даних та втручання в особисте життя особи суб'єкт персональних даних має право звернутися до власника або розпорядника персональних даних із вмотивованою вимогою:

- заборонити таку обробку;
- внести зміни до своїх персональних даних (у випадку їх недостовірності);
- вимагати їх видалення (знищення).

Якщо ця вимога суб'єкта персональних даних не буде виконана, то особа може оскаржити вказані дії чи бездіяльність власника або ж розпорядника персональних даних в Уповноваженого Верховної Ради з прав людини та/або до суду.

ЯК УБЕЗПЕЧИТИ СВОЇ ПЕРСОНАЛЬНІ ДАНІ В СОЦІАЛЬНИХ МЕРЕЖАХ

Будь-яка соціальна мережа передбачає надання їй деяких відомостей про зареєстрованого користувача. Якщо людина вказує дійсні відомості про себе, то вносить у її інформаційну систему свої персональні дані. І перелік цих даних може бути досить широким — від прізвища, ім'я та по батькові, віку, місця проживання до улюбленого актора, кольору тощо. У зв'язку із цим виникає потреба в захисті особистих даних. Одним із найактуальніших завдань безпеки в даному контексті є забезпечення конфіденційності, тобто надання своїх персональних даних лише заздалегідь визначеному колу осіб у рамках соціальної мережі (наприклад, тільки друзям).

Крім конфіденційності, важливо ще й забезпечення цілісності персональних даних, а також механізмів, що гарантують справжність сторінки користувача. Остання вимога має силу через існуючі сторінки-клони, з яких зазвичай відбуваються дії недобросовісного характеру (нібито від імені власника сторінки).

Тому доцільно навести кілька простих правил, яких потрібно дотримуватися для збільшення особистої безпеки в соціальних мережах:

1) Звертайте увагу на те, кого ви додаєте в друзі.

Шахраї теж ведуть сторінки в соціальних мережах: це їх безпосередній шлях до вашого облікового запису. Додавання вас у друзі дає їм можливість отримати доступ до інформації, яку ви приховали для перегляду незнайомим особам. Природно, що з'являється можливість писати вам приватні повідомлення під приводом якоїсь акції, реклами або приватного листування з метою дізнатися про вас більше, або «підсунути» вірусну програму для отримання ваших особистих даних із метою шахрайських дій. Уважно вивчайте людину, яка пропонує вам «дружбу», а краще ігноруйте такі запити та видаляйте їх.

2) Видаляйте акаунти, якими ви не користуєтесь.

В основної маси користувачів соціальних мереж є сторінки в тій чи іншій соціальній мережі, про які вже давно забули, але ви повинні пам'ятати, що там знаходиться ваша особиста інформація, яку ви, швидше за все, не видалили. Якщо ви вже не користуєтесь такими сторінками, то просто видаліть їх, щоб не залишати вашу інформацію в загальному доступі, навіть якщо вона застаріла: це може бути важелем тиску на вас із боку шахраїв. Та й стежити за всіма своїми сторінками легко за допомогою безлічі різних сервісів, які ви з легкістю зможете знайти в інтернеті.

3) Використовуйте складні паролі.

Простий пароль — це недостатній захист ваших особистих даних, що може призвести до злому з подальшими шахрайськими діями. Отже, встановлюйте складний і унікальний пароль, і краще запам'ятовуйте, а не записуйте, адже втратити «аркушик» із паролями дуже легко.

4) Налаштуйте посилений захист.

Посилений захист — це двофакторна аутентифікація: ще один інструмент для підвищення рівня захисту ваших даних, крім пароля. Це дасть можливість створити ще один бар'єр для входу у ваш акаунт. Різні соціальні мережі надають безліч типів такої аутентифікації, від кодового слова до пароля, який буде приходити до вас на особистий номер телефону, який прив'язаний до сторінки, для підтвердження входу. Це, у свою чергу, сильно ускладнить можливість входу у ваш акаунт третім особам і допоможе знизити ризик втрати важливої інформації.

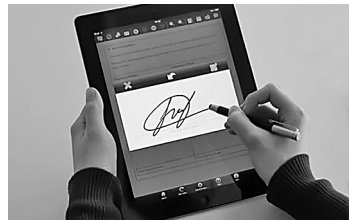
5) Не використовуйте конфіденційну інформацію.

Соціальна мережа створена для спілкування з друзями або однодумцями, але ніяк не для прив'язки акаунтів на якісь сумнівні сайти, які можуть вимагати особисту інформацію про вас або ваших друзів. Звичайно ж, потрібно думати, яку інформацію ви надаєте у вигляді новин: не варто писати, що ви виграли мільйон або зібралися звільнити квартиру для відпочинку на курорті. Це може стимулювати шахраїв на певні неправомірні дії.



3. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС (ЕЦП)

За допомогою послуг електронного цифрового підпису (ЕЦП) можна підписувати електронні документи, користуватися електронними послугами, реєструватися на державних порталах тощо. Документи, підписані за допомогою ЕЦП, мають таку саму юридичну силу, як і паперові оригінали.



Електронний цифровий підпис (ЕЦП) за правовим статусом прирівняний до власноручного підпису або печатки.

3. Електронний цифровий підпис (ЕЦП)

ЕЦП — це дані в електронній формі, отримані за результатами криптографічного перетворення, які додаються до інших даних або документів і забезпечують їх цілісність та ідентифікацію автора.

Електронний підпис — електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються й використовуються ним як підпис.

В Україні з 7 листопада 2018 року, згідно із Законом «Про довірчі послуги» електронний підпис може бути трьох категорій:

- простий електронний підпис та печатка — низький рівень довіри;
- удосконалений електронний підпис та печатка — середній рівень довіри;
- кваліфікований електронний підпис та печатка — високий рівень довіри.

Лише кваліфікований електронний підпис прирівнюється до власноручного (частина 4 статті 18 Закону про ЕЦП).

Щоб отримати підпис офлайн, вам потрібно особисто звернутися до одного з надавачів послуги. Для цього заповніть реєстраційну форму та вкажіть паспортні дані й номер платника податків.

ЧИ Є ЕЛЕКТРОННИЙ ПІДПИС НАДІЙНИМ

У використанні електронного підпису надважливою є впевненість у тому, що він був уведений безпосередньо власником. Тому використання такого підпису відбувається під пасивним наглядом провайдера, який надає послугу.

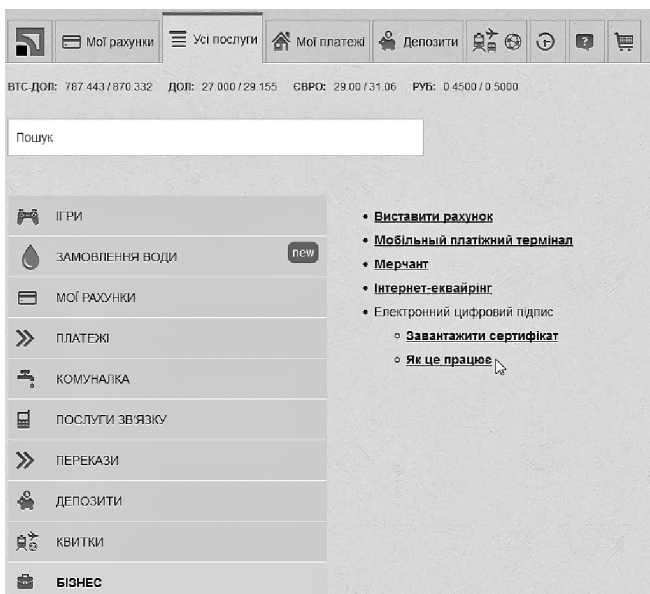
Аби скористатись електронним підписом, користувач завантажує документ на сайт провайдера, накладає свій підпис та надсилає його на електронну адресу другого контрагента. У свою чергу, інший користувач може продивитись інформацію про те, ким він був підписаний, і також додати свій підпис. Згодом у кожного з користувачів буде відображатися підписаний документ з інформацією про осіб, які його підписали.

ЯК ОТРИМАТИ ЦИФРОВИЙ ПІДПИС У ПРИВАТБАНКУ

Перший спосіб

Якщо ви є клієнтом Приватбанку, можете отримати ЕЦП через систему Приват24.

- 1) Зайдіть у меню «Усі послуги»/«Бізнес»/«Завантажити сертифікат».



- 2) Заповніть заявку на отримання сертифіката. Зверніть увагу, що поле «E-mail» обов'язкове для заповнення. Зверніть увагу на написання прізвища, імені та по батькові — вони мають збігатися з паспортними

3. Електронний цифровий підпис (ЕЦП)

даними. Не забудьте перевірити точність написання електронної пошти з дотриманням прописних літер. Після перевірки даних натисніть одну з кнопок: «Дані вірні» або «Дані невірні».

- 3) Оберіть директорию, у якій у вас є права на запис, для створення в ній файлу — сховища ключів.

The screenshot shows the Privat24 web interface. At the top, there is a navigation bar with icons for 'Мои расчеты', 'Услуги', 'Мои платежи', 'Депозиты', and other services. Below the navigation bar, the user's account information is displayed: 'ВТС-ДОЛ: 787.443/870.332', 'ДОЛ: 27.000/29.155', 'ЕВРО: 29.00/31.06', and 'РУБ: 0.4500/0.5000'. A search bar with the placeholder 'Поиск' is visible. The main content area displays the text 'Виберіть директорию для зберігання ключів' (Select a directory for key storage). Below this text are two buttons: '< Назад' (Back) and 'Обрати >' (Select).

- 4) Створіть пароль на файл — сховище ключів. Мінімальна довжина паролю — 8 символів, він має включати у себе букви латинського алфавіту та цифри.

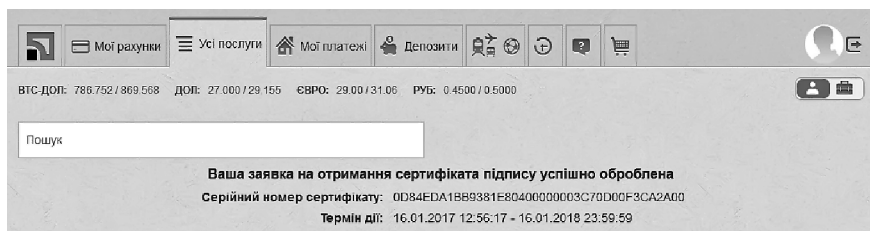
The screenshot shows the Privat24 web interface. The navigation bar and account information are the same as in the previous screenshot. The main content area displays the text 'Ваш ключ буде записано у файл: C:\Program Files (x86)\pb_3269409759.jks' (Your key will be saved to the file: C:\Program Files (x86)\pb_3269409759.jks). Below this text, there are two input fields for creating a password. The first field is labeled 'Вигадайте пароль до сховища ключів' (Create a password for the key storage) and the second field is labeled 'Повторіть пароль до сховища ключів' (Repeat the password for the key storage). Below the input fields, there is a note: 'Мінімальна довжина пароля 8 символів, символи латинського алфавіту і цифри.' (Minimum password length 8 symbols, Latin alphabet and digits). At the bottom, there are two buttons: '< Назад' (Back) and 'Далі >' (Next).

- 5) На наступній сторінці пароль, що надійшов у SMS або мобільному додатку Privat24. Установіть галочку

The screenshot shows the Privat24 web interface. The navigation bar and account information are the same as in the previous screenshots. The main content area displays the text 'На Ваш телефон +380971636396 надіслано SMS з кодом.' (An SMS with the code has been sent to your phone +380971636396). Below this text, there is a prompt: 'Для підтвердження операції введіть код з SMS:' (To confirm the operation, enter the code from the SMS:). There are four input fields for entering the code, each containing the digit '11'. Below the input fields, there is a checkbox with the text 'Я ознайомлений та згоден з умовами та правилами надання банківських послуг і підтверджую коректність введених мною даних.' (I am familiar and agree with the terms and conditions of the provision of banking services and I confirm the correctness of the data entered by me). At the bottom, there are two buttons: '< Назад' (Back) and 'Далі >' (Next).

навпроти пункту «Я ознайомлений та згоден з Умовами та правилами надання банківських послуг і підтверджую коректність даних, відправлених мною» та натисніть «Далі».

- 6) Заявка на отримання сертифіката сформується автоматично. З'явиться вікно з відповідним повідомленням та інформацією щодо сертифіката.



Другий спосіб

Ви можете отримати ЕЦП через будь-який із центрів реєстрації. Для цього треба буде виконати 4 кроки:

- 1) зібрати документи;
- 2) зареєструватися в одному із Центрів сертифікації;
- 3) прийти в Центр із документами та чистим носієм інформації (флеш-пам'ять чи диск DVD-R);
- 4) за допомогою фахівців згенерувати ключі та записати їх на носій.

4. НАДІЙНИЙ ПАРОЛЬ

Головним помічником у боротьбі за кібербезпеку є складний для хакерів пароль. Ділимося з вами, як створити надійний пароль, де і як правильно його зберігати та яких заходів треба вживати для того, щоб він забезпечував стабільний захист від зловмисників.



Скільки разів на день вам доводиться вводити пароль та логін, щоб увійти до того чи іншого особистого кабінету

4. Надійний пароль

або сторінки? Та чи знаєте ви, наскільки надійним є ваш пароль?

Паролі забезпечують захист облікових записів користувачів, користувацьких даних та доступу до них.

ЩО ТАКЕ ПАРОЛЬ. ЯКИЙ ПАРОЛЬ Є НАДІЙНИМ

Пароль — це секретне умовлене слово, фраза (згідно з Тлумачним словником).

Ненадійні паролі — це звичайні слова або фрази, букви або цифри, що йдуть поспіль. Пароль є ненадійним, якщо він складається:

- з послідовності цифр: 12345, 337799, 10011001;
- з дати народження: 13051990, 19900513, 0513;
- з номера телефону: 0998765432, 0976543210;
- з поширених слів: password, qwerty, administrator;
- з вашого імені, імен родичів або домашніх тварин: anton, alex, sveto4ka, barsik, kasha;
- з географічної назви: ukraine, mississippi, pacificoccean;
- з юзернейма або його частини: username_example, antonio;
- з електронної пошти: example@ukr.net, pochta@gmail.com.

Такі паролі легко підібрати. Наприклад, хакерові знадобиться менше доби, щоб підібрати пароль «anton13051990». І всього 13 секунд для пароля «qwerty12345».

Існує сайт для перевірки надійності пароля: <https://howsecureismypassword.net/>

ENTER PASSWORD

 Entries are 100% secure and not stored in anyway or shared with anyone

Please Note: This tool is now being maintained over at Security.org

ЯКІ ПАРОЛІ Є НАДІЙНИМИ

Надійний пароль — це комбінації з великих і малих літер, цифр і спеціальних символів. Спробуйте пробігтися пальцями по клавіатурі й отримати такі паролі:

Qi@8zh0!kX74a

E5u73\$zOf&9azUa

YgC3£i4%rJqyB80

84aP@E&39uzxC1ka0

Щоб підібрати такі паролі, знадобиться кілька століть.

Характерні риси надійного пароля:

- містить великі та малі літери;
- містить цифри та символи;
- завдовжки понад 8 символів;
- не є словом у жодній з мов, діалектів, жаргонів, сленгу;
- не ґрунтується на персональній інформації.

А ще безпечний пароль не має зберігатися в паперовій або електронній формі без відповідного захисту носія.

ЯКІ ПАРОЛІ НЕ МОЖНА ВИКОРИСТОВУВАТИ

Для облікових записів користувачів компанії не можна використовувати:

- той самий пароль, що й для інших інформаційних систем (наприклад, домашній інтернет-провайдер, електронна пошта, форуми тощо);
- той самий пароль для різних корпоративних систем;
- однакові паролі в операційних системах Unix і Windows.

ЧОГО СЛІД УНИКАТИ В РОБОТІ З ПАРОЛЯМИ

- Повідомляти пароль іншим особам, зокрема адміністративному персоналу.
- Повідомляти принципи створення пароля (наприклад, на основі прізвища).
- Повідомляти пароль в електронних опитуваннях, незнайомих формах авторизації або де-небудь ще.
- Передавати пароль колегам на час вашої відсутності (відпустки або відрядження).

ЯК СЛІД ЗБЕРІГАТИ ПАРОЛІ

- Не записуйте паролі на папері.
- Не залишайте інформацію про паролі в будь-яких файлах або на носіях, доступ до яких є не тільки у вас.
- Не зберігайте паролі, які були встановлені вам адміністраторами за замовчуванням.
- Не зберігайте паролі в ПЗ, не призначеному для цього (в браузерях, утилітах підключення до інших сервісів тощо).

ЯК СТВОРИТИ НАДІЙНИЙ ПАРОЛЬ

- 1) Створюйте різні паролі для різних служб.

Якщо хакеру вдається зламати пароль в одному місці, він може спробувати це зробити в іншому. Необхідно мати різні «ключі» для різних «замків».

- 2) Змінюйте паролі регулярно.

Деякі програми мають налаштування, які нагадуватимуть вам про часту зміну паролів. Наприклад, якщо ви використовуєте Windows, ви можете вибрати опцію змінювати свій пароль для входу у Windows часто, використовуючи параметри пароля у вкладці Local Security Policy (місцева політика безпеки). Просто виберіть політику паролів у розділі «Політика облікового запису». Двічі клацніть вікно «Максимальний строк дії паролю» на панелі справа, уведіть кількість днів, після спливу яких потрібно поміняти паролі, та натисніть кнопку ОК. Тепер ви налаштували для себе нагадування.

- 3) Виберіть правильний пароль.

Паролі мають містити щонайменше 16 символів із комбінації цифр, символів, великих літер, маленьких літер. Вони не мають бути ані повторюваними, ані фактичним словом чи ідентифікатором вашої особи.

- 4) Виберіть двохетапну перевірку.

Gmail разом із Facebook пропонує цей бездоганний спосіб збереження вашої безпеки. Під час входу програма просто просить вас увести код, який було попередньо надіслано на ваш телефон.

5) Вимкніть автозаповнення для імен користувача та паролів.

Важливо відключити автозаповнення, коли ви виходите із системи, особливо знаходячись далеко від свого комп'ютера. Звичайно, дратує, коли вам постійно пропонують уводити цей складний пароль, якщо ви залишаєте свій комп'ютер протягом декількох хвилин, але це вкрай важливо, коли ви користуєтесь загальнодоступним комп'ютером.

Щоб вимкнути цю функцію в Google Chrome, натисніть кнопку меню Chrome. Унизу сторінки налаштувань натисніть кнопку «Показати розширені налаштування». Унизу знайдіть розділ «Паролі та форми». Зніміть прапорець поруч із параметром «Увімкнути автозаповнення».

Головна

Особисті дані

Дані й персоналізація

Безпека

Люди й доступ

Оплата й підписки

Про обліковий запис Google

Немає підозрілих дій і сповіщень системи безпеки за останній час (28 дн.)

Вхід в обліковий запис Google

Пароль	Остання зміна: 13 черв.	>
Двохетапна перевірка	Увімк.	>
Паролі додатків	Немає	>

Способи підтвердження вашої особи

Це допоможе підтвердити вашу особу під час входу або зв'язатися з вами, якщо ми виявимо підозрілу активність в обліковому записі

Конфіденційність Умови Довідка

Інформація

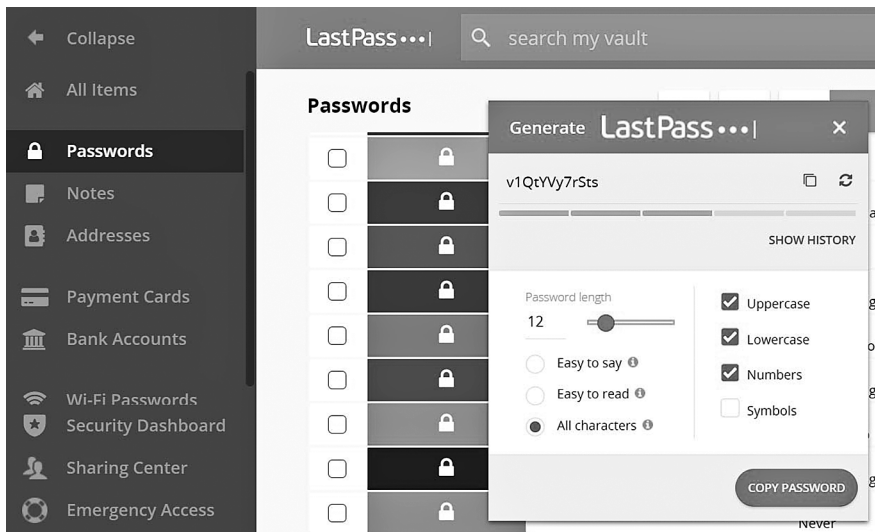
6) Користуйтеся підказками диспетчера паролів.

Є безліч диспетчерів паролів, які просто зберігають усі ваші коди й заповнюють логін. Це схоже на те, ніби ви маєте у своєму розпорядженні невелику карту пам'яті. Є спеціальні опції — це Password, LastPass (див. рисунок на с. 47), Roboform. Усе, що вам потрібно запам'ятати, — це майстер-пароль для входу в диспетчер паролів.

7) Не повідомляйте свій пароль електронною поштою та по телефону.

Це ніби й так зрозуміло, але ви ніколи не знаєте, коли вам може знадобитися невелике нагадування стосовно очевидного.

4. Надійний пароль



8) Використовуйте спеціальні сервіси для генерування паролів.

Таких сервісів у мережі інтернет багато, наприклад:

- <https://2ip.com.ua/> (зазначаєте, які символи ви хочете бачити в паролі й скільки символів має містити пароль, і отримуєте один варіант паролі);
- <http://www.parolemanager.com/> (тут можна не лише згенерувати пароль бажаної довжини й складності, а й перевірити його на зламостійкість за допомогою вбудованого аналізатора);
- <http://genpass.at.ua/> (сервіс не лише згенерує вам потрібну кількість паролів заданої складності, а й у рубриці «Як слово» запропонує паролі, які буде легко запам'ятати);
- <https://lastpass.com/uk/> (онлайн-сервіс, який об'єднує генератор паролів та сховище для зберігання в одному місці всіх ваших паролів, завдяки чому вам потрібно пам'ятати лише один, так званий «майстер-пароль», тобто пароль від самого сховища, а всі інші паролі можна в разі потреби подивитися на вашій персональній сторінці. Існує також спеціальне розширення для користувачів Chrome та програма для Android, завдяки

яким ваші логіни й паролі підставлятимуться у відповідні поля входу автоматично).

Якщо не зовсім довіряєте генераторам паролів, ніхто не заважає згенерований пароль ще ускладнити на власний розсуд, доповнивши його іншими символами, чи замінивши одні символи на інші.

Генератор паролів дозволяє вам створювати згенеровані у випадковий спосіб паролі високого рівня надійності, які складно підібрати через комбінацію в них великих та малих літер, а також використання чисел, розділових та інших знаків.

Увага! Генератор паролів ніде не зберігає паролі й не нагадує їх.

Щоб упорядкувати паролі, скористайтесь «Менеджером паролів».

Для створення паролів, будь ласка, налаштуйте необхідні вам опції та натисніть «Згенеруйте мені паролі!».

Порада: використання чисел, розділових та інших знаків додатково до літер дозволяє створювати більш надійні паролі, які вкрай складно підібрати наявними нині звичайними технічними засобами.

ГЕНЕРАТОР ПАРОЛІВ «2IP»

(<https://2ip.com.ua>)



Онлайн генератор паролів

Тут ви можете самі створити пароль будь-якої довжини та будь-якої складності

Бажана довжина пароля:

8

Згенерувати пароль:

6

☒ Використовувати цифри

☒ Використовувати малі літери

☒ Використовувати великі літери

☐ Використовувати спеціальні символи

ЗГЕНЕРУВАТИ

4. Надійний пароль

ГЕНЕРАТОР ПАРОЛІВ «PAROLE MANAGER»

(<http://www.parolemanager.com/ukrainian/password-generator.html>)

Password Manager (English) Менеджер Паролей (Русский) Менеджер паролів (Українська)

Інструмент

Довжина кожного паролю символів.

- ☒ Містить букви (наприклад: abcdef)
- ☒ Містить великі та малі літери (наприклад: AbcDEf)
- ☒ Містить числа (наприклад: a9b8c7d)
- ☐ Містить знаки пунктуації та інші знаки (наприклад: a!b*c_d)
- ☒ Не містить схожі знаки (наприклад: i, l, o, 1, 0, I)

Кількість паролів:

Ваш список паролів:

ЗБЕРІГАЧ ПАРОЛІВ

Зберігач паролів призначений для надійного збереження ваших паролів, а також для доступу до них із будь-якого місця в будь-який час.

Рекомендують для управління вашими обліковими записами користуватися «Менеджером паролів». Проте в деяких випадках, наприклад, коли паролі присвоюються автоматично, це неможливо. У такому випадку доводиться зберігати паролі. Цей сервіс збереже ваші паролі надійно та зробить доступ до них максимально зручним.

Зберігач паролів не вимагає реєстрації, не зберігає даних про вас. Уведена вами інформація про майстер-пароль (девіз) і адреса вашої електронної скриньки перетворюються за допомогою унікального алгоритму в спеціальний унікальний ключ. Уведені вами дані не можуть бути зворотно відновлені без знання вашого майстер-паролу, і тому ніхто не зможе їх розшифрувати.

Усі дані про ваші облікові записи (URL, ім'я користувача, пароль і т. д.) передаються й зберігаються на сервері в зашифрованому вигляді й не зможуть бути декодованими

навіть у випадку заволодіння ними. Процес шифрування та декодування відбувається на цій сторінці й у цьому вікні.

Сервіс не зберігає дані в куках або кешах, тому як тільки ви залишите сторінку, усі дані про вашу сесію будуть знищені й ніхто не зможе скористатися ними з комп'ютера, яким ви користувались.

Будь ласка, пам'ятайте, що сервісу невідомі дані про ваш майстер-пароль (девіз) і адреса вашої електронної скриньки. Якщо ви випадково забудете їх, сервіс не зуміє відновити та розшифрувати вашу інформацію.

Звертаємо вашу увагу і на те, що користуватися подібними програмами ми не рекомендуємо на незнайомих комп'ютерах. Зловмисники можуть перехопити дані, уведені вами безпосередньо з клавіатури.

Цей сервіс повністю безкоштовний.

Зберігач паролів «Parole Manager»

(<http://www.parolemanager.com/ukrainian/password-saver.html>)

Інструмент

* Ваш особистий майстер-пароль або девіз (наприклад: ps70, Не нароби зла):

* Ваш основний Email або Ім'я користувача (наприклад: test@gmail.com, bond):

Подивитись мої паролі!

* Всі поля обов'язкові для введення. Довжина кожного поля повинна мати більше семи символів. Інформація, яка вводиться в ці поля, необхідна для генерації унікального ключа, нікуди не передається і ніде не зберігається. Якщо ви вперше на цій сторінці, реєстрація проведеться автоматично.

АНАЛІЗАТОР ПАРОЛІВ

Аналізатор паролів призначений для перевірки якості пароля. Він проводить миттєву перевірку на вашому комп'ютері. Ваші дані нікуди не передаються та ніде не зберігаються.

Рекомендуємо перевірити ваш майстер-пароль перед використанням.

Для віддаленого підключення варто використовувати паролі якістю вище 30 одиниць, а при локальному підключенні — паролі якістю вище 40 одиниць.

5. Водяні знаки — захист авторських прав на світлини, рисунки, зображення

Аналізатор паролів

(<http://www.parolemanager.com/ukrainian/password-tester.html>)

Інструмент

Пароль (девіз):

Аналізувати

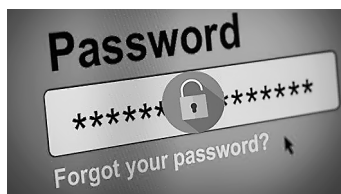
Якість пароля складає 0 одиниць.

Для підбирання пароля необхідно зробити максимум 1 операцій.

Пароль гарантовано підбирається за 0 дні(ів) при локальному підключенні.

Пароль гарантовано підбирається за 0 дні(ів) при віддаленому підключенні.

Онлайн інтернет-паролі схожі на ключі до вашого будинку. Що б не сталося, ви хочете переконатися в тому, що ваш світ надійно захищений.



5. ВОДЯНІ ЗНАКИ — ЗАХИСТ АВТОРСЬКИХ ПРАВ НА СВІТЛИНИ, РИСУНКИ, ЗОБРАЖЕННЯ

Водяний знак — це знак на зображенні (світлинах, рисунках, документах тощо), який вказує на авторство або власника цього зображення. Як правило, він має бути напівпрозорим і ледве помітним, тому він і називається водяним.



Водяні знаки пройшли шлях від перших італійських водяних знаків на купюрах та документах 1281 року до інтернету сьогодні. З появою перших авторських зображень люди прагнули зберегти своє ім'я — захистити авторське право.

Водяний знак (англ. watermark) використовують для того, щоб не допускати **копіювання** зображень сторонніми ресурсами, які не вказують на джерело.

Перевага водяних знаків у тому, що вони допомагають популяризувати власника контенту. Багато фотографів та

ілюстраторів протягом кількох років набули популярності саме завдяки водяним знакам.

Цифрове водяне маркування — це процес вбудовування інформації в медіа-файл, який використовують для перевірки авторства та його достовірності.

Водяний знак буває видимий або невидимий.

Видимий цифровий водяний знак — це позначки, видимі на фотографії. Зазвичай інформацією є текст або логотип, який ідентифікує власника фотографії. Ця інформація об'єднується в інформацію про зображення, але все ще видима.



Невидимий цифровий водяний знак — це позначки, які вбудовані в дані зображення фотографії, але розроблені таким чином, щоб вони були непомітні для зору людини, тому вони є прихованою інформацією.

ТИПИ ВОДЯНИХ ЗНАКІВ

- Текстовий — назва бренду чи спільноти, написана оригінальним шрифтом.
- Символьний символ, значок або невелика ілюстрація, що асоціюються з брендом або спільнотою.
- Комбінований — водяний знак, у якому є і текст, і символ.
- Емблема — комбінований водяний знак, уписаний у геометричну форму.

ПЛЮСИ ТА МІНУСИ ВОДЯНИХ ЗНАКІВ

Плюси:

- 1) **Захист від злодійства.** Один із методів боротьби з інтернет-зłodіями — водяні знаки. Якщо водяний знак розташований на зображенні так, що його складно або зовсім неможливо замаскувати, це запобігатиме копіюванню вашого контенту.

- 2) **Безкоштовне просування.** Яскравий приклад водяних знаків для особистого просування — фотографії Instagram-блогерів. На багатьох можна побачити значки або прості підписи з посиланням на обліковий запис. Велика кількість фотографів і моделей стали популярними завдяки такому безкоштовному піару.
- 3) **Брендинг компанії.** На рекламних зображеннях завжди можна побачити водяні знаки. Логотипи бренду розміщуються на будь-якому типі контенту, тому watermarks є необхідним елементом для компаній.

Мінуси:

- 1) **Псуєть загальний вигляд зображення.** Якщо це фотографія, основна мета якої — естетика, то вона буде помітно зіпсована водяним знаком. Водяні знаки мають бути максимально непомітними, хоча навіть крихітні символи на фото відштовхують людей.
- 2) **Тимчасові витрати.** Якщо ви випускаєте безліч зображень, доведеться витратити додатковий час на додавання водяних знаків. Можна спростити цей процес за допомогою онлайн-сервісів та плагінів, але вони займають деякий час.
- 3) **Легко стерти.** Водяний знак захистить від масового копіювання, але постійних порушників авторського права це не потурбує. Водяні знаки видаляються в редакторах без втрати якості зображення. Якщо невеликі знаки стоять у кутку, то фотографії просто обрізаються.
- 4) **Юридичного захисту немає.** Якщо вам доведеться захищати авторські права в суді, водяні знаки не допоможуть. Вони не несуть жодного реального фізичного захисту, якщо ваші зображення та логотипи не захищені авторським правом.
- 5) **Не популярні.** Серйозні видання не використовують чужий контент — вони знають законодавство. І останнім часом навіть невеликі сайти використовують посилання на джерело, тож необхідність прикріплювати водяні знаки вже суттєво відпала.

СПОСОБИ НАКЛАДАННЯ ВОДЯНИХ ЗНАКІВ

Створення водяних знаків — техніка накладання одного зображення на інше. Таким чином можна показати іншим, що це зображення належить саме вам. Нанесення водяного знака найчастіше застосовують фотографи, щоб позначити авторство фотографії. Також часто ватермарк використовують власники інтернет-магазинів для захисту від копіювання.

Також вам варто звернути увагу на **розмір водяного знака**. Він має бути досить великим, щоб покрити більшу частину деталей зображення. У такому разі водяний знак неможливо видалити непомітно, без будь-яких дефектів. Найкраще, якщо тавро закриває щонайменше тридцять відсотків фотографії.

НАНЕСЕННЯ ВОДЯНИХ ЗНАКІВ У ADOBE PHOTOSHOP

Спочатку потрібно зробити водяний знак. Берете ваш логотип або підпис і додаєте йому максимальну прозорість так, щоб логотип можна було побачити, не напружуючи очі. Далі відкриваєте зображення, додаєте другий шар та наносите на нього ваш напівпрозорий логотип. Виберіть оптимальний розмір водяного знака та його розташування.



НАНЕСЕННЯ ВОДЯНИХ ЗНАКІВ ЗА ДОПОМОГОЮ WATERMARK

WATERMARK (<https://watermark.ws/>) — онлайн сервіс для нанесення водяних знаків на зображення, фото.

Як це працює

- 1) **Імпорт файлів.** Імпортуйте фотографії або відео зі свого пристрою або з того місця, де вони існують у хмарі, у наш вебредактор.
- 2) **Водяний знак і редагування.** Використовуйте цей веб-редактор, щоб створити водяні знаки для своїх файлів і внести додаткові зміни, такі як обрізання та зміна розміру.
- 3) **Експорт файлів.** Завантажте файли з водяними знаками на свій пристрій або експортуйте їх безпосередньо в іншу програму.

5. Водяні знаки — захист авторських прав на світлини, рисунки, зображення



Можливості

- Створення власного водяного знака (створіть водяний знак із нуля, налаштувавши його власним текстом і стилем).
- Завантажте власні шрифти, авторські символи.
- Імпортуйте свій логотип (завантажте свій логотип або імпортуйте його зі свого Dropbox, Google Диска або з кількох інших місць).
- Підписні логотипи (використовуйте генератор фірмових логотипів, щоб створити фірмовий водяний знак; використайте своє ім'я та слоган).

НАНЕСЕННЯ ВОДЯНИХ ЗНАКІВ ЗА ДОПОМОГОЮ WATERMARK IMAGES

WATERMARK IMAGES (<https://www.watermark-images.com/>) — онлайн сервіс для нанесення знаків на

файли різних типів: Mp3 редактор тегів, ш, DOC в XLS, XLS в DOC, HTML в XLS, DWG в JPG, ODS в XLS, CR2 в JPG, редактор зображень DWG в PDF, XLS в PDF.

Алгоритм створення

- 1) Зайти за посиланням <https://www.watermark-images.com/>.
- 2) Вибрати зображення.
- 3) Установити властивості водяних знаків.
- 4) Вибрати зображення водяних знаків.
- 5) Зробити попередній перегляд.
- 6) Завантажити зображення з водяним знаком.

① Виберіть Зображення

Виберіть Зображення

② Встановити властивості водяного знака

Скинути налаштування

Текст водяного знака ^	Попередній перегляд (клацніть зображення, щоб збільшити) Очистити зображення
(c) Copyright	
Властивості шрифту v	
Розташування водяного знака v	
Спецефекти v	
Поле навколо тексту v	

③ Фотографії водяних знаків

Зображення водяних знаків

Завантажити зображення

НАНЕСЕННЯ ВОДЯНОГО ЗНАКА НА ФАЙЛ PDF

PlovePDF (<https://www.ilovepdf.com/>) — онлайн сервіс для вставлення водяного знака на PDF файл.

I♥PDF [ОБ'ЄДНАТИ PDF](#) [РОЗДІЛИТИ PDF](#) [СТИСНУТИ PDF](#) [КОНВЕРТУВАТИ PDF](#) [УСІ ІНСТРУМЕНТИ PDF](#) [Увійти](#) [Регістрація](#)

Вставте водяний знак у PDF

Виберіть зображення або текст, який потрібно вставити у PDF. Виберіть положення, прозорість та шрифт.

Вибрати PDF файл

або перетягніть PDF сюди

6. Пароль на флешку, папку, файл

Завантажте свій логотип або розмістіть текстовий водяний знак. Завантажте PDF файл та накладіть водяні знаки.



Збережіть документ.

6. ПАРОЛЬ НА ФЛЕШКУ, ПАПКУ, ФАЙЛ

ЯК ПОСТАВИТИ ПАРОЛЬ НА ФЛЕШКУ

Щоб встановити пароль на переносний накопичувач, можна використовувати одну з таких утиліт / програм:

- Rohos Mini Drive;
- BitLocker.
- USB Flash Security;
- TrueCrypt;

Розглянемо деякі з них.

СПОСІБ 1. Rohos Mini drive

Rohos Mini drive — це безкоштовна утиліта для шифрування даних на USB-накопичувачах, що створює прихований, захищений розділ на будь-якому USB-накопичувачі.



Rohos Disk Browser (Portable) — портативна версія. Вона запускається з USB drive на будь-якому ПК і дозволяє повноцінно працювати із захищеною частиною USB drive.

Якщо у вас багато важливих даних на USB-накопичувачі, ви можете уберегти їх від сторонніх очей за допомогою пароля та надійного шифрування. Саме Rohos Mini

допоможе вам створити на USB drive секретний розділ, захищений паролем та миттєвим шифруванням.

Налаштування та використання

Інтуїтивний майстер налаштування Rohos Mini автоматично визначає ваш USB-накопичувач і налаштовує параметри зашифрованого розділу (буде видно вам як віртуальний диск R:\). Потім потрібно лише вказати пароль. Шифрування відбувається автоматично. Натиснувши на іконку Rohos Mini (поруч із годинником), ви зможете відключити диск наприкінці роботи.

Захищений розділ буде доступний після введення правильного пароля

Якщо необхідно відкрити захищений розділ на чужому комп'ютері, потрібно лише клікнути на іконку Rohosmini.exe, що знаходиться в корені USB-накопичувача, і ввести пароль до диска. Rohos Mini відкриє віртуальний контейнер.

Основні характеристики захисту даних під час використання Rohos Mini

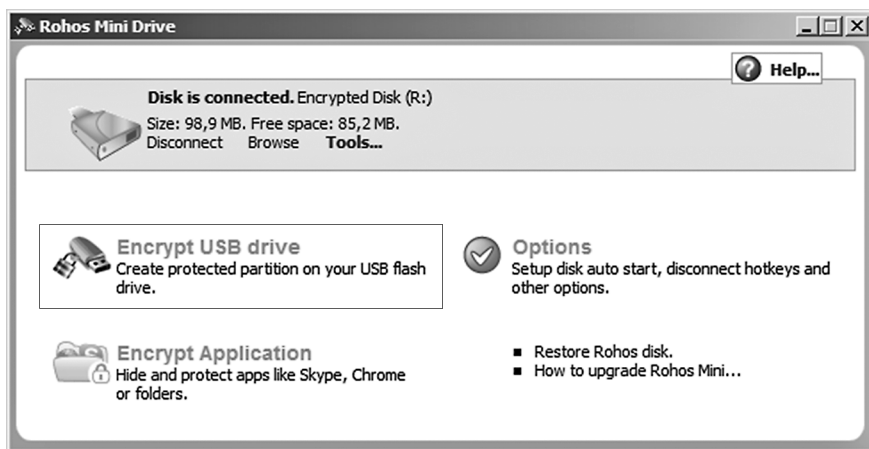
- Створюється віртуальний зашифрований розділ (диск) за допомогою вільного об'єму USB-накопичувача.
- Автоматично визначається конфігурація вашого USB-накопичувача та створюється зашифрований розділ, захищений паролем.
- Шифрування відбувається автоматично.
- Віртуальна клавіатура захищає пароль доступу до USB-накопичувача від клавіатурного шпигуна.
- Папка Autorun. Збережені ярлики програм/файлів будуть автоматично запущені після підключення диска.
- 8 Гб — лімітований розмір зашифрованого розділу в безкоштовній версії.
- Rohos Disk Browser допомагає працювати із зашифрованим розділом на комп'ютері без адміністративних прав, а також не залишає слідів секретних даних на ПК. Ви можете запустити програму безпосередньо з USB-накопичувача. Rohos Disk Browser відкриває файл у відповідній програмі без попереднього розшифрування та розміщення в тимчасовій папці.

6. Пароль на флешку, папку, файл

Програма створює віртуальний розділ на USB-накопичувачі. Таким чином, коли ви підключаєте USB-накопичувач, у вікні Windows спочатку з'явиться лише буква цього накопичувача. Інша літера (для захищеного розділу) з'явиться в системі після підключення зашифрованого диска.

Алгоритм використання програми

- 1) Запустіть програму та натисніть «Зашифрувати USB диск».



- 2) Програма автоматично визначить флешку. Натисніть «Параметри диска». Тут можна задати букву захищеного диска, його розмір і файлову систему (краще вибирати ту ж, що вже є на флешці). Щоб підтвердити всі виконані дії, натисніть «ОК».
- 3) Уведіть пароль та підтвердіть його. Потім запусить процес створення диска, тому потрібно натискати відповідні кнопки.
- 4) Тепер частина пам'яті на вашій флешці буде захищена паролем. Щоб отримати доступ до цього сектора, запусить в корені флешки Rohosmini.exe



(якщо програма встановлена на даному ПК) або RohosMiniDrive(Portable).exe (якщо на даному ПК цієї програми немає).

- 5) Після запуску однієї з вищевказаних програм уведіть пароль і натисніть «ОК».
- 6) Прихований диск з'явиться в переліку жорстких дисків. Туди ж можна перекинути всі найцінніші дані. Щоб його знову заховати, знайдіть значок програми, клікніть по ньому правою кнопкою і натисніть «Вимкнути R» («R» — ваш прихований диск).
- 7) Рекомендуємо відразу створити файл для скидання пароля на випадок, якщо Ви його забудете. Для цього включіть диск (якщо вимкнено) і натисніть «Створити резервну копію».
- 8) Серед усіх варіантів виберіть пункт «Файл для скидання пароля».
- 9) Уведіть пароль, натисніть «Створити файл» і виберіть шлях збереження. У даному випадку все просто: з'являється стандартне для Windows вікно, у якому можна вручну вказати, де буде зберігатися даний файл.

Разом із Rohos Mini Drive можна поставити пароль на папку та на деякі програми. Процедура буде точно така ж, як описано вище, але всі дії виконуються з окремою текою або ярликом.

СПОСІБ 2. BitLocker

Шифрування диска BitLocker — це функція захисту даних, яка інтегрується в операційну систему та запобігає загрозі розкрадання даних або розкриття інформації на втрачених, украдених або неправильно виведених з експлуатації комп'ютерах.



Використовуючи стандартний BitLocker, можна обійтися без програм від сторонніх виробників. Даний інструмент є в Windows Vista, Windows 7 (причому у версіях Ultimate і Enterprise), Windows Server 2008 R2, Windows 8, 8.1 і Windows 10.

6. Пароль на флешку, папку, файл

Алгоритм використання

- 1) Натиснути правою кнопкою на значок флешки й вибрати у випадаючому меню пункт «Включити BitLocker».



- 2) У розділі «Оберіть способи зняття блокування диску» поставити галочку біля «Використовувати пароль для зняття блокування диску». Увести пароль двічі. Натиснути «Далі».
- 3) Зберегти у файлі на комп'ютері або роздрукувати ключ відновлення. Він знадобиться, якщо ви вирішите змінити пароль. Визначившись із вибором (поставте позначку біля потрібного пункту), натиснути «Далі».
- 4) Натиснути «Почати шифрування» і дочекатися закінчення процесу.
- 5) Пароль на диск створено. Тепер, коли ви будете вставляти флешку, з'явиться вікно з полем для введення пароля.

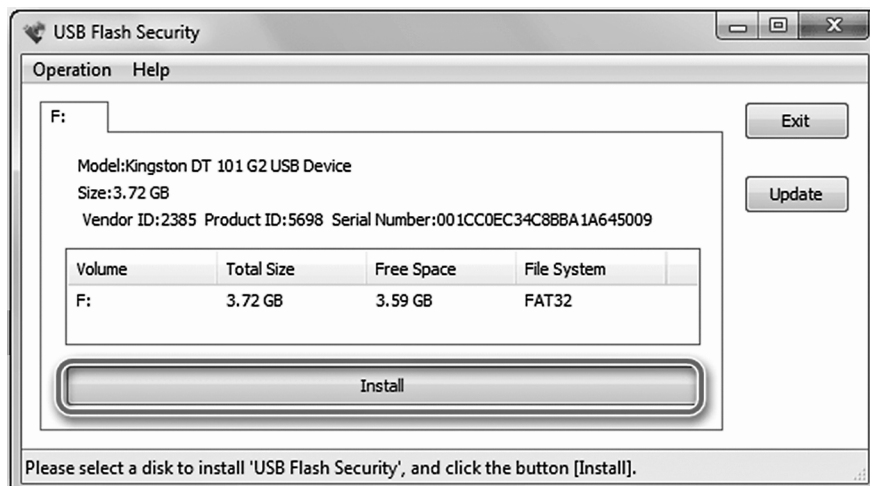
СПОСІБ 3. USB Flash Security

Ця утиліта в кілька кліків дозволить захистити паролем усі файли на флешці. Щоб завантажити безкоштовну версію, на офіційному сайті необхідно натиснути кнопку «Download Free edition».



Алгоритм використання

- 1) Запустивши програму, ви побачите, що вона вже визначила носій та вивела інформацію про нього. Натисніть «Install».



- 2) З'явиться попередження, що під час процедури зникнуть усі дані на флешці. Тому попередньо скопіюйте все найпотрібніше й натисніть «ОК».
- 3) У відповідні поля введіть і підтвердьте пароль. У поле «Hint» можна вказати підказку на випадок, якщо ви його забудете. Натисніть «ОК».



6. Пароль на флешку, папку, файл

- 4) Знову з'явиться попередження. Поставте галочку й натисніть кнопку «Begin the installation». Тепер ваша флешка буде відображатися так, як показано на фото праворуч. Якраз такий її зовнішній вигляд і свідчить про те, що на ній є якийсь пароль. Усередині вона буде містити файл `UsbEnter.exe`, який вам потрібно буде запустити.
- 5) У вікні введіть пароль і натисніть «OK».



СПОСІБ 4. TrueCrypt

TrueCrypt — програма дуже функціональна, можливо, у ній найбільша кількість функцій серед усіх представлених у нашому огляді зразків ПО. При бажанні ви можете запаролити не тільки флешку, а й жорсткий диск. Але перед виконанням будь-яких дій завантажте її на свій комп'ютер.

Використання цієї програми є важкою для новачків, але надійною.

За допомогою TrueCrypt можна створювати віртуальні зашифровані логічні диски та повністю шифрувати розділ жорсткого диска або іншого носія інформації, наприклад флопі-диска або флеш-пам'яті USB.

Усі збережені за допомогою TrueCrypt дані повністю шифруються, включаючи імена файлів і каталогів — їх неможливо прочитати (розшифрувати) без використання правильних паролів / ключових файлів або без правильних ключів шифрування.

Завдяки цьому організації та приватні особи можуть тримати всі свої важливі файли та паролі в безпеці. Так, за допомогою TrueCrypt НКО може уникнути контролю з боку держави, засекретивши свої файли, або використовувати інструмент для зберігання особистих даних про співробітників.

Змонтований том TrueCrypt подібний до звичайного логічного диска, тому працювати з ним можна як зі звичайним логічним диском.

TrueCrypt існує у версіях для Windows 7/Vista/XP, Mac OS X та Linux.

Можливості TrueCrypt

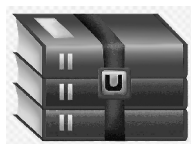
- Створення зашифрованого віртуального диска.
- Забезпечення двох рівнів правдоподібного заперечення наявності зашифрованих даних, необхідного у разі вимушеного відкриття пароля користувачем.
- Перенесення, що дозволяє запускати TrueCrypt без встановлення в операційній системі.
- Підтримка створення динамічного зашифрованого файлу на дисках NTFS.
- Шифрування системного фізичного чи логічного диска для Microsoft Windows-систем із дозагрузочною аутентифікацією.
- Зміна паролів та ключових файлів без втрати зашифрованих даних.
- Можливість використовувати TrueCrypt на комп'ютері з правами звичайного користувача.

Повну версію інструкції англійською мовою можна знайти на офіційному сайті TrueCrypt у розділі з документацією.

ЯК ПОСТАВИТИ ПАРОЛЬ НА ПАПКУ

Архівація

Цей спосіб підійде, якщо потрібно передати запаролену папку: надіслати поштою, скинути на флешку, опублікувати в інтернеті. Якщо ви збираєтеся зберігати її на комп'ютері, краще використовувати



файл-архів

6. Пароль на флешку, папку, файл

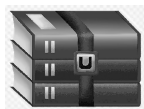
спеціальну програму. Зашифрувати дані — це складніше, але надійніше.

Архівація — це процедура пакування даних, у результаті якої створюється файл-архів. На цей файл можна встановити пароль, і поки користувач його не введе, отримати доступ до даних він не зможе.

Алгоритм створення пароля

- 1) Архівуємо папку під паролем.
- 2) Видаляємо оригінал (початкову папку).
- 3) У разі, якщо треба щось відредагувати, розпаковуємо архів і видаляємо його.
- 4) Після правок знову архівуємо папку й видаляємо оригінал.

Для створення таких архівів можна використовувати WinRAR або 7-Zip.



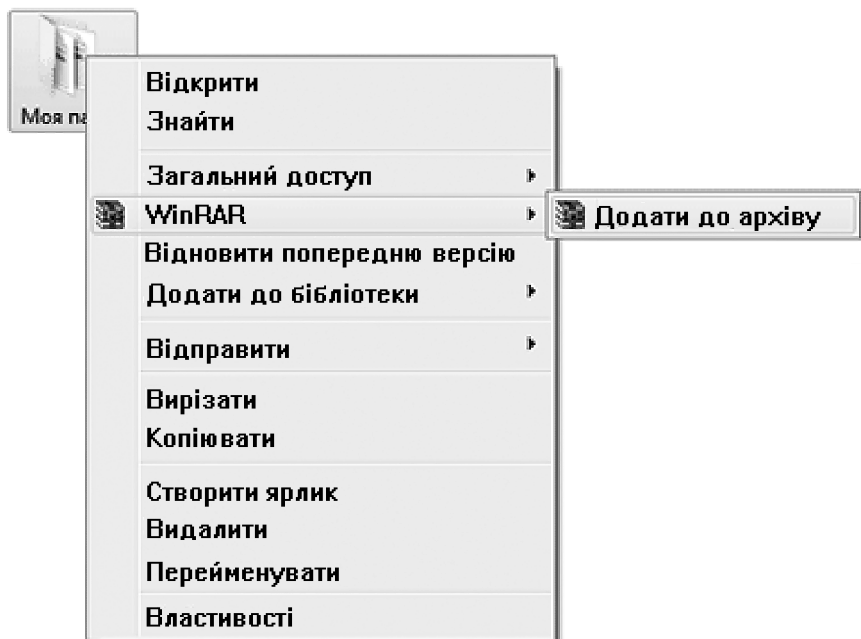
WinRAR



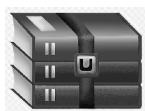
7-Zip

Алгоритм виконання

- 1) Клацніть правою кнопкою миші за каталогом, на який потрібно поставити пароль. У контекстному меню, якщо ви у WinRAR, виберіть «Додати в архів...» (Add to archive...). А якщо в 7-Zip → «Додати до архіву...». Якщо ви у WinRAR, то відкриється невелике віконце, де потрібно натиснути кнопку «Встановити пароль...» (може перебувати у вкладці «Додатково»). Після цього з'явиться ще одне вікно, куди і вводимо код. У 7-Zip вказуємо його відразу внизу віконця (праворуч).
- 2) Пароль повинен бути надійним: щонайменше 10 знаків, включаючи цифри, а також маленькі та великі англійські літери. Коли код призначений і про всяк випадок записаний у надійне місце, натисніть на кнопку «ОК» і чекайте, поки папка заархівується. Якщо файлів у ній небагато і вони невеликого розміру, це станеться досить швидко.



3) У результаті з'явиться новий файл-архів.



Моя папка або **Моя папка**

Це і є запаролений каталог. Таким чином у нас залишається і оригінал, і його копія, але в архіві під кодом.



Моя папка

Моя папка

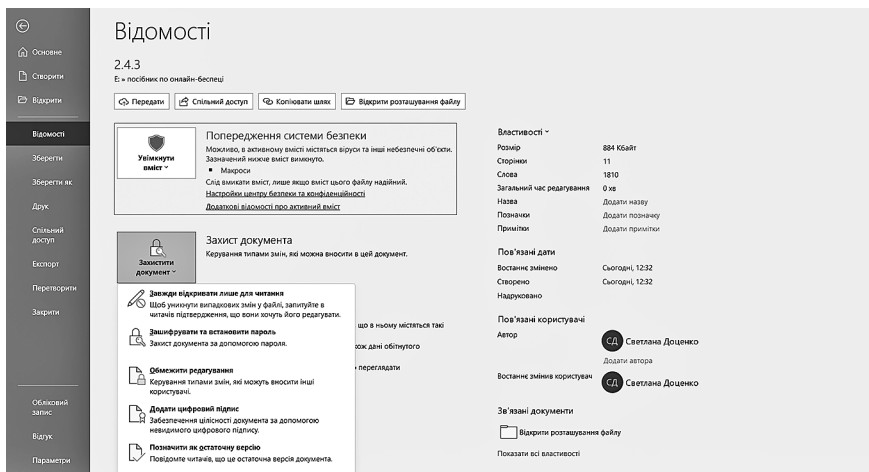
ЯК ПОСТАВИТИ ПАРОЛЬ НА ДОКУМЕНТ MICROSOFT WORD АБО EXCEL

Пароль на документ Word 2019 (Office 365)

- 1) Відкрити документ Word, на який потрібно встановити пароль, натиснути «Файл».

6. Пароль на флешку, папку, файл

- 2) У меню ліворуч вибрати пункт «Відомості». Обрати команду «Захистити документ» → «Зашифрувати та встановити пароль».



- 3) Вигадати та ввести пароль у відповідне поле вікна «Шифрування документа». Підтвердити пароль.

Пароль створено. Тепер, щоб відкрити зашифрований документ, необхідно правильно ввести заданий вами пароль.

Зверніть увагу: якщо ви забули пароль, відновити його буде неможливо. Отже, ви втратите і доступ до документа. Рекомендується зберігати свої паролі в надійному місці, наприклад, у спеціальній програмі (менеджери паролів: RoboForm, Bitwarden, KeePass, Sticky Password та ін.).

Захист паролем документів Excel 2019 (Office 365)

За аналогією можна зашифрувати будь-який документ Excel, Access або PowerPoint у Microsoft Office 2019 (Office 365).

Інші версії Office

- 2003: «Сервіс» → «Параметри» → «Безпека» → «Пароль для відкриття файлу».
- 2007: «Меню» → «Підготувати» → «Зашифрувати документ».
- 2010/2013/2016: «Файл» → «Відомості» → «Захист документа» → «Зашифрувати з використанням пароля».

Як зняти пароль із зашифрованого документа Microsoft Word

- 1) Увести пароль → відкрити документ.
- 2) Обрати «Файл» → «Відомості» → «Захистити документ» → «Зашифрувати з використанням пароля».
- 3) Стерти старий пароль, залишаючи поле порожнім → Натиснути «ОК».

Пароль вилучено. Тепер, щоб відкрити документ Word, Excel, Access, PowerPoint у Microsoft Office, пароль не потрібний.

ЯК ПОСТАВИТИ ПАРОЛЬ НА ФАЙЛ PDF

pdf2go (<https://www.pdf2go.com/>) — онлайн сервіс для створення пароля на файл PDF.



Як захистити PDF-файл паролем

- 1) Завантажити PDF-файл.
- 2) Увести та повторити відкритий пароль.
- 3) Налаштувати права доступу.
- 4) Увести та повторити пароль обмежень.
- 5) Натиснути «Почати».

Налаштування

Установіть пароль для відкриття документа та введіть його двічі. Цей пароль можна використовувати для обмеження доступу до файла. Його не можна використовувати для обмеження функціональності PDF-файла. Якщо ви встановите обмеження на використання та вкажете лише пароль обмежень, деякі програми зможуть його обійти. Виберіть відкритий пароль, щоб зашифрувати та захистити PDF-файл.

Права доступу:

- Заборонити друк
- Заборонити копіювання
- Заборонити зміни

Додаткові налаштування: растрування. Для додаткового захисту можна обмежити доступ до редагування або перегляду прихованих частин файлу. Ця функція дозволяє об'єднати весь вміст в один шар без пошуку.

7. БАТЬКІВСЬКИЙ КОНТРОЛЬ

Батьківський контроль — це набір інструментів, що допомагає батькам контролювати процес використання інтернету їхніми дітьми: фільтрація вебсайтів та їх вмісту, керування екранним часом тощо.



За даними американських науковців (2019), 52 % батьків використовують батьківський контроль для обмеження доступу дітей до певних сайтів. І для цього є вагома причина: якщо батьківський контроль стає частиною процесу виховання дітей, то він може допомогти розвинути здорові онлайн-звички в дитини, а також захистити домашню мережу та пристрої.

Батьківський контроль дає можливість не тільки обмежувати екранний час і зміст сайтів, але й допомагає запобігти кіберзлочинності та крадіжці даних, захищаючи вашу дитину від можливої ризикованої поведінки в інтернеті.

Тому потрібно розглянути можливість спільного використання програмного забезпечення для батьківського контролю та системи захисту від кіберзлочинності з метою захисту всіх членів вашої родини під час використання інтернету.

Утім посилений захист удома не може повністю захистити від небезпек: у якийсь момент ваша дитина може вийти в інтернет з іншого пристрою або в іншій мережі, наприклад з одним зі своїх друзів, у яких не встановлена функція батьківського контролю. Тут має приходити на допомогу виховання.

Те, що ваша дитина може отримати доступ до інтернету, не означає, що їй потрібен доступ до всіх ресурсів інтернету. Важливо вивчити такі, що відповідають її віку, додатки та сайти, щоб зрозуміти, коли ваша дитина може їх використовувати.

Сайти соціальних мереж мають вікові обмеження. Facebook, Instagram, Tik Tok і YouTube вимагають, щоб користувачам було не менше 13 років. Проте це лише рекомендації: ви, як батьки, повинні визначити, чи готова ваша 13-річна дитина отримати доступ до тих чи інших додатків і сайтів.

Якщо ви вирішили, що ваша дитина готова до налаштування облікових записів і додатків або до самостійного використання телефону чи пристрою, є кілька способів забезпечити її безпеку в інтернеті.

Безпеку в інтернеті батьки можуть забезпечити за допомогою безкоштовних інструментів або мобільних додатків на пристроях своєї дитини:

- **батьківський контроль на iPhone:** обмеження інформації певного змісту, програм та встановлення обмеження екранного часу. Якщо у вашої дитини є власний iPhone, додайте її пристрій у свою «сім'ю» за допомогою налаштувань екранного часу телефону. У ньому, навіть якщо ви використовуєте пристрій спільно, ви можете встановити різні параметри керування;
- **Google Family Link (для пристроїв Android):** вибір елементів керування й обмеження екранного часу віддалено з вашого пристрою. Для початку роботи потрібно знайти Google Family Link в Google Play;
- **безпечний режим YouTube:** блокування вмісту для дорослих. На будь-якій сторінці YouTube знайдіть нижній колонтитул, у якому наведені налаштування. Натисніть кнопку «Обмежений режим», щоб увімкнути або вимкнути цю функцію;
- **безпечний пошук у Google:** фільтрація відвертого сексуального вмісту за результатами пошуку Google. Перевірте та задайте налаштування пошуку або ввімкніть

і всіх користувачів молодше 13 років за допомогою програми Google Family Link;

- параметри конфіденційності для соціальних мереж: обмежить активність і можливість надання інформації друзям та контролюйте, хто підписується на отримання новин. Перевірте налаштування облікового запису соціальної мережі своєї дитини, щоб обмежити можливість її пошуку.

БАТЬКІВСЬКИЙ КОНТРОЛЬ У WINDOWS 10

За допомогою цього програмного компонента дитина може використовувати комп'ютер та інтернет більш безпечно. Батьківський контроль відкриває батькам доступ до таких функцій:

- моніторинг дій, які виконувала дитина;
- можливість завантажувати та встановлювати ігри залежно від вікового цензу;
- контроль за використанням браузерів, збереження історії відвідувань вебсайтів;
- установлення обмежування часу використання пристрою дитиною.

Після оновлення Windows 10 з'явилися додаткові можливості цього програмного компонента. За їх допомогою ви зможете контролювати покупку додатків та ігор в онлайн-магазині Windows відповідно за п'ятьма віковими категоріями:

- для будь-якого віку;
- від 6-ти років;
- від 12-ти років;
- від 18-ти років.

Для налаштування батьківського контролю (Windows 10) необхідно створити обліковий запис дитини. Для цього потрібно відкрити в «Параметрах» розділ «Облікові записи», де на вкладці «Сім'я та інші користувачі» натиснути на посилання «Додати члена сім'ї».

У діалоговому вікні обрати опцію «Додати обліковий запис дитини» та ввести поточний обліковий запис вашої дитини.

Якщо в дитини немає облікового запису на Microsoft, то в системі є можливість її створити. Для створення облікового запису потрібен буде надійний пароль.

Зверніть увагу! Якщо вік дитини менше восьми років, система відразу встановить налаштування з підвищеними заходами безпеки для цього облікового запису. Для старших восьми років усі налаштування доведеться робити батькам самостійно. Після створення та введення акаунта дитини до переліку облікових записів він буде автоматично доданий до членів сім'ї з правом входу в систему.

Тепер на вашому комп'ютері з'явиться новий обліковий запис, під яким дитина може увійти в систему, однак, якщо ви — один із батьків і налаштовуєте батьківський контроль Windows 10, рекомендуємо перший вхід виконати самостійно («Пуск» — клік по імені користувача), через те що можуть знадобитися додаткові налаштування нового користувача (та й при першому вході з'являється повідомлення про те, що «Дорослі члени сім'ї можуть переглядати звіти про ваші дії»).

Радимо налаштувати права молодого члена сім'ї тільки як стандартного користувача, тому що з правами адміністратора дитина зможе прибрати всі ваші налаштування.

НАЛАШТУВАННЯ ПАРАМЕТРІВ БАТЬКІВСЬКОГО КОНТРОЛЮ

Після того як ви створили обліковий запис дитини та додали її до користувачів пристрою, потрібно налаштувати функцію «Батьківський контроль». Дорослому члену сім'ї необхідно скористатися лінком «Управління сімейними налаштуваннями через інтернет». Це посилання автоматично відкриється у вашому браузері за замовчуванням. На сторінці оберіть обліковий запис дитини для налаштування функції моніторингу та контролю за її діями в інтернеті. Ви зможете контролювати дії дитини, бачити, у які ігри вона грає та навіть як довго вона перебуває на ігровому ресурсі, де і коли робила покупки, а то й зовсім заборонити їй здійснювати такі дії, заблокувавши можливість оплати за допомогою кредитної картки. Розглянемо кожен пункт детальніше.

Недавні дії. У цьому розділі можна відстежувати дії своєї дитини в інтернеті, знати, на які сайти вона заходила, що переглядала, а також загальний час перебування її за комп'ютером.

Для цього обов'язково має бути включена опція «Звіти про дії включені», інакше ваша дитина зможе заходити в мережу інкогніто. А все тому, що буде можливість включити режим InPrivate, який дозволить дитині анонімно переглядати сайти або грати на ігрових ресурсах. Ви цього не будете бачити, адже сайти не зберігатимуть жодної інформації про відкриті сторінки. Діти до восьми років автоматично не можуть включити цей режим.

Перегляд вебсторінок. Цей розділ є одним із головних через те, що саме в ньому ви можете дозволити використовувати або помістити в список заблокованих той чи інший сайт. Усе досить просто та зрозуміло: варто включити повзунок на опції «Блокування небажаних вебсайтів», і всі сайти для дорослих, а також сайти зі сценами насильства й жорстокості будуть автоматично заблоковані.

Важливо знати, що всі ваші налаштування щодо обмеження працюють виключно для стандартних браузерів Microsoft. Отже, вам доведеться додатково попрацювати над блокуванням можливостей сторонніх браузерів для облікового запису дитини. Для цього потрібно поставити позначку в опції «Перегляд лише вебсайтів зі списку дозволених». У разі якщо ваша дитина захоче подивитися певний фільм або мультфільм, то в списку буде тільки той сайт, який дозволений їй для перегляду. Цим самим ви врятуєте свій пристрій від завантаження небажаних вірусів і троянів. Дуже часто під виглядом сайтів із дитячими фільмами, мультфільмами або іграми можуть бути ресурси, які поширюють небажане програмне забезпечення, зокрема віруси.

Отже, ви маєте можливість окремим списком заборонити певні сайти або соціальні мережі.

Додатки, ігри та мультимедіа. Розділ «Додатки, ігри та мультимедіа» допоможе батькам контролювати, у які ігри грає їхня дитина, здійснювати моніторинг фільмів, серіалів і мультфільмів, які їй дозволені.

Також батьки зможуть визначати віковий ценз додатків та ігор, які будуть завантажені з «Магазину». Для цього достатньо вибрати вік дитини, а система самостійно встановить вікові обмеження.

Таймер роботи з пристроєм. У більшості батьків виникає проблема з обмеженням часу, який дитина проводить за комп'ютером. Існує безліч програм, які встановлюють своєрідний таймер роботи за пристроєм.

У Windows 10 є така можливість. У розділі «Таймер роботи з пристроєм» можна обмежити час перебування вашої дитини за комп'ютером або ігровою приставкою, наприклад Xbox.

Для цього треба встановити ліміт часу: за допомогою повзунка потрібно активувати опцію «Set limits for when my child can use devices» (Установити ліміт, коли моя дитина може використовувати пристрій).

Можна визначити ліміт часу по днях: на кожен день тижня встановлюється певна кількість годин, протягом яких дитина може користуватися комп'ютером у зручний для неї час, але, наприклад, не раніше й не пізніше встановленого часу.

Є можливість попросити в батьків додатковий час роботи з комп'ютером, якщо дитина не встигла дограти, а від цього залежать бонуси. Як тільки вона побачить на екрані повідомлення про те, що час минув, у цьому ж повідомленні вона зможе скористатися кнопкою «Отримати додатковий час».

На пошту батьків надходить лист із проханням про продовження часу перебування за комп'ютером. Батьки самі вирішують, скільки часу ще можна додати дитині для гри, обравши одне з посилань. Система автоматично встановить час, а дитина зможе дограти або поспілкуватися в чаті з друзями.

Покупки та витрати. У наш час уже нікого не здивуєш тим, що в інтернет-магазині можна купити практично все. Навряд чи знайдеться людина, яка б хоч раз нічого не купувала в інтернеті. Навіть на ігрових ресурсах можна купити різні доповнення до гри, які можуть допомогти пройти

певний рівень або й виграти бій. Для цього потрібні грошові ресурси з кредитних карток, які слід захистити від шахраїв.

У розділі «Покупки та витрати» батьки зможуть контролювати, що купує їхня дитина. Також можна встановити, які програми та ігри вона може завантажувати з «Магазину», щоб зберегти або контролювати свої кошти.

Пошук дитини. Цей розділ використовується для пошуку місця перебування дитини при використанні переносних пристроїв на Windows 10 з функціями визначення місцезнаходження (смартфон, планшет, деякі моделі ноутбуків). Ви зможете побачити місцезнаходження вашої дитини, а також визначати, де в цей момент перебуває її смартфон або планшет, навіть якщо пристрій було вкрадено. У пристрої дитини має бути постійно включена функція визначення місця перебування, інакше налаштування не зможуть працювати.

Видалення облікового запису дитини. Якщо батьки вирішили видалити обліковий запис дитини з комп'ютера, ноутбука або планшета, необхідно зайти на вебсайт програми «Безпека» за посиланням в розділі «Облікові записи» — «Сім'я і інші люди», або через «Параметри сім'ї» «Захисника» Windows. Знайти потрібний обліковий запис дитини та вибрати посилання «Додаткові параметри».

БАТЬКІВСЬКИЙ КОНТРОЛЬ НА YOUTUBE

YouTube — один із найбільш відвідуваних сайтів в інтернеті. Це відеохостинг, на якому діти можуть знайти цікаві й розвиваючі відео, мультфільми, корисні матеріали для навчання та багато іншого. Однак YouTube містить матеріали з позначкою «18+», не призначені для перегляду неповнолітніми. Діти не звертають увагу на попередження. Тому потрібен батьківський контроль на YouTube.



Для цього треба зайти в налаштування облікового запису, унизу сторінки знайти розділ «Безпечний режим» і поставити там позначку.

Значна кількість користувачів YouTube переглядають контент не тільки на ПК або ноутбуках, а й на мобільних

пристроях. Тому функцію батьківського контролю потрібно налаштувати на кожному з використовуваних пристроїв.

Для цього потрібно авторизуватися в додатку YouTube:

- 1) натиснути на іконку профіля вгорі екрану, щоб увійти до облікового запису;
- 2) у меню обрати розділ «Налаштування»;
- 3) натиснути на опцію «Фільтрація пошуку»;
- 4) у вікні меню обрати опцію «Суворе». YouTube пропонує лише два варіанти — «Суворі фільтрації» та «Не фільтрувати»;
- 5) натиснути кнопку «Повернення» (у вигляді стрілки) для підтвердження налаштувань.

8. **МОБІЛЬНІ ДОДАТКИ БАТЬКІВСЬКОГО КОНТРОЛЮ**

За допомогою спеціальних мобільних додатків батьки можуть «віртуально наглядати» за своїми дітьми.

- 1) *Обмеження часу користування гаджетом.* Припустимо, дитина повернулася зі школи о 14:00, і щоб нічого не відволікало її від виконання домашнього завдання, установить обмеження на вихід в інтернет, наприклад до восьмої вечора.
- 2) *Обмеження використання додатків.* Батьки можуть заборонити дитині грати в ігри, які містять сцени насильства або еротичні елементи; обмежити встановлення програм, що пропонують електронні покупки, розіграші та інші грошові операції.
- 3) *Вебфільтрація.* Ця функція на різних пристроях та додатках реалізується декількома способами. Найчастіше програма має доступ до бази даних, де містяться небажані для дітей ресурси, і автоматично їх блокує. Особливість полягає в тому, що не всі браузері підтримують цю функцію.
- 4) *Відстеження місцезнаходження.* Додатки дають змогу дізнатися не лише про те, де перебуває дитина в цей момент, а й подивитися історію переміщень за місяць. У деяких випадках програма сповістить батьків про те,

що дитина вийшла за межі дозволеної локації або дісталася небажаних районів (ринки, вокзали, занедбані території тощо).

- 5) *Контроль спілкування*. Тут функціонал додатків відрізняється. Одні дають батькам змогу побачити лише перелік дзвінків, другі — читати смс-повідомлення й слухати телефонні дзвінки, треті оповістять, що відбувається в листуваннях у соціальних мережах.
- 6) *SOS*. Такий сигнал вбудований у саму операційну систему. Якщо його немає, допоможуть спеціальні додатки з такою функцією. Дитина може дати сигнал, що сталася біда, і батьки дізнаються, де вона перебуває.

СІМЕЙНИЙ GPS ТРЕКЕР KIDCONTROL

KidControl (Контроль за дитиною) — безкоштовна програма для Android телефону та комп'ютера, яка дає вам змогу спостерігати, відслідковувати на мапі вашого міста вашу дитину в реальному часі та отримувати інформацію про заряд батареї її телефону.



KidControl

Основні функції програми KidControl:

- відстеження поточного перебування дитини та зберігання історії переміщень за два минулі дні: сьогодні й учора;
- кнопка SOS, щоб послати за потреби сигнал тривоги своїм батькам або рідним;
- створення до 2 місць вхідних/вихідних повідомлень, які надходять на телефон вашої дитини;
- визначення місцезнаходження навіть із вимкненим GPS (отримання геоданих);
- отримання автоматичних повідомлень, коли телефон дитини розряджається (наприклад, 15 % заряду) або в разі повного розрядження;
- побудова маршруту до дитини по мапі;
- пошук загубленого або вкраденого телефону;
- відстеження не тільки однієї дитини, а й інших родичів;

- перегляд на графіку рівня заряду акумулятора телефону, який характеризує частоту його використання. За даними розробників програми, додаток дуже економічний і впливає на денну витрату заряду акумулятора телефону в межах 1–7 %;
- налаштування «Небезпечної зони» для отримання попереджень, якщо в таких зонах виявляються ваші діти;
- у Преміум-версії можливість включення архіву «Бортовий самописець» — запис маршруту, коли немає інтернету.

Інструкція зі встановлення програми.

Програма повністю безкоштовна та поширюється через магазин Google Play. Для встановлення програми після переходу за посиланням натисніть «Встановити».

- 1) Після скачування встановіть програму в режимі «батьки».
- 2) При першому вході створіть свій логін і зареєструйте акаунт. Для встановлення іншим користувачам у режимі «батьки» або «дитина» також проведіть аналогічне встановлення, але при першому вході вкажіть дані облікового запису, уведені першого разу.
- 3) Програма в режимі «дитина» може встановлюватися тільки на телефон під управлінням ОС Android. Однак у режимі «батьки» можна користуватися програмою з телефонів під управлінням інших операційних систем: iPhone, iPad або Windows. Для цього в браузері зайдіть у ваш «Особистий кабінет» на сайті www.go.kid-control.com під вашим логіном і паролем.
- 4) Після встановлення програми її буде видно в списку встановлених програм. Дитині пояснити, що для того, щоб програма працювала, не потрібно відключати Wi-Fi або GPS на своєму телефоні.

Робота програми.

Програма дуже проста та інтуїтивно зрозуміла. При вході в програму ви відразу ж бачите карту вашого міста. Ліворуч унизу — список людей у вашому обліковому записі. Для визначення місцезнаходження людини на карті досить

натиснути на її іконку в лівому нижньому кутку і ви відразу ж побачите її поточний стан і час, скільки хвилин тому її було визначено та заряд батареї.

Можна вибрати карту, яка буде відображатися: Open street maps, google hybrid, google streets.

При натисканні на іконку людини з'явиться меню, у якому можна переглянути історію переміщень її по карті, відстежити стан батареї пристрою та інтернету.

Стан батареї відображається на графіку використання батареї. У меню «Батарея і інтернет» видно, як часто дитина ставить телефон на зарядку, як швидко витрачається батарея, о котрій годині вона знімає телефон із зарядки. За цими даними можна робити висновки, як активно дитина користується телефоном.

У меню повідомлення можна налаштувати повідомлення при зниженні заряду батареї і створити «Місця геодзвінка», при вході/виході з яких вам надсилається автоматичне повідомлення на телефон і e-mail. Також можна прокласти маршрут на карті до людини. І в меню «Налаштування» можна призначити ім'я людині, змінити аватар або видалити людину.

Методи визначення місця знаходження телефону.

За даними розробників програми, визначення місцезнаходження відбувається за трьома напрямками:

- 1) GPS: точність 10–50 м лише на вулиці;
- 2) Wi-Fi: точність до 10–40 метрів та працює в приміщенні;
- 3) LBS-вишка: базові станції GSM-операторів мобільного зв'язку. Точність низька, приблизно 100–2000 м.

SENTRY — РОЗУМНИЙ БАТЬКІВСЬКИЙ КОНТРОЛЬ

Sentry — мобільний додаток батьківського контролю для батьків і дітей, які використовують пристрої Android.

Основні функції програми.

Компанія Sentry розробила алгоритми, що захищають дітей від небезпеки, яку спричиняє безконтрольне використання смартфонів і планшетів. Sentry перевіряє інтернет-трафік, мобільні додатки,



контент месенджерів та соціальних мереж у смартфоні / планшеті дитини щодо небезпечного текстового або візуального змісту, а також підозрілих активностей.

Додаток оповіщає батьків про можливі небезпеки за допомогою повідомлень. Залежно від виду загрози повідомлення може містити уривок підозрілого повідомлення або скриншот картинки. Dodatok не надає батькам доступ до вмісту телефону дитини, що дозволяє зберегти конфіденційність дитини та підтримувати здорові відносини між батьками й дітьми.

Установлення програми.

Спочатку додаток встановлюється на мобільний пристрій одного з батьків дитини. На вказаний під час реєстрації номер телефону надсилається посилання для скачування програми, яке потрібно встановити на смартфоні або планшеті дитини. Зверніть увагу на те, що іконка програми Sentry буде видна на телефоні дитини, тому ми рекомендуємо заздалегідь обговорити з дитиною мету встановлення програми.

Після встановлення програми батькам буде доступна така інформація:

- перегляд підозрілих картинок, отриманих або створених на пристрої дитини;
- місцезнаходження дитини (відстежування в режимі реального часу);
- статистика використання додатків на пристрої дитини;
- заряд батареї смартфона / планшета дитини;
- режим звуку, включений у цей момент на мобільному пристрої дитини (Без звуку / Вібрація / Звук);
- моніторинг усіх вхідних і вихідних дзвінків;
- історія перегляду вебсторінок;
- керування повідомленнями, які батьки бажають мати у випадку змін на мобільному телефоні.

GOOGLE FAMILY LINK — МОБІЛЬНИЙ ДОДАТОК БАТЬКІВСЬКОГО КОНТРОЛЮ

За допомогою **Family Link** батьки можуть зі свого пристрою віддалено встановлювати правила користування цифровим контентом для дітей різних вікових



Google Family Link

категорій. Це допоможе їм розумно розподіляти час між навчанням, іграми й інтернетом. Крім того, для дітей віком до 13 років (або відповідного віку для вашої країни) у Family Link можна створити обліковий запис Google, який функціонуватиме, як ваш, і матиме доступ до більшості сервісів Google.

Вимоги для встановлення Family Link.

- Телефон або планшет дитини повинен мати Android 7.0 або новішу версію ОС. На офіційному сайті повідомляється, що є деякі пристрої з Android 6 і 5, які також підтримують роботу, проте конкретні моделі не вказані.
- Пристрій батька може мати будь-яку версію Android, починаючи із 4.4, також можливе керування з iPhone або iPad.
- На обох пристроях має бути обліковий запис Google (його потрібно зробити заздалегідь). Також потрібно знати пароль від нього.
- При підключенні програми обидва пристрої мають бути підключені до інтернету (необов'язково до однієї мережі).

Інструкція налаштування Family Link.

- 1) На пристрої одного з батьків установити додаток «Google Family Link (для батьків)». Його можна завантажити з Play Маркет. Для iPhone/iPad, в App Store завантажити додаток Family Link. Запустити додаток та ознайомитися з можливостями батьківського контролю.
- 2) На запитання «Хто буде користуватися цим телефоном?» натиснути «Батьки». На наступному екрані — «Далі», а потім на запит «Станьте адміністратором сімейної групи» натиснути «Почати».
- 3) Дайте відповідь «Так» на запит про те, чи є в дитини акаунт Google (його потрібно зробити заздалегідь).
- 4) На екрані з'явиться запит «Візьміть пристрій вашої дитини». Натиснути «Далі». На наступному екрані буде показано код налаштування. Залишити свій телефон відкритим на цьому екрані.

- 5) Завантажити на телефон вашої дитини Google Family Link для дітей із Play Маркет.
- 6) Запустити в додатку запит «Вибрати пристрій, яким потрібно керувати». Натиснути «Цей прилад».
- 7) Увести код, що відображається на вашому телефоні.
- 8) Увести пароль від облікового запису дитини. Натиснути «Далі», а потім — «Приєднатися».
- 9) На вашому пристрої в цей момент з'явиться запит «Бажаєте налаштувати батьківський контроль для цього акаунта?» Відповісти «Так».
- 10) Ознайомитися з можливостями батьківського контролю і, у разі згоди, натиснути «Дозволити». Увімкнути менеджер профілів Family Link Manager (кнопка внизу екрану).
- 11) Увести ім'я для пристрою (як воно буде відображатися у вас) та вказати дозволені додатки (потім можна буде змінити).
- 12) Налаштування завершено. Натиснути «Далі». На пристрої дитини з'явиться екран з інформацією про те, що саме можуть відстежувати батьки.
- 13) На вашому пристрої на екрані «Фільтри та налаштування керуванням» обрати «Налаштувати батьківський контроль» і натиснути «Далі» для налаштування основних параметрів блокувань та інших параметрів.
- 14) На екрані з'явилися «плитки», перша з яких веде до налаштувань батьківського контролю, інші повідомляють основну інформацію про пристрій дитини.
- 15) Після налаштування на вашу електронну пошту та пошту дитини надійде кілька листів з описом основних функцій і особливостей функціонування Google Family Link, з якими рекомендовано ознайомитися.

Важлива інформація:

- налаштування Family Link можуть відрізнятися залежно від пристрою, яким користується дитина;
- за посиланням families.google.com/familylink/setup ознайомтеся з переліком сумісних пристроїв;

- ретельно перевіряйте додатки на контрольованому пристрої дитини й вимикайте ті, якими їй не варто користуватися. Зверніть увагу на те, що деякі попередньо встановлені додатки не можна вимкнути;
- щоб бачити місце знаходження пристрою дитини, цей пристрій має бути ввімкненим, активованим і під'єднаним до інтернету.

Хоча Family Link надає батькам інструменти для контролю дії дитини в інтернеті, це не робить всесвітню мережу безпечнішою. Завдання додатка — допомогти батькам обирати прийнятний для дитини контент і пояснити їй, як потрібно користуватись інтернетом.

9. ЕКРАННИЙ ЧАС. ЦИФРОВИЙ ДОБРОБУТ

Екранний час — кількість часу, проведеного за пристроєм з екраном (смартфоном, комп'ютером, телевізором чи відеогрою). Дослідження показують, що екранний час безпосередньо впливає на розвиток дитини, а також на психічне та фізичне здоров'я.

ВИКОРИСТАННЯ ФУНКЦІЇ «ЕКРАННИЙ ЧАС» НА IPHONE, IPAD АБО IPOD TOUCH

За допомогою функції «Екранний час» можна в режимі реального часу отримати доступ до звітів, у яких показано, скільки часу ви проводите з iPhone, iPad або iPod touch. Також можна встановлювати різні обмеження для тих аспектів, якими потрібно керувати.

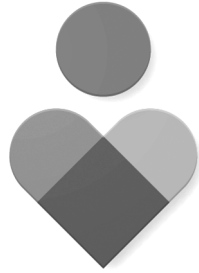


Включення функції «Екранний час».

- 1) Перейти до розділу «Налаштування» → «Екранний час».
- 2) Натиснути «Включити Екранний час».
- 3) Натиснути «Продовжити».
- 4) Вибрати «Це мій [пристрій]» або «Це [пристрій] моєї дитини».

«ЦИФРОВИЙ ДОБРОБУТ» НА ТЕЛЕФОНАХ ANDROID

На деяких телефонах можна отримувати інформацію про те, як ви використовуєте пристрій, зокрема, як часто розблоковуєте його або скільки часу працює кожний додаток. За допомогою цих даних можна покращити свій цифровий добробут. Наприклад, ви можете налаштовувати таймери додатків або планувати час переходу екрана в сплячий режим.



Як налаштувати «Цифровий добробут».

Для того, щоб «Цифровий добробут» відображався як додаток, знайдіть його в налаштуваннях і ввімкніть опцію «Показувати в списку додатків». Коли ви вперше відкриєте «Цифровий добробут», вам потрібно буде налаштувати свій профіль:

- 1) Відкрийте додаток «Налаштування»;
- 2) Натисніть «Цифровий добробут і батьківський контроль»;
- 3) У розділі «Інструменти Цифрового добробуту» натисніть «Показати мої дані».

Порада: ви також можете керувати обліковим записом своєї дитини, якщо ваш обліковий запис — батьківський для її пристрою.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Які емоційні симптоми мережевої залежності ви можете додати, крім визначених в посібнику?
2. Що відносять до персональних даних? Як ви поясните дитині необхідність захисту чи обмеження доступу сторонніх осіб до її персональних даних?
3. Як учителям забезпечити захист персональних даних під час дистанційного навчання?
4. Як захистити персональні дані під час спілкування в соціальних мережах?
5. Назвіть способи отримання електронного підпису.

ПРАКТИЧНІ ЗАВДАННЯ

1. Складіть пораду про створення надійного пароля, яка буде цікавою та зрозумілою дитині.
2. Налаштуйте опцію «батьківський контроль». Які поради ви можете дати іншим батькам із власного досвіду?
3. Складіть чек-лист алгоритму мережеских покупок (на 4–6 позицій). Оформіть його за допомогою ресурсу інфографіки.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА

1. Aircrack-ng home page [Електронний ресурс]. — Режим доступу : <https://www.aircrack-ng.org/> (дата звернення 15.07.2021).
2. Nipe [Електронний ресурс]. — Режим доступу : <https://kali.tools/?p=5019> (дата звернення 15.07.2021).
3. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник]/В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. — К., 2019. — 218 с.
4. Глобальна мережа інтернет. Основи інформаційної безпеки [Електронний ресурс]. — Режим доступу : <https://sites.google.com/site/kniginashevseua/lekciini-zanatta/globalna-mereza-internet-osnovi-informacijnoie-bezpeki> (дата звернення 15.07.2021).
5. Конспект лекцій із дисципліни «Захист інформації в комп'ютерних системах» [Електронний ресурс]. — Режим доступу : http://elartu.tntu.edu.ua/bitstream/lib/29278/1/%21%21_Lek_print_zahust_123.pdf (дата звернення 15.07.2021).
6. Уязвимости корпоративных информационных систем, 2019 [Електронний ресурс]. — Режим доступу : <https://www.ptsecurity.com/ru-ru/research/analytics/corporatevulnerabilities-2019/> (дата звернення 15.07.2021).

1. ПРИНЦИПИ СПІВПРАЦІ ПСИХОЛОГІВ І ОСВІТЯН ЩОДО ПІДТРИМКИ, ЗБЕРЕЖЕННЯ ПСИХІЧНОГО ЗДОРОВ'Я ДИТИНИ

Наведемо основні принципи співпраці психологів і освітян з означеного питання.

- Принцип поваги до індивідуальності дитини (це дозволить об'єктивно вивчити відповідні схильності й здібності).
- Принцип колективних взаємодій (конструктивний розвиток психологічних особливостей і доцільна корекція ризикової поведінки краще реалізуються в системі організованої колективної діяльності).
- Принцип розумної вимогливості (нормування поведінки законом, правилами шкільного розпорядку, нормами суспільної моралі, системою персонально значущих ціннісних орієнтирів).
- Принцип узгодження з віковими психологічними особливостями.
- Принцип діалогічних комунікацій.
- Принцип доцільної психолого-педагогічної підтримки.
- Принцип самоактуалізації мотиваційно-потребнісної сфери.

Увага! Перехід від дитинства до дорослості може відбуватися гостро й драматично. У цей період найвиразніше виявляються суперечливі тенденції фізіологічного, психічного, особистісного розвитку.

ПСИХОЛОГІЧНІ ОСОБЛИВОСТІ ПІДЛІТКОВОГО ВІКУ

Підлітковий вік характеризується нестійкою емоційною сферою, самоствердженням самостійності й індивідуальності, виникненням труднощів у відносинах із людьми старшого віку (наприклад негативізм, упертість), формуванням самооцінки, виробленням соціально значимого характеру,

акцентуацій характеру й дезадаптивних форм поведінки; формуванням власних поглядів на фоні значної міри навіюваності в середовищі однолітків, появою сексуальних потягів, формуванням самосвідомості через призму егоцентричності, виникненням надмірної втомлюваності через імпульсивні поведінкові прояви.

У цьому віці схильність до ризику часто пов'язана з агресивністю як такою, є засобом самоствердження. Підлітковому віку притаманні незрілість моральних настановлень, нігілізм. Це так само формує сприятливе середовище ризикової поведінки.

Створення належної атмосфери психологічного комфорту потребує уваги до ризикової поведінки підлітка. Конфліктність, нестриманість у проявах емоційних станів, невміння опановувати себе можуть стати сприятливим джерелом його асоціальної поведінки.

Психологічні особливості підліткового віку за Л. Абсаямовою¹:

- тенденція ідентифікації особистості, що виявляється у приписуванні та виявленні у собі відповідних рис Я-образу;
- тенденція становлення суб'єктності, що виявляється у визначенні власної інтенційності, усвідомлення спрямованості власних дій, за якими діяч відчуває власне авторство;
- тенденція інтенсивного розвитку самосвідомості, коли виникає активна потреба в самопізнанні, самовдосконаленні та саморозвитку;
- тенденція формування та розвитку рефлексії, коли дитина усвідомлює й себе у своїй цілісності та саморозвитку.

Характерні для підліткового віку суперечливість і подвійність відчуттів, емоційної сфери, що виявляються в усіх сферах життєдіяльності підлітків (наприклад, контраверсійна субкультура), вважаються нормою і необхідною умовою психо-фізіологічного розвитку в підлітковому віці:

¹ Абсаямова Л. М. Психолого-педагогічні передумови готовності до ризику у підлітків // Наукові записки Інституту психології ім. Г. С. Костюка АПН України. Київ, 2005. Вип. 26, т. I. 508 с.

нерівномірність розвитку функціональних систем організму, статеве дозрівання й пов'язані із цим переживання; прагнення до самостійності й відсутність реальних можливостей її втілення; наявність двох значущих і водночас суперечливих ціннісних систем — колективних настановлень і орієнтирів батьківського виховного впливу; переживання образи, самотності, персональної незатребуваності, відчуження внаслідок уявної чи надуманої втрати щирих відносин із батьками, почуття нерозділеного романтичного кохання, ревності, переживання через неспокій у родині, у зв'язку зі смертю близьких людей; загострене відчуття провини, образи, самозвинувачення внаслідок порушення стабільних позитивних відносин у найближчому оточенні; страх насмішок, глузування чи приниження, покарання за провини чи власне сам факт ризикової поведінки з негативними наслідками (проступок, правопорушення, шкода здоров'ю тощо), страх перед наслідками якогось неуспіху (незадовільна оцінка) тощо.

Підлітковому віку притаманні й деструктивні відчуття, які використовують підлітки в прагненні ухилитися від неприємних наслідків, прагнучи впливати на інших: жага помсти, злоба, протест, погрози, шантажування, бажання викликати співчуття, наслідування кіногероїв чи блогерів, моди, нереалізованість у персонально значущих аспектах життєдіяльності. Поведінка підлітків часто є непередбачуваною, може містити суперечливі ознаки, протилежні реакції. Наприклад, цілеспрямованість і наполегливість поєднуються з імпульсивністю, прагнення активності — з апатією, самовпевненість — із вразливістю характеру.

У підлітковому віці відбувається ретельне пізнання світу. Це часто пов'язано з деструктивною поведінкою, бо пошук форми самовираження «Я» часто не підкріплений достатнім інтелект-базисом (наприклад необдумана готовність до подвигу).

У США підлітків почали називати Screenagers: screen — екран, teenager — підліток. В Україні, як і у світі загалом, масове використання гаджетів спровокувало певне обмеження комунікативної активності в середовищі підлітків. Нині кількість часу, який вони щоденно проводять у мережі, викликає занепокоєння лікарів, педагогів, батьків і психологів.

Поширеним є твердження про те, що люди, які безконтрольно використовують інтернет, зазвичай не вміють адекватно оцінювати ризики навколишнього світу, відчувають труднощі в спілкуванні та не вміють співпереживати. Згодом це може призвести до проблем у працевлаштуванні, будіванні кар'єри, особистому житті.

У підлітковому віці не існує смерті, не сформовано цінності життя. Дитина не може усвідомити, а тому не відчуває цінностей життя й потенційної загрози смерті. Через це підлітки легко стають жертвами небезпечних ігор, флешмобів і маніпуляцій. Це зумовлено також тим, що в цьому віці простіше піти за натовпом, ніж знайти в собі сміливість бути незалежним, уміти відстояти свою індивідуальність.

Наведені вище психологічні особливості підліткового віку визначають необхідність формування системи попередження й пропедевтики ризикової поведінки з опорою на значущі досягнення підлітка:

- особистісне зростання, коли структурується свідоме ставлення до себе як до дорослої людини;
- готовність і здатність конструктивно діяти в ситуації ризику.

ПСИХОЛОГІЧНИЙ СУПРОВІД І ПІДТРИМКА ПІДЛІТКІВ ЗІ СХИЛЬНІСТЮ ДО РИЗИКОВОЇ ПОВЕДІНКИ

Психологічний супровід і підтримка підлітків зі схильністю до ризикової поведінки реалізується в таких контекстах:

- розвивальному (зміна мотивації до персонально та соціально значущої безпечної діяльності, розвиток творчих здібностей для самовираження особистості);
- інтеграційному (через взаємодію всіх соціальних інститутів), управлінському (що передбачає оптимізацію умов для позитивних змін, усіх способів комунікації підлітків);
- захисному (через створення ситуацій співчуття, співпереживання, взаєморозуміння);
- компенсувальному (умови для самовираження у форматі безпечного творчого самовираження й самореалізації потенцій);

- комунікативному (позитивний емоційний фон усіх контактів і взаємодій із підлітками);
- корекційному (корегувальні методи в конструктивних взаємодіях підлітків із ризиковою поведінкою).

Нині фактично кожна шоста людина на планеті — підліткового віку. Більшість підлітків мають достатньо міцне здоров'я, однак серед причин підліткової смертності часто є захворювання та серйозні травми.

За матеріалами ВООЗ, останніми роками у світі щоденно трапляється понад 3000 випадків смертей підлітків переважно з причин, які можна було завбачити чи попередити. Серед основних проблем, що в підлітковому віці пов'язані з ризиком для здоров'я, та спричиняють смертельні наслідки, ВООЗ виокремлює: випадкові травми (дорожньо-транспортні пригоди, керування транспортним засобом без дозвільних документів), утоплення (одна з десяти наймасовіших причин смертності в підлітковому віці), порушення психічного здоров'я (депресія як причина психічних розладів, інвалідності й суїцидів), факти насилля (у тому числі всі види булінгу), бідність і неприймання соціального розмаїття, приниження й відчуття непотрібності в родині. З-поміж інших причин: уживання ПАР, алкоголю, наркотичних речовин, ВІЛ/СНІД, інші інфекційні захворювання, завчасна вагітність серед дівчат підліткового віку, дітонародження.

Крім того, більшість психічних розладів починають виявлятися у віці 14 років, однак їхній перебіг майже непомітний, тому в дорослому віці захворювання стають невиліковними.

Єдиним доцільним засобом підтримки й розвитку психічного здоров'я є формування в підлітків гнучких життєвих навичок, надання психосоціальної підтримки, провадження програм, покликаних допомогти зміцненню зв'язків у родинях, де виховуються підлітки. Серед цілей у галузі сталого розвитку є забезпечення до 2030 року глобального всезагального доступу до послуг з охорони сексуального й репродуктивного здоров'я¹.

¹ SDG Indicators, Global Database <https://unstats.un.org/sdgs/indicators/database/?indicator=3.7.2>

2. КОМУНІКАТИВНА АКТИВНІСТЬ ЯК БАЗИС ПСИХОЛОГІЧНОГО ЗДОРОВ'Я

З упровадженням карантинних заходів істотно знизився рівень розвитку колективного життя в дитячих соціальних групах, переважна більшість форм колективної взаємодії перейшли в площину віртуальних заходів, геймерської активності. Заклад освіти як організаційне ядро в системі виховання втратив свою значимість. Поряд із зовнішнім фактором зростання вільного часу значно послабилася якісна його складова — раціональне використання цього вільного часу.

Вільний час суттєво впливає на розвиток особистості підлітка загалом і зокрема — на вдосконалення окремих форм діяльності підлітків.

Сучасне розуміння активності особистості, необхідної для діяльності, розглядається через джерела комунікації. Так, активність людини в психоаналітиків зумовлюється інстинктивними потягами (переважно це статевий інстинкт та інстинкт агресії). Активність трактується як біологічна сила та протиставляється суб'єкту¹.

Джерелом активності людини є потреби, що спонукають її діяти в певному напрямі². Задоволення комунікативних потреб людини передбачає процес оволодіння комунікативною діяльністю, опанування комунікативних умінь і навичок, які визначаються під впливом соціального оточення, культури в середовищі родини, типових соціальних інституціях.

Комунікативна активність виявляється в плануванні комунікативної діяльності, використанні різних комунікативних засобів, подоланні комунікативних бар'єрів, комунікативній взаємодії особистості з найближчим оточенням і середовищем друзів. Комунікативна активність певною мірою співвідноситься з комунікативними нормами та правилами, хоча вона визначається самим суб'єктом, мотивами й потребами в комунікативній взаємодії.

¹ Шинкарьок А. І. Психологія діяльності / А. І. Шинкарьок, В. А. Шинкарьок, Р. Г. Симко. — Кам'янець-Подільський : Оіум, 2009. — 207 с.

² Скрипченко О. В. Загальна психологія / О. В. Скрипченко, Л. В. Волинська, З. В. Огороднійчук. — Київ : Каравела, 2009. — С. 278.

Комунікативна активність належить тільки людині, а також має особистісно та емоційно забарвлені характеристики суб'єкта діяльності (психічні, моральні, соціальні тощо). Комунікативна активність виникає як життєвий витвір особистості, яка усвідомлює, що все необхідне від суспільства вона отримає тільки завдяки діяльності, якою вона обмінюється з іншими людьми.

Комунікативна активність породжується потребою в комунікативній взаємодії, опосередковується вищими життєвими потребами. Якщо не сформувалася комунікативна діяльність, то й комунікативна активність виявляється неповною мірою. Якщо комунікативна діяльність особистості агресивно орієнтована, то й комунікативну активність вона також може виявляти у вигляді агресивних проявів.

На комунікативну активність впливають особистісні, характерологічні риси, тип темпераменту. Комунікативна активність є мінливою, залежить від соціальних настроїв, тенденційної спрямованості, яку задають мас-медіа чи соціальні мережі.

Комунікативна активність може бути орієнтованою позитивно або негативно, на налагодження стосунків з оточенням, встановлення дружніх відносин.

Психологічну характеристику активності становлять: мотиви особистості, її спрямованість, ціннісні орієнтації, пізнавальні можливості.

До внутрішньої організації активності належать *мотиваційна, цільова та інструментальна* основи. Внутрішні переживання людиною стосунків із зовнішнім світом спонукають її до комунікативної діяльності.

На *мотиваційну основу комунікативної активності* впливають життєві потреби у їжі, продовженні роду; соціальні інтереси (необхідність комунікативно взаємодіяти з іншими людьми, набувати певного соціального статусу); екзистенціальні спонукання (потреба бути суб'єктом свого життя, створювати щось нове).

Цільова основа комунікативної активності спрямована на досягнення певної мети за допомогою комунікації. Комунікативна діяльність передбачає наявність у комунікативній активності здійсненого наміру, мети.

Інструментальна основа комунікативної активності складається з комунікативних знань, умінь та навичок. Це дає змогу людині визначати комунікативні стратегії. Засвоєння комунікативної діяльності виражається через комунікативні дії. Комунікативні дії частіше є усвідомленими, адже спрямовані на досягнення певної усвідомленої мети. Комунікативні дії, що часто повторюються, набувають функції комунікативних навичок.

Однією з форм проявів зниженої (або відсутньої) комунікативної активності є комунікативна неадаптивність. Інколи людина ставить собі комунікативну мету (недостатньо усвідомлену), досягнення якої є проблематичним (бракує комунікативних знань, умінь, навичок, заважають риси характеру, інтелектуальні здібності або інші обставини). Прикладів у соціальних мережах достатньо.

Недосягнення комунікативної мети породжує обмеження активної комунікації. Суть пасивної комунікативної неадаптованості полягає в тому, що людина не намагається досягнути комунікативної мети, є пасивною в комунікативній діяльності, не прагне до комунікативної взаємодії.

Особистісна комунікативна активність формується тоді, коли в людини виробляється свій стиль комунікативної активності. Під стилем комунікативної активності розуміємо певні комунікативні засоби та методи, активно застосовуючі які, особистість досягає комунікативної мети.

ЕТАПИ ФОРМУВАННЯ КОМУНІКАТИВНОЇ АКТИВНОСТІ ОСОБИСТОСТІ

- 1) Орієнтування на вибір комунікативного наміру, мотивація та добір засобів здійснення комунікативної діяльності відповідно до означеної мети.
- 2) Планування певних висловлювань із застосуванням вербальних і невербальних засобів.
- 3) Реалізація комунікації.
- 4) Самоконтроль за висловлюваннями, за відповідністю мови комунікативному задуму.
- 5) Оцінка результату комунікативного акту (задоволеність або незадоволеність результатом).

У світлі подій, що відбуваються у зв'язку з карантинними заходами, активна комунікація проходить у соціальних мережах, на численних платформах відеоконференцій. Важливий момент: від березня 2020 року онлайн-подій стало надміру багато, це почасти призводить до втрати характерологічно-особистісних рис. Однак зручні й креативні формати онлайн-комунікативної активності, вийшовши з резерву, залишаються в життєвій практиці назавжди. На другий план відійшла взаємодія з пресою, ми на довгий час відклали всі івенти, а діджитал-комунікації цікаві тільки в контексті персональних комунікацій (Zoom, Slack, Meet).

Внутрішні комунікації корисно здійснювати відповідно до компетентнісного підходу: говорити правду, оперувати фактами, нічого не приховувати, не перекладати відповідальність за ситуацію на когось, виконувати обіцяне й пояснювати, що ви робите.

Розглянемо основні виклики для ефективної внутрішньої комунікації. Згідно зі звітом Covid-19 Leadership Communication Research¹.

Сьогодні для успішної комунікації важливими є такі три основні чинники:

- бути зрозумілими й послідовними у своїй комунікації;
- чітко визнати, що вам відомо, а що ні;
- бути доступними для запитань і зворотного зв'язку.

У часи кризи зворотний зв'язок набуває особливої значущості. Комунікація точно не має бути односторонньою. Варто звернути увагу на такі моменти: чи є платформи та канали, де підліток може озвучити свої запитання? Чи є ресурси вчасно відповідати на ці запитання? Чи готові дорослі приділяти цьому час?

Ситуація невизначеності посилює негативні чинники обмеження комунікативної активності. Динамічність ситуації й неможливість спрогнозувати розвиток подій вимагають миттєвих коментарів. Висловлене вчора може виявитися не зовсім

¹ Див.: https://orangeifiery.com/uploads/Orangeifiery_COVID19_Leadership_Communications_Research_040320.pdf

3. Формування в підлітків безпечної поведінки в інтернет-мережі

коректною інформацією, і сьогодні вже треба її уточнити, відкоригувати та визнати, що висловлювання є неправильним.

«Будуть ситуації, коли вам, можливо, доведеться змінити свій підхід до чогось, повідомити, що попередня інформація вже застаріла, або попросити інших зробити щось, чого вони ніколи не робили. Визнайте, що ще можуть трапитися ситуації, у яких обставини змінюються поза вашим контролем чи виявляються абсолютно іншими, аніж ви очікували, і всім треба бути гнучкими», — зазначає у своєму брифі для лідерів «Navigating COVID-19» консалтингова компанія OrgangeFiery.

У ситуації невизначеності також діє правило «Не применшуйте ситуації». В Україні стан погіршується низьким рівнем довіри до офіційної інформації: 53 % опитаних переконані, що влада приховує ситуацію, а 38 % вважають, що медіа применшують серйозність епідемії (за опитуванням Соціологічної групи «Рейтинг»).

Тільки максимальна відвертість сприятиме довірі та підтримці. Пандемія лишить серйозний слід у комунікаційній культурі. Уміння виявляти повагу, підтримку, емпатію — ресурс людяності.

Як стверджують автори брифу CEO's New Role: Chief Empathy Officer, «комунікувати факти — це лише половина обов'язків для лідерів. CEO, серед іншого, мають реагувати на емоційні потреби своїх підлеглих — своїми словами та вчинками... щоб мотивувати їх у ці непрості часи».

Досить часто через неприйняття підлітків дорослими виникає посередник в образі комп'ютера. Якщо зважати на потреби та інтереси підлітків, стимулювати та підтримувати їхній розвиток, то можна уникнути багатьох проблем, пов'язаних із зануренням дитини у віртуальну реальність.

3. ФОРМУВАННЯ В ПІДЛІТКІВ БЕЗПЕЧНОЇ ПОВЕДІНКИ В ІНТЕРНЕТ-МЕРЕЖІ

В Україні з 2008 року за підтримки компанії «Майкрософт-Україна» та проєкту «Онляндія» створено та підписано Коаліцію за безпеку дітей в інтернеті, метою якої

є інформування користувачів інтернет-мережі щодо ризиків, які існують у віртуальному світі. У Польщі щорічно проводиться науково-практична конференція «Поведінка дітей та молоді в інтернеті». Головне питання, що розглядалося на ній фахівцями з різних країн світу (Дж. Карр, О. Дікс, Дж. Роман, М. Войтас), — діяльність дітей та молоді в соціальних мережах.

Детермінанти ризикової поведінки молоді у віртуальному світі:

- велика кількість необ'єктивної й неправдивої інформації, яку може розміщувати на вебпорталах будь-який користувач інтернет-ресурсів;
- спілкування з небезпечними особами, які видають себе не за тих, ким вони є насправді; залучення до асоціальних організацій;
- можливість реальної зустрічі з невідомими віртуальними співрозмовниками, які в реальному житті можуть бути небезпечними для дитини;
- навігація без мети, тобто «блукання інтернетом»;
- значна кількість спаму; поширення порнографії, а також фото- та відеофайлів із зображенням сцен жорстокості чи знущання;
- виникнення інтернет-адикції, тобто ризик заміни реального світу на віртуальний у свідомості дитини¹.

Якщо порнографічні матеріали чи матеріали з ненормативною лексикою можна відносно легко ідентифікувати та не використовувати їх або ж установити фільтрації, то від небажаної інтернет-інформації інших типів підлітків захистити досить важко. Наприклад, через типову для мережі інтернет анонімність матеріалів вона дає змогу розміщувати будь-якому користувачеві необ'єктивну, неправдиву інформацію сумнівної якості, так зване «інформаційне сміття», що призводить до хаотизації та знецінення знання, інтелектуально-пізнавальної діяльності, формування фрагментарних, «мозаїчних», безсистемних

¹ Веретенко Т. Г. Детермінанти формування безпечної діяльності молоді в мережі інтернет / Т. Г. Веретенко, М. А. Снітко. — [Електронний ресурс]. — Режим доступу : <http://elibrary.kubg.edu.ua/1310/>.

і невідповідних уявлень про світ, створює можливості для маніпуляцій свідомістю підлітка, нівелює загальні життєві цінності.

На численних дитячих сайтах можна зустріти різноманітні форми прояву ненависті: від радикального расизму до грубого висміювання певних явищ чи осіб. Найтиповіший формат анімаційних відео для підлітків — пранки. Вони, на перший погляд, можуть здаватися безпечними для підлітків, проте роблять певний внесок у формування молодіжної онлайнової культури та діяльності, у якій грубість, насміхання вважаються нормою. За допомогою мережі інтернет асоціальні організації легко знаходять сприйнятливих користувачів та затягують їх у свої спільноти, використовуючи для цього чати та електронну пошту. Спілкування у віртуальному просторі з представниками асоціальних організацій може призвести до реальної зустрічі з ними та залучення підлітків до таких організацій. Зважаючи на те, що віртуальний світ, як і реальний, має свій злочинний сегмент, однією з найпоширеніших форм протиправної діяльності у віртуальному просторі є хакерство. Зламавши поштовий сервер, хакери отримують доступ до величезної кількості електронних адрес. Після цього вони відправляють на ці адреси несанкціоновані поштові розсилки провокативного змісту. Значна частина підлітків часто відкриває такі повідомлення та діє відповідно до їхнього змісту. Невміння працювати з комп'ютером і орієнтуватися в інтернет-просторі в сучасному суспільстві можна порівняти з функціональною неграмотністю¹. Комп'ютер, інший гаджет є не тільки розвагою, але й засобом спілкування, самовираження та розвитку. У кіберпросторі існує значна кількість спеціальних сайтів, адресованих дітям різного віку.

Знання цих небезпек, урахування вікових та індивідуальних інтересів і потреб підлітків дадуть змогу їх уникнути.

¹ Вакуленко О. В. Формування безпечної поведінки підлітків в інтернет-мережі як психолого-педагогічна проблема / О. В. Вакуленко, В. В. Гнатюк // Наукові записки Вінницького державного педагогічного університету імені Михайла Коцюбинського. Серія : Педагогіка і психологія. — 2014. — № 42(2). — С. 122–125. [Електронний ресурс]. — Режим доступу : http://nbuv.gov.ua/UJRN/Nzvdpu_pr_2014_42%282%29__31.

Альтернативою має стати створення здорових адекватних умов для повноцінної соціалізації дитини поза віртуальним світом.

ФАЗИ ДЕСТРУКТИВНОЇ ПОВЕДІНКИ ПІДЛІТКА

Перша фаза (стихийно-адаптаційна) характеризується низькою психічною стійкістю, невпевненістю у виборі стратегії поведінки в небезпечних ситуаціях, сам вибір здійснюється методом спроб і помилок, вирішальну роль відіграють випадковість та оточення.

Друга фаза (стимульно-формувальна) виявляється в копіюванні стилів життя та діяльності інших, шаблонності поведінки, повною мірою не усвідомлюється вплив власної поведінки на рівень ризику в процесі діяльності.

Третя фаза (потребово-мотиваційна) визначається формуванням власної системи поглядів, переконань та відповідною безпечною поведінкою, теоретичні знання використовуються не за шаблоном, а інтерпретуються залежно від ситуації, власних потреб, інтересів і досвіду. На цьому етапі створюється обернений зв'язок між знаннями, переконаннями та вірою в досягнення мети.

Четверта фаза (самоактуалізацій) передбачає достатньо стійкий світогляд, високий рівень інтелектуальної активності, здатність урахувати наслідки прийнятих рішень, прогнозувати розвиток небезпечної ситуації залежно від зміни умов та власної поведінки.

ПОКАЗНИКИ ГОТОВНОСТІ ПІДЛІТКІВ ДО БЕЗПЕЧНОЇ ПОВЕДІНКИ:

- когнітивний (наявність знань про способи безпечного поводження, пізнавальна активність, аналітичний стиль мислення);
- потребово-мотиваційний (спрямованість і мотивація підлітків на безпечну поведінку, потреба й бажання підлітків у забезпеченні особистої й суспільної безпеки, рівень внутрішньої мотивації учнів до підготовки й самопідготовки у сфері безпеки);
- діяльнісно-практичний (навички, уміння, необхідні для реалізації безпечного поводження, фізична

3. Формування в підлітків безпечної поведінки в інтернет-мережі

підготовленість, нервово-психологічна стійкість, рівень тривожності як показник розвитку впевненості підлітків, реалізація безпечного поводження в повсякденному житті);

- творчий (уміння бачити проблеми, нестандартність мислення, здатність до інновацій).

Відповідно виокремлюють *чотири етапи у формуванні безпечної поведінки*:

- *перший етап* — ознайомлення дітей із загальними нормами, алгоритмами, правилами безпечної поведінки. Учень має знати, як потрібно себе поводити в небезпечних ситуаціях і чому саме так;
- *другий етап* — формування ставлень. Учителю необхідно викликати позитивне ставлення учнів до норм і правил безпечної життєдіяльності, сприяти готовності дитини сприйняти їх як значущі для себе;
- *третій етап* — формування поглядів і переконань. Цей етап характеризується сприйняттям і перетворенням норм, правил безпеки, алгоритмів дій в особисте надбання;
- *четвертий етап* передбачає формування спрямованості особистості.

ШЛЯХИ ЗМІЦНЕННЯ ПСИХІЧНОГО ЗДОРОВ'Я:

- традиції в найближчому оточенні (родинному колі, учнівському колективі; створення стабільної обстановки, що відповідає потребам дітей стосовно здоров'я та харчування, що забезпечує захист від небезпечних факторів і можливості для раннього навчання та спілкування з іншими в позитивному емоційному тоні);
- підтримка дитини (розвивальні чи навчальні курси);
- підтримка жінки-матері, літніх людей, дитини, яка перебуває у вразливій ситуації;
- програми з профілактики стресу;
- стратегії у сфері поліпшення умов дозвілля й комунікації дітей;
- залучення до продуктивної діяльності (волонтерство, меценатство, екологічні акції тощо).

ЛИСТІВКА-ПОРАДНИК

Ситуації, коли краще діяти

упевнено:

- тобі пропонують щось небезпечне або те, що тобі не підходить;
- хочеш повернути бракований товар;
- хочеш попросити про послугу або допомогу;

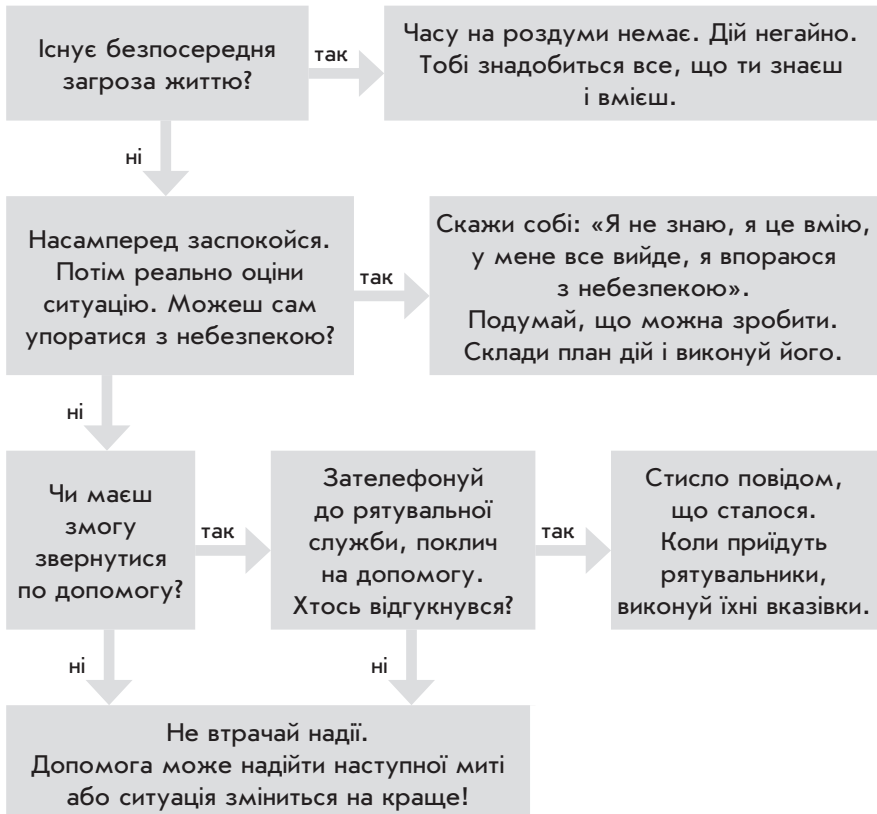
пасивно:

- у ситуації, коли будь-яке загострення стосунків є небезпечним;

агресивно:

- на тебе напали або намагаються кудись затягти.

АЛГОРИТМ ДІЇ В СИТУАЦІЇ НЕБЕЗПЕКИ



4. МЕРЕЖЕВИЙ ЕТИКЕТ УЧАСНИКІВ ФОРУМІВ ТА ЧАТІВ

Уживають ще терміни «інтернет-етикет», «нетикет» — від слова *Netiquette* (англ. *network etiquette*). Тут основна увага звертається на правила спілкування та взаємодії користувачів в інтернеті.

Правила спілкування та взаємодії мають дорадчий характер. Вони координують діяльність та інші види активностей у дистанційних форматах комунікування. Мережевий етикет в основі повторює норми й правила етики в спілкуванні й взаємодії між людьми у звичному форматі.

Дотримання цих правил і порад сприятиме тому, що спілкування в мережі дасть змогу привернути позитивну увагу до своєї особи і ви можете бути приємним співрозмовником.

Форум — асинхронний спосіб комунікації. Класичний варіант — текстові повідомлення. Може містити гіпертекст, посилання, графічні зображення чи відео. Форуми бувають вузькотематичні й політематичні. Цілі форумів: освітні, інформаційно-аналітичні, виробничі, навчальні тощо.

Чат — сервіс обміну текстовими, візуальними повідомленнями в реальному часі. Одночасно можуть спілкуватися численні групи людей.

Модератор — людина, яка визначає правила й тематику форуму або чату, іншої мережевої спільноти, контролює дотримання всіма учасниками правил етичного спілкування та корегує можливі технічні порушення чи утруднення під час дискусій.

ПРАВИЛА, ЯКІ СТАНУТЬ У ПРИГОДІ ПІД ЧАС СПІЛКУВАННЯ НА ФОРУМАХ, У ЧАТАХ

1) Загальні поради.

У мережі ми спілкуємося з людиною. Слід до цього ставитися уважно. Перш ніж долучитися до дискусії, дайте собі відповідь на запитання: «Ви знаєте цю людину? Думка цієї людини для вас цінна? Ви знаєте, у якому емоційному й фізичному стані перебуває людина під час конкретного сеансу спілкування?».

Пам'ятайте: усе, що ви виклали в мережі, залишиться там назавжди. Будьте розважливими. Написане і поширене вами колись може бути використане проти вас.

Зважайте на силу слова, думайте спершу, ніж писати, щоб написане не образило співрозмовника.

Виявляйте рефлексію. Будьте завжди ввічливі. Будьте терплячі. Виявляйте толерантність. Ігноруйте виклики на конфлікт і суперечку.

2) *Рекомендації щодо мовлення.*

Дотримуйтеся норм писемного мовлення, демонструйте грамотність і широкий словниковий запас.

Намагайтеся дотримуватися стилістичних і граматичних правил текстових повідомлень. Якщо не можете висловитися чітко, краще втримайтеся від участі в дискусії.

Ураховуйте, що ваш співрозмовник може не володіти емпатією чи рефлексією. Тому висловлюйте свою думку чітко, зрозуміло, однозначно.

Не користуйтеся чужими висловлюваннями без указівки авторства.

Використовуйте й поширюйте тільки об'єктивно достовірну інформацію. В іншому випадку будьте розважливими: пам'ятайте, що буде незручно, якщо ви станете поширювачем чи створювачем пліток або фейкової інформації.

У висловлюваннях дотримуйтеся логіки: самого висловлювання, відповідності вашій позиції та логіці висловлювань інших учасників.

У тексті вживайте зрозумілі, бажано, короткі, прості речення. Іншим буде простіше і швидше сприймати запропонований текст.

Перш ніж долучитися до дискусії, ретельно вивчіть тему, зміст попередніх висловлювань, характер і стиль відповідей, проаналізуйте загальну тональність спілкування. Подумайте, чи варто вести полеміку.

У мережі поведіть себе так само, як поводити себе в реальному житті, коли хочете справити приємне враження на інших.

Якщо виникла етична проблема в мережевому просторі, продумайте спосіб її розв'язання в реальному житті — і ви знайдете правильне рішення.

3) *Правила, які допоможуть зберегти цінності мережевого спілкування.*

Цінують час і увагу свої та інших людей.

Цінують можливості й ресурси мережевого спілкування. Можливості тут ужито в значенні пропускової здатності каналу, порту, фізичної ємності носіїв інформації на відданому носії. Якщо ви сім повідомлень відправили на одну конференцію або чат чи форум, то ви забрали час, ресурси збереження інформації інших учасників марно шість разів поспіль.

Перш ніж написати щось, подумайте, чи інші учасники потребують вашої інформації, чи не жалкуватимуть вони про час, витрачений на прочитання вашого повідомлення. Якщо у вас виник сумнів, краще не пишіть.

Допомагайте іншим там, де можете зробити це ефективно. Намагайтеся презентувати цікаву чи корисну інформацію для багатьох. Щедро діліться своїм продуктивним досвідом. Демонструйте свою експертність у конкретній галузі. Утім залишайте можливість поспілкуватися іншим учасникам форуму чи конференції.

Шанобливо реагуйте на приватні повідомлення.

Не розміщуйте висловлювання й тексти провокативного характеру. Дискусія в мережі навряд чи вирішить проблему. Шукайте шлях розв'язання проблеми в реальній взаємодії.

Виявляйте делікатність. Якщо ви помітили помилку чи виявили порушення правил, краще звернутися до модератора, адміністратора чи написати приватне повідомлення тому, хто помилився. У такому повідомленні коректно викладіть суть і спосіб виправлення помилки чи хиби.

У форумах і чатах є нормою, коли учасники допомагають іншим орієнтуватися в потоці повідомлень так: «+» — корисна інформація, «-» або «0» — на повідомлення не марнувати час.

Якщо ви хочете поділитися інформацією з кимось, але така інформація не пов'язана з темою цього форуму чи чату, краще скористатися приватним повідомленням з поміткою OFF.

Не використовуйте Caps Lock, це відволікає увагу учасників і вимагає додаткових пояснень, адже більшість користувачів мережі сприймає це за крик.

4) *Формат підпису учасника чату чи форуму.*

Використовуйте позитивний ресурс анонімності. Зокрема, ви можете створити собі псевдонім (краще не вживати імена інших людей), який делікатно виражатиме вашу харизму, або ж можете виступити користувачем 12345 (набір цифр — довільний). На конференціях, форумах, де кількість людей перевищує 30 осіб, краще зберігати анонімність.

Якщо ж чат чи форум професійний, навчальний, доречно використовувати тільки власне ім'я та прізвище.

РИЗИКИ СПІЛКУВАННЯ НА ФОРУМАХ І В ЧАТАХ

Флейм — суперечка заради суперечки. Краще уникати такого явища в онлайн-спілкуванні. Ознаки флейму: учасником втрачено основну тему чи думку діалогу, співрозмовник у висловлюванні не враховує думку інших учасників онлайн-спілкування, його висловлювання вкрай емоційні, він використовує багато різноманітних смайлів, розділових знаків без потреби, висловлюється про особистість, допускає оцінні судження з приводу національності, релігії, статі, професійного розвитку, зовнішності інших людей, провокує конфлікт. Краще уникати й не підтримувати флеймерів.

Оверквотінг — надмірне цитування. Під час відповідей на форумі часто звертаються до першоджерела, яке визначило тематику цього конкретного форуму. Тож доцільно під час кожної відповіді не цитувати увесь лист, а лише фрагмент, який стосується вашої відповіді. У разі згоди висхідне цитування взагалі не варто робити.

Флуд — низка коротких однорядкових повідомлень, що не мають спільної теми та чіткої зрозумілої мети. Це повідомлення, які можна видалити без шкоди для загальної дискусії. Мета флуду — привернути до себе увагу, відволікти увагу від суті поданої на форумі інформації, збільшити витрати часу та інших ресурсів учасниками форуму. Смайли допомагають візуалізувати емоцію в тексті. Однак краще

в тексті використовувати за змістом не більше двох смайлів, інакше текст важко сприймати.

Оффтоп — відхід від теми дискусії. Схожий на флуд і, по суті, у нього переростає. Модератори мають відслідковувати це. Однак варто й самим учасникам намагатися чітко дотримуватися заявленої теми.

Бан — обмеження активності в мережевому спілкуванні отримує той, хто порушив заявлені правила спілкування, чи поводить себе непристойно. Це суворий захід покарання — забанений втрачає доступ до ресурсу. Банять за відверте хамство, перехід на особистості, розпалювання конфлікту, навмисне поширення неправдивої та шкідливої інформації. Зазвичай напередодні чи на початку форуму або чату визначаються правила й умови спілкування, указується, за що модератор може забанити учасника.

5. БЕЗПЕКА КОРИСТУВАННЯ ЕЛЕКТРОННОЮ ПОШТОЮ

Безпека й етика електронного листування, використання електронної пошти — це один із пріоритетів системи кібербезпеки, яку повинен будувати кожен користувач ПК. Усі авторизації акаунтів, зміна паролів, конфіденційна інформація приватного та фінансового характеру проходять через персональний e-mail. Контролюючи поштову скриньку людини, можна з імовірністю в 90 % отримати доступ до її фінансових ресурсів.

Електронна скринька — зручна мішень для спаму або ймовірності, що через заповнення вашої скриньки спамом, власне і ваші листи автоматично будуть віднесені до спаму. Це істотно ускладнить можливість зворотного зв'язку. Також використання інформації з електронної пошти третіми особами може призвести до протиправних дій щодо ваших партнерів, друзів, родичів. Можливі анонімне ображення електронною поштою, агресія або переслідування.

Умовою психологічного здоров'я є впевненість у збереженні персональних даних і контролю за потоком інформації через листування. Електронне листування може бути особистим, корпоративним, навчальним, професійним

тощо. Інформація листування має узгоджуватися з безпекою в цифровому мережевому просторі, учасники повинні дотримуватися загальних правил етики електронного листування.

Електронна пошта, e-mail — спосіб обміну інформацією з використанням цифрових пристроїв (ПК, смартфон тощо). Можна пересилати інформацію в будь-якому форматі (текстові документи, відео, аудіо, візуальний контент, програми тощо).

Операції з електронною поштою: створення, відправлення, копіювання листів (зокрема прихована копія), прийом, відповідь, пересилання листів, видалення.

Фішинг — вид мережевого шахрайства, коли злочинець надсилає підроблений електронний лист, меседж нібито з офіційного джерела з проханням надати чи підтвердити конфіденційну інформацію. Приклад: електронні листи з пропозиціями підтвердити реєстрацію облікового запису з посиланням на сайт, інтерфейс якого зовні здається достовірним.

Спам — масове розсилання листів із рекламою без попередньої згоди отримувача.

НАЙПОШИРЕНІШІ ПРОГРАМИ ЗІ СТВОРЕННЯ ЕЛЕКТРОННОЇ ПОШТИ¹

1) <https://www.ukr.net/>

Обсяг безкоштовної поштової скриньки — безлімітний. Інтерфейс скриньки доступний українською, російською та англійською. Мобільний додаток відсутній. Можливість підключати свій домен не передбачена. Збір пошти з інших скриньок неможливий. Під час відправлення листа з вкладенням понад 20 мегабайт поштовий сервіс завантажить його на внутрішній файлообмінний сервіс eDisk. Тільки одержувач зможе завантажити вкладення, якщо він теж є користувачем Ukr.net.

2) <http://www.i.ua/>

Обсяг безкоштовної поштової скриньки — 1,6 Гб з можливістю його збільшити не частіше ніж раз на

¹ Source. [Електронний ресурс]. — Режим доступу : <https://samoosvita.in.ua/ukrayinska-elektronna-poshta-oglyad-bezkoshtovnyh-servisiv>

місяць. Інтерфейс скриньки — тільки російською. Мобільний додаток відсутній. Можливість підключати свій домен не передбачена. Збір пошти з інших скриньок неможливий. Пошта передається по незахищеному з'єднанню, і будь-хто може перехопити ваш пароль. Функціонал поштової служби, заявлений в описі, не відповідає доступним функціям.

3) <http://meta.ua/>

Обсяг безкоштовної поштової скриньки — 0,1 Гб з можливістю його збільшити не частіше одного разу на місяць. Інтерфейс скриньки доступний українською, російською та англійською. Мобільний додаток відсутній. Можливість підключати свій домен не передбачена. Збір пошти з інших скриньок можливий не частіше ніж через 3 години, і не більше 200 листів за раз (повідомлення понад 30 Мб не будуть прийняті). Пошта передається по незахищеному з'єднанню, і будь-хто може перехопити ваш пароль. Функціонал поштової служби не відповідає доступним функціям.

4) <http://www.bigmir.net/>

Обсяг безкоштовної поштової скриньки — 1 Гб з можливістю його збільшити не частіше ніж раз на місяць. Відсутній інтерфейс українською. Мобільний додаток відсутній. Можливість підключати свій домен не передбачена. Збір пошти з інших скриньок неможливий, хоча функціонал заявлений. Пошта передається по незахищеному з'єднанню, і будь-хто може перехопити пароль. Функціонал поштової служби не відповідає доступним функціям.

5) <https://gmail.com/>

Поштовий сервіс компанії Google. Один із найстабільніших і надійних поштових сервісів.

Інтегроване хмарне сховище файлів на 15 Гб (але Gmail ділить його з Google Photo, Google Drive та іншими сервісами, які є частиною Google-акаунта). Один із кращих алгоритмів для виявлення і фільтрації спаму. Зрозумілий інтерфейс, зручний пошук листів, фрагментів повідомлень. Усі повідомлення автоматично розподіляються за категоріями, такими як «Основні», «Реклама», «Форуми» тощо. Продуманий захист конфіденційності особистої інформації.

Стандарти POP і IMAP дають доступ Gmail до будь-якої програми електронної пошти та девайсів. Gmail розміщує контекстну рекламу поруч із прочитаними листами.

6) <https://outlook.com/>

Поштовий сервіс компанії Microsoft дає багато можливостей, особливо для роботи в Microsoft Office. Простий сервіс, але за функціональністю він не поступається Gmail.

Надається безкоштовне сховище на 15 Гб (але воно є загальним для Office і OneCloud та інших сервісів Microsoft). Передбачена синхронізація з іншими сховищами. Усі важливі повідомлення автоматично виділяються й збираються в одну папку.

Запрошення та повідомлення про події можуть синхронізуватися з календарем. Є вбудована підтримка Skype, а також доступ до Evernote, PayPal, GIPHY, Yelp, Uber.

7) <http://mail.yahoo.com/>

Поштовий сервіс компанії Yahoo!. Інтерфейс сервісу нагадує Gmail, але функціональні можливості скромніші. Актуальні доповнення: зручний фільтр для повідомлень, передбачена синхронізація з Facebook, імпорт контактів з інших сервісів, наприклад, із Facebook, Gmail, Outlook, підтримка облікових записів інших електронних пошт, які підтримують стандарти IMAP або POP, інтеграція з хмарним сховищем Dropbox.

За своєю функціональністю Yahoo! поступається Gmail і Outlook. Однак користуватися поштою Yahoo! дуже зручно: вільна форма маркування й розумні папки, фільтр очищення спаму працює ефективно.

8) <https://www.icloud.com/mail/>

Поштовий сервіс компанії Apple. iCloud Mail — це безкоштовна електронна пошта від компанії Apple з великою пам'яттю, IMAP-доступом і цікавим функціональним вебдодачком. Маєте доступ до своїх електронних листів із будь-якого з ваших пристроїв Apple, але також можете керувати календарями та контактами й синхронізувати інформацію.

Однак інтерфейс iCloud не пропонує функції для продуктивної роботи або організації листів, також цей сервіс не підтримує доступ до інших акаунтів електронних сервісів. Доступ до POP в iCloud теж відсутній.

9) <http://webmail.aol.com/>

Поштовий сервіс компанії AOL (Американський медійний конгломерат) — безкоштовний поштовий сервіс із необмеженим онлайн-сховищем, дуже хорошим захистом від спаму і простим інтерфейсом. AIM Mail має захист від спаму і надійні функції безпеки. Багатий інтерфейс спрощує використання AIM Mail та інтегрує календар, чат і соціальні мережі.

AIM Mail пропонує необмежений онлайн-простір для зберігання електронної пошти та доступ до POP або IMAP.

Недолік — у продуктивності (немає ярликів, розумних папок і коментаря текстових повідомлень, що стосуються однієї теми або питання).

ПРАВИЛА ДОРАДЧОГО ХАРАКТЕРУ, ЯКІ СТАНУТЬ У ПРИГОДІ ПІД ЧАС КОРИСТУВАННЯ ЕЛЕКТРОННОЮ ПОШТОЮ

Не нехуйте загальною безпекою вашого гаджета, ПК. Користуйтеся надійними актуальними програмами антивірусного захисту.

Будьте уважними під час перегляду отриманої кореспонденції. Не розпаковуйте вкладені в них архіви, не переходьте за посиланнями, розміщеними в тілі сумнівного листа.

У разі отримання підозрілого листа від незнайомого користувача видаліть повідомлення. Якщо такий лист надійшов від вашого знайомого, з'ясуйте, чи саме він надсилав такого листа.

Не відповідайте на підозрілі листи. Не грайте зі зловмисниками.

Перевіряйте прикріплені файли антивірусною програмою.

Не передавайте свій пароль від електронної пошти третім особам, яким ви не довіряєте, під час реєстрації, заповненні форм, на прохання для уточнення інформації тощо.

Якщо електронною поштою користується дитина, дорослі можуть зробити таке:

- установити фільтр спаму. Рекомендується, щоб адреса електронної пошти, якою користуватиметься дитина, була отримана від постачальника послуг інтернету, який пропонує автоматичний антивірусний захист та фільтрування спаму;

- установити фільтр за адресами. Дитина таким чином отримає доступ лише до пошти, що надійшла з визначених батьками адрес;
- використовувати анонімну електронну адресу. Адреси електронної пошти часто мають формат «ім'я.прізвище@hotmail.com». Якщо ваша дитина бажає обмінюватися повідомленнями електронної пошти зі своїми онлайн-співрозмовниками, краще використовувати адресу електронної пошти, яка не містить у назві її повне ім'я, використовувати псевдонім, або набір цифр, наприклад «986754231010@hotmail.com». Цифрові електронні адреси рідше атакуються спамом, оскільки їх важко підібрати.

Якщо Ваша дитина отримує зловмисні повідомлення електронною поштою, поясніть їй таке:

- дитина не повинна відкривати повідомлення від незнайомих осіб. Не варто відповідати на листи з погрозами;
- варто зберегти скрін такого повідомлення для подальших дій;
- якщо образи почастішали, краще змінити адресу електронної скриньки;
- можна скоригувати налаштування програми електронної пошти, щоб сумнівні листи відправлялися в папку «спам»;
- у разі обізнаності з каналом неетичного листа, можна відправити копію зловмисного повідомлення постачальнику інтернет-послуг із проханням скасувати зазначену адресу електронної пошти. Якщо не знаєте адреси відправника, попросіть вашого постачальника інтернет-послуг надати вам допомогу;
- не потрібно надавати особисту інформацію невідомим особам. У разі відсутності відповіді на ваші запитання краще не передавати жодних даних такому абоненту.

ЗАХОДИ БЕЗПЕЧНОЇ ЕЛЕКТРОННОЇ ПОШТИ

Шифрування електронної пошти.

У такий спосіб можна захистити особисту інформацію від хакерів. Шифрування дає змогу отримати доступ до

листування з вами певним користувачам. Можна завантажити чи придбати додаткове програмне забезпечення, яке підключається до Microsoft Outlook. Можна інсталиувати сертифікат електронної пошти, зокрема PGP (Pretty Good Privacy), за допомогою якого, наприклад, професійна спільнота зможе поділитися відкритим ключем з усіма, хто хоче надсилати вам електронну пошту. За допомогою закритого ключа можна розшифровувати всі отримані повідомлення.

Ще одне рішення — це служба електронної пошти з можливістю шифрування в Office 365 (послуга платна).

Використання безпечних паролів.

Пароль має бути складним: 12 символів (цифри, розділові знаки, великі і малі літери).

Треба змінювати пароль не менше ніж раз на три місяці.

Як пароль не слід використовувати очевидне: дати народження, імена дітей, дівоче прізвище тощо.

Не варто використовувати однаковий пароль для різних облікових записів або вебсайтів.

Корисно користуватися менеджерами паролів або функцією єдиного входу CommonKey, LastPass і Password Genie.

Підписка на контрольні служби PwnedList, Breach Alarm допоможе відстежувати інформацію про вразливість вашої електронної скриньки.

Розважлива політика збереження електронної пошти.

Сортуйте листи.

Регулярно видаляйте листи-спами.

Розподіліть електронну пошту на особисту й робочу. У робочій поштової скриньці зберігайте тільки ділову кореспонденцію. Здійснюйте регулярне очищення поштових скриньок від застарілої інформації.

Не взаємодійте з кореспонденцією сумнівного характеру від невідомих чи прихованих адресатів: не відкривайте листи, надіслані посилання чи архіви.

Не відповідайте на електронні листи із запитом про пароль чи персональні відомості, як би офіційно не виглядало «тіло» листа.

Регулярно оновлюйте антивірусні програми.

Перед відправленням шифруйте листи з конфіденційними даними (завжди).

Не користуйтеся корпоративною поштою для особистого листування.

Не розсилайте листи корпоративної пошти адресатам з інших систем електронної пошти.

У професійній діяльності варто суворо дотримуватися корпоративних правил використання особистих мобільних пристроїв: обов'язково шифрувати дані, захищати пристрій складним паролем, інстальювати схвалені програми безпеки, щоб не допустити неавторизований доступ до пристрою через загальнодоступний Wi-Fi.

Не варто залишати гаджет без нагляду.

Відкритий ключ можна передати будь-кому. Закритий ключ, який розкодує повідомлення, зберігається тільки в адресата. Механізм: власники електронних скриньок у програмі до пошти генерують собі ключ (невеликий файл на комп'ютері), який складається з двох половинок: відкритої і закритої. Закритий ключ — це як пароль, але значно довший, генерується програмою. Він зберігається у вас на комп'ютері й не передається нікому.



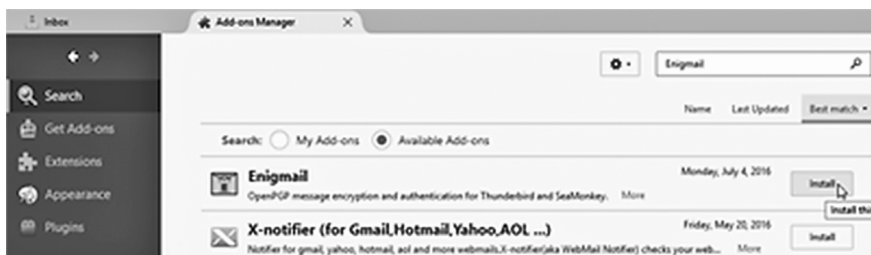
Натомість, відкритий ключ ви можете пересилати своїм друзям і знайомим, щоб вони мали змогу надіслати вам захищеного листа, а також попросити, щоб вони переслали вам свої відкриті ключі. Ви також можете опублікувати свій відкритий ключ на власному вебсайті.

Відкритий ключ може тільки закодувати лист перед надсиланням, але не розкодувати його. Щоб прочитати листа, потрібен ваш закритий ключ, який є тільки у вас і захищений паролем.

Заінстальуйте **Mozilla Thunderbird** і під'єднайте до неї вашу електронну скриньку (увести ім'я, адресу й пароль під час запуску).

Через менеджер додатків Thunderbird установіть Enigmail (кнопка меню ≡ → Додатки):

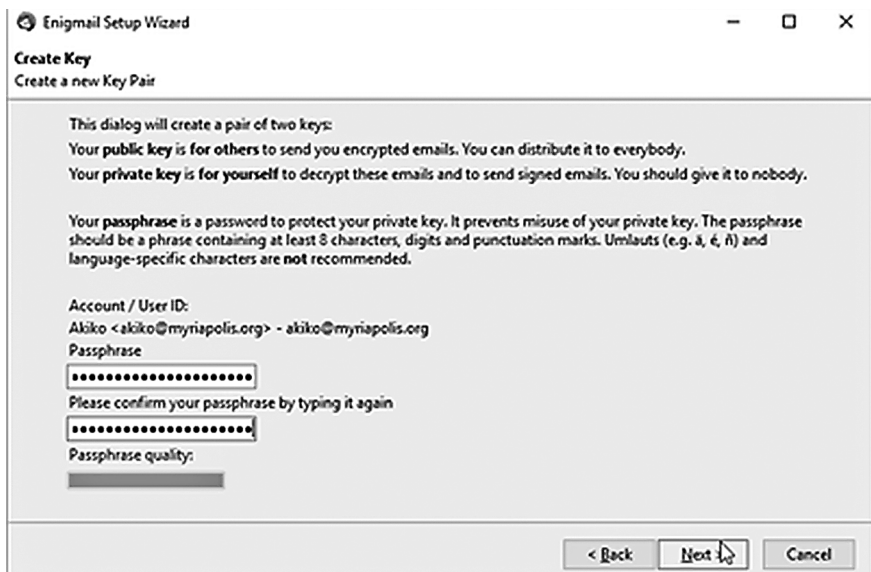
5. Безпека користування електронною поштою



Під час встановлення Enigmail також завантажить та встановить **Gnu Privacy Guard** (відому також як GPG). Це компонент, який власне здійснює саме шифрування. На більшості систем Gnu/Linux GPG вже встановлено.

При першому запуску Thunderbird з установленим Enigmail відкриється вікно налаштування Enigmail. Вам буде запропоновано створити персональний ключ.

Придумайте складний пароль для захисту свого закритого ключа: до 4 слів, які ви можете запам'ятати, інші ж не зможуть вгадати.



Розіслати ключ можна так: у віконці «Key management» треба вибрати ваш ключ і натиснути «Send Public Keys by Email».

У листі зазначте про те, що дбаєте про безпеку персональних даних.

Щоб імпортувати чийсь ключ, який прийшов вам на скриньку, достатньо клацнути правою кнопкою миші на приєднаний до листа файл і вибрати «Import OpenPGP Key».

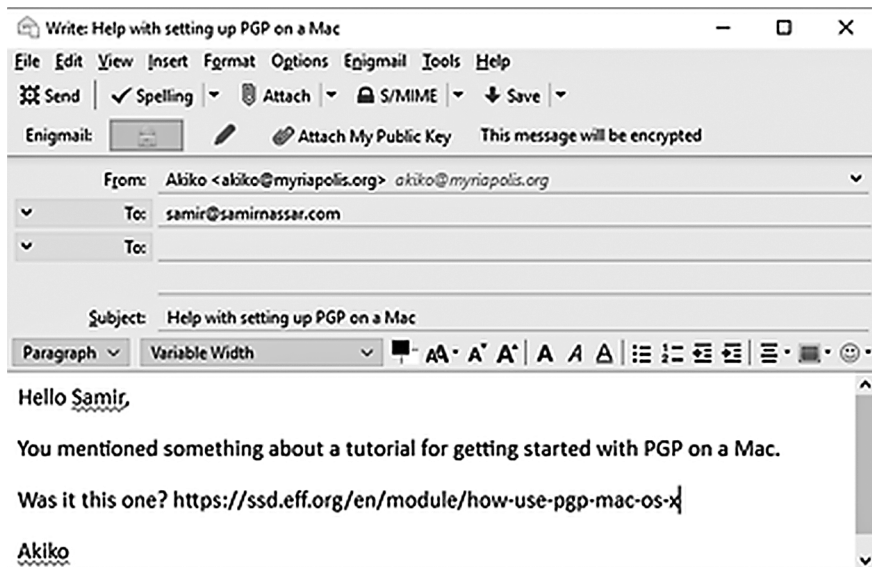


У вікні створення повідомлення з'явиться рядок кнопок «Enigmail», де можна вмикати /вимикати шифрування. Якщо ви пишете листа до когось, чий відкритий ключ у вас є, шифрування листа буде увімкнено автоматично. (Див. рисунок на с. 115.)

OpenPGP дає можливість додати до листа цифровий підпис. Підпис генерується на основі змісту самого повідомлення, яке ви надсилаєте, згідно з вашим закритим ключем, доступ до якого є тільки у вас. Якщо раптом повідомлення хтось перехопив і поміняв, підпис автоматично стає недійсним. Поміняти підпис неможливо, бо закритий ключ тільки у вас. При цьому перевірити автентичність підпису можуть усі, у кого є ваш відкритий ключ.

Коли вам приходить захищене повідомлення, програма автоматично його розкодує й перевіряє, чи відповідає воно підпису відправника (якщо він є). Для розкодування потрібен пароль до вашого закритого ключа.

6. Етика електронного листування



6. ЕТИКА ЕЛЕКТРОННОГО ЛИСТУВАННЯ

- 1) Указуйте тему листа.
- 2) Висловлюйтеся коротко й за темою листа.
- 3) Не використовуйте заголовні літери для підсилення ефекту тексту: це утруднює його сприйняття.
- 4) Уживайте абзацні відступи.
- 5) Пишіть грамотно та літературною мовою.
- 6) Уникайте публічних флеймів (лист написаний спонтанно, під впливом емоцій): краще листуватися в стані зрівноваженості та спокою.
- 7) Якщо ви використовуєте різні стилі оформлення тексту (шрифт, курсив тощо), подумайте, чи ваш адресат підтримає й зрозуміє виділене.
- 8) Нагадуйте, відповідаючи, тему дискусії електронного листування. Це полегшить розуміння. Цитування виділяйте знаками < >.
- 9) Намагайтеся не поєднувати в одному листі особисте та професійне.

- 10) Перш ніж відповісти, подумайте: чи є потреба у вашій відповіді всім зі списку розсилки, чи варто відповісти організатору розсилки.
- 11) Підпис наприкінці листа має бути скромним, коротким та помірно інформативним.
- 12) У висловлюваннях будьте делікатними, намагайтеся уникати оцінних суджень, контраверсійних тем (політика, релігія, економіка, національна приналежність).
- 13) Уживайте слова ввічливості, вітайтеся й прощайтесь.
- 14) Важливо усвідомити, що не існує надійної системи електронного листування, тому важливі персональні дані краще передавати наживо.
- 15) Не перенасичуйте лист візуалізацією та смайлами.
- 16) Перш ніж надіслати листа, перечитайте своє послання. Подумайте краще. Відправлений лист не можна зупинити та повернути.
- 17) Щоб відповісти на лист, скористайтесь спеціальною кнопкою «Відповісти» — це дозволить відстежити всю попередню переписку.
- 18) Адресу одержувача краще вказувати в останню чергу — це позбавить незручної помилки, коли незакінчений лист потрапляє до адресата через випадкове натискання кнопки «Відправити».
- 19) Уникайте сарказму.
- 20) Поважайте конфіденційність інших. Не вказуйте і не надсилайте особисту електронну пошту без дозволу автора.

7. КОРИСНІ ПОРАДИ ЩОДО ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ

ФЕЙСБУК

Згідно зі statista.com, найпопулярнішою соцмережею у світі є Facebook, який у наш час налічує майже 2,5 мільярди активних користувачів на місяць.

Для особистих питань використовуйте тільки месенджер — не варто з'ясовувати



стосунки, домовлятися щодо якоїсь важливої справи в стрічці новин чи в коментарях.

Недоречно публікувати допис на стіні іншого користувача без попередньої згоди.

Не додавайте своїх друзів у групи без їхньої згоди. Краще написати допис про певну групу й дати свою обґрунтовану рекомендацію.

Запитуйте дозволу на те, щоб виставити в соціальній мережі й відзначити людину на спільній із вами фотографії.

Не варто використовувати відеодзвінок без попередньої згоди з абонентом. Спершу краще запитати в чаті про можливість відеодзвінка.

Не поширюйте інформацію сумнівного характеру чи з недостовірного джерела. Так само не варто зловживати постами, наприклад, із проханням узяти на догляд кошенят, цуценят чи пожертвувати кошти на лікування тощо.

Не варто виставляти для широкого загалу пости й дописи про ваші плани щодо відпустки, придбання дорогоцінних речей тощо.

Навчіться самі й навчіть дитину ставитися до змісту дописів критично.

Пам'ятайте про можливу небезпеку спілкування з невідомими людьми.

Принципово значущим є формування дописів і постів про дітей. Важливо керуватися принципом: соціальна мережа формує імідж кожного з нас. Ваша дитина — не виняток. Можливо, краще не квапитися та дати змогу дитині самостійно під мудрим наглядом дорослої людини сформуванню власну сторінку. А батькам краще сфокусувати увагу своїх друзів-дописувачів на своїй персоні.

Так само варто звернути увагу на таке: краще не приставати на запрошення взяти участь у сумнівному онлайн-опитуванні, віртуальній грі на кшталт «ким ти був у минулому житті», оскільки такі кроки є традиційними в маркетингових технологіях, і ваша активність призведе до появи спаму чи утворення своєрідної інформаційної кульки (одноманітна інформація, новини з однієї теми, пропозиції тощо).

Обережно слід ставитися до пропозицій узяти участь у черговому челенджі. Перш ніж пристати на подібну пропозицію, дайте відповідь на просте запитання: «З якою метою я братиму участь у цьому челенджі? Кому і навіщо потрібна від мене така інформація?»

Обережно поставтеся до слів і буквосполучень із хештегом #. Зазвичай підтримка чи залучення до таких дописів так само заведе вас в інформаційну кульку.

Дедалі більше українських дітей долучаються до мережі Facebook услід за своїми батьками, серед яких вона є дуже популярною. Аби убезпечити дитину від небажаних матеріалів у Facebook, радимо перевірити налаштування конфіденційності.

ШВИДКІ НАЛАШТУВАННЯ КОНФІДЕНЦІЙНОСТІ У ФЕЙСБУК

«Швидкі налаштування конфіденційності» доступні під знаком «↓швидка допомога» у верхньому правому куті (для браузера) / або через плитку з 3 крапками під фото профілю (для мобільної версії).

У цьому меню доступна функція «Перевірка основних налаштувань конфіденційності», яка допоможе максимально убезпечити свою сторінку.

Налаштувати безпечний перегляд вашого профілю (інформація, дописи) іншими користувачами: ↓ «Налаштування та конфіденційність» — «Конфіденційність» — «Швидкі налаштування конфіденційності» — «Перевірка основних налаштувань конфіденційності» — «Хто може бачити ваші дописи» — «Продовжити».

На першій сторінці можемо обрати, яка інформація буде доступна тільки користувачу, друзям або публічно, зокрема, ↓ «Налаштування та конфіденційність» — «Швидкі налаштування конфіденційності» — «Перевірка основних налаштувань конфіденційності» — «Хто може бачити ваші дописи» — «Продовжити» — «Рідне місто».

Обираємо доступне налаштування з правого боку — «Публічно, Друзі, Лише я». За допомогою такого ж алгоритму можливо змінити доступ до всіх розділів особистої інформації (день народження, рідне місто, робота тощо).

У розділі «Швидкі налаштування конфіденційності» Facebook ви зможете знайти для підлітків та батьків поради з безпечного користування мережею: ↓ «Налаштування та конфіденційність» — «Швидкі налаштування конфіденційності» — «Безпека» — «Пошук ресурсів для батьків» / «Допомога в боротьбі із цькуванням».

У налаштуваннях конфіденційності можна окреслити коло осіб, які можуть додавати сторінку дитини в друзі. За замовчуванням це всі користувачі Facebook, проте радимо змінити це на «Друзі друзів», аби уникнути небажаних знайомств.

Наприклад, «Налаштування та конфіденційність» — «Швидкі налаштування конфіденційності» — «Перевірка основних налаштувань конфіденційності» — «Як люди можуть знаходити вас у Facebook» — «Продовжити» — «Хто може надсилати вам запити на дружбу» — «Друзі друзів».

Якщо ви хотіли б заблокувати профіль у Facebook / небажані повідомлення, можна скористатися функцією «Блокування» у загальних «Налаштуваннях», що міститься під ↓ у верхньому правому куті: «Налаштування» — «Обмеження» — «Блокування користувачів» / «Заблокувати повідомлення».

Можна поскаржитися на коментар чи публікацію. Для цього потрібно затиснути коментар та вибрати опцію «Надіслати запит на підтримку або скаргу на коментар», указати причину у спливаючому меню. Функція «Надіслати запит на підтримку або скаргу на допис» доступна в меню, позначеному трьома крапками у верхньому правому куті публікації.

ІНСТАГРАМ

Instagram невпинно поширюється: понад 1 мільярд користувачів, ресурс розвитку бізнесу, існує просування продуктів, розширена аналітика.

Ваш контент буде публікуватися за потрібним графіком, а штучний інтелект — ставити за вас лайки.

Понад половина користувачів Instagram у всьому світі має вік до 34 років. Додаток для обміну фотографіями посів друге місце за популярністю серед підлітків у США,



поступившись тільки Snapchat. Традиційно половина всіх охоплених соціальною мережею підлітків перевіряють свої сторінки щогодини або частіше.

Більшістю соціальних мереж можна користуватися з 13-ти років. Тому значна частина матеріалів, які є у вільному доступі на цих платформах, не призначені для перегляду дітьми до 13-ти років.

Налаштування за замовчуванням роблять профілі користувачів відкритими та всі їхні публікації доступними, у тому числі за запитом у пошукових системах, на кшталт Google.

Переважний контент цієї соціальної мережі — зображення та фотографії.

Небажано виставляти на огляд друзям неякісні фото чи відео. Також не варто часто виставляти візуальний контент без підпису.

Краще, якщо ваша стрічка формуватиметься із цікавих дописувачів, а не випадкових людей. Розбавляйте потік нескінченних селфі інтелектуальними постами.

Дитина має знати, що не варто публікувати особисту інформацію на власних вебсайтах, онлайн-ових щоденниках (блогах).

ЯК ЗРОБИТИ АКАУНТ ДИТИНИ ПРИВАТНИМ

Натисніть три крапки або три смуги у верхньому правому куті сторінки профілю, оберіть «Налаштування» — «Конфіденційність» — «Конфіденційність облікового запису» — «Приватний обліковий запис».

Щоб знизити ризики фейкових контактів, періодично переглядайте списки своїх друзів, видаляйте сумнівних чи повторюваних дописувачів. Для цього у своєму акаунті оберіть «Читачі» згори екрану профілю, оберіть тих, кого хочете видалити, натиснувши видалити праворуч від їхнього профілю. Вони не отримають сповіщень про те, що більше не слідкують за вами, просто більше не бачитимуть ваші публікації.

Якщо ваша дитина більше не хоче стежити за чийось акаунтом, оберіть зверху екрана «Відстежуються», оберіть профіль людини, за якою більше не хочете стежити, натисніть на плитку «Відстежується» та прослідкуйте, аби вона змінилась на «Стежити».

Захиститися від некоректних коментарів можна в такий спосіб: у правому верхньому куті натисніть три крапки або три смуги — це меню вашої сторінки, прогортайте меню, що відкрилось, нижче, оберіть «Налаштування» — «Сповіщення» — «Дописи, розповіді й коментарі» та перевірте, аби профіль міг отримувати коментарі тільки від «Людей, за якими я стежу».

Реагування на образливі коментарі або спам: натисніть на коментар або прогорніть його вліво (залежно від операційної системи), натисніть на значок знаку оклику, що з'явиться; оберіть «Поскаржитися на коментар» та причину, з якої ви це робите. Також можна видалити коментар, натиснувши «кошик».

Автоматично сховати образливі коментарі або заблокувати коментарі від небажаних осіб можна так:

«Налаштування» — «Конфіденційність» — «Коментарі» — «Сховати образливі коментарі»;

«Налаштування» — «Конфіденційність» — «Коментарі» — «Блокувати коментарі від».

Переконайтеся, аби налаштування дитини дозволяли тільки її підписникам реагувати на сторіс: «Налаштування» — «Конфіденційність» — «Розповідь» — «Ваші читачі».

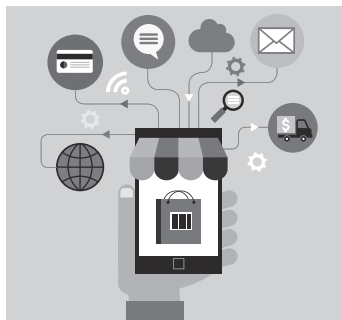
БЛОКУВАННЯ КОРИСТУВАЧІВ ТА ЗВІТУВАННЯ ПРО НЕНАЛЕЖНИЙ КОНТЕНТ

Перебуваючи на сторінці користувача, який публікує неприйнятний контент, натисніть три крапки у верхньому правому куті та оберіть відповідну функцію в меню: «Обмежити», «Блокувати» або «Поскаржитися».

8. ІНТЕРНЕТ-МАРКЕТИНГ

Інтернет-маркетинг — це дія, спрямована на продаж товарів та послуг в інтернеті.

Основна мета інтернет-маркетингу — перетворити відвідувачів сайтів на покупців та збільшити прибуток.



Переваги інтернет-маркетингу:

- інтерактивність: в інтернеті можна напряду взаємодіяти з аудиторією, підтримувати зв'язок із клієнтами та контролювати ситуацію;
- таргетування: це механізм, який дозволяє з усієї аудиторії виділяти лише цільову аудиторію та показувати рекламу лише їй;
- вебаналітика: допомагає розуміти, які дії є максимально ефективними та залучати на сайт більше покупців, які потім конвертувалися в покупки.

Соціальні мережі насичені рекламними матеріалами. Закон України «Про рекламу» (див.: <https://zakon.rada.gov.ua/laws/show/270/96-вр#Text>) містить вимоги до маркетингу, до якого долучаються неповнолітні. Однак дія цього Закону не завжди регулює соціальну мережу. Тому слід дотримуватися порад:

- формуйте спільний із дитиною досвід мережових покупок;
- учіться разом аналізувати рекламу й рекламні кроки узгоджувати із системою ваших потреб;
- не долучайтеся до шопінгу з недобросовісними постачальниками. Зазвичай недобросовісні постачальники нехтують авторським правом, не дають чіткого алгоритму зворотного зв'язку;
- навчіть дитину бути обережною та критично ставитися до пропозицій узяти участь в інтернет-змаганнях, голосуваннях тощо. Часто в такий спосіб людина стає вимушеним покупцем певного виду товарів;
- контакти з будь-якими службами, за які треба сплатити, можливі тільки за умови узгодження своїх дій із дорослими;
- установіть на мобільному телефоні дитини необхідне блокування, ліміт витрат на розмови та меседж;
- краще створити сімейну адресу електронної пошти, яку всі члени родини можуть використовувати в разі потреби здійснити онлайн-покупку.

На багатьох вебсайтах користувачів просять зареєструватися або в інший спосіб надати персональну інформацію

9. Рекомендації щодо організації роботи за комп'ютером без шкоди для здоров'я

задня права отримати якусь винагороду (доступ до послуги, участь у лотереї, безкоштовні продукти тощо), узяти участь у групі спілкування. Комерційні компанії прагнуть отримати законним шляхом контактну чи персональну інформацію про дітей та молодь для більш точних маркетингових досліджень.

Навчіть дітей виявляти обережність у схожих ситуаціях, передусім керуватися міркуваннями безпеки, а не легкого збагачення.

9. РЕКОМЕНДАЦІЇ ДЛЯ УЧАСНИКІВ ОСВІТЬОГО ПРОЦЕСУ ЩОДО ОРГАНІЗАЦІЇ РОБОТИ ЗА КОМП'ЮТЕРОМ БЕЗ ШКОДИ ДЛЯ ЗДОРОВ'Я

Гігієнічні вимоги, нормативи чинників, що створюються при експлуатації персональних комп'ютерів у навчально-виховному процесі встановлюють Державні санітарні правила й норми «Влаштування і обладнання кабінетів комп'ютерної техніки в навчальних закладах та режим праці учнів на персональних комп'ютерах».

Щоб запобігти перевтомі, потрібно:

- обмежити тривалість роботи учня за комп'ютером;
- робити гімнастику очей;
- правильно облаштувати робоче місце дитини;
- використовувати якісні програми відповідно до віку дитини.

Екран монітора має бути розташований на відстані 400–800 мм від очей користувача з урахуванням розмірів алфавітно-цифрових знаків і символів.

Безперервна робота перед екраном комп'ютера повинна тривати не більше:

- для учнів 10–11 класів на першій годині занять — 30 хвилин, на другій годині занять — 20 хвилин;
- для учнів 8–9 класів — 20–25 хвилин;
- для учнів 6–7 класів — до 20 хвилин;
- для учнів 2–5 класів — 15 хвилин.

Науковці Оксфордського університету вирахували, що підлітки можуть проводити за екранами по 257 хвилин на

добу (4 години 28 хвилин). Цього часу вистачає для розвитку соціальних зв'язків і навичок та виконання різних завдань.

ПРАВИЛА ПІД ЧАС РОБОТИ ЗА КОМП'ЮТЕРОМ

- Тримайте поставу.
- За комп'ютером сидіть рівно та слідкуйте, аби спина не прогиналася. Варто обирати якісне робоче крісло.
- Провітрюйте кімнату.
- Чистіть монітор за допомогою мікрофібри та спеціальних спреїв чи серветок.
- Монітор необхідно встановлювати на рівні 70–80 см від вашого обличчя, і нижче рівня очей.
- Моргайте кожні 5 секунд, якщо відчули, що очі перенапружені. Це масажує очі та сприяє зволоженню рогівки.
- Для «наведення різкості» в очах підійдіть до вікна і сфокусуйте погляд спочатку на недалеких об'єктах, потім подивіться удалечінь. Такі вправи допоможуть очам відпочити та відновитися.
- Відпочивайте чи змінюйте вид діяльності кожні 30–40 хвилин.
- Робіть гімнастику для очей чи для тіла.

ВПРАВИ ДЛЯ ЗНЯТТЯ ВТОМИ ОЧЕЙ НА 5 ХВИЛИН¹

- 1) Розітріть долоні, щоб у них з'явилося відчуття тепла, складіть їх навхрест, прикладіть до повік, передаючи таким чином енергію їх тепла до очей. Затримайтеся в такому положенні на 30–40 секунд. Після закрийте очі й повільно натискайте на повіки кінчиками пальців по 20 разів.
- 2) Закрийте очі, зробіть по 10 обертальних рухів очними яблуками за годинниковою стрілкою і проти неї. Після цього заплющіть очі, відкрийте очі. Зробіть 5 повторень.

¹ Співак О. Вправи для очей від втоми після роботи з комп'ютером. [Електронний ресурс]. — Режим доступу : <https://fitness.org.ua/krashi-vprava-dlia-ochei-vid-vtomi-pislia-roboti-z-komputer/>.

9. Рекомендації щодо організації роботи за комп'ютером без шкоди для здоров'я

- 3) Зробіть кілька легких постукуючих рухів пальцями двох рук по голові, почавши із чола й поступово перейшовши до потилиці.
- 4) Мигніть очима 2 рази, сильно й різко примружтеся й різко відкрийте очі. Зробіть 10 разів.
- 5) Сильно розітріть долоні, щоб відчути теплоту, а після м'яко п'ять разів натисніть на очні яблука.

Ці вправи рекомендується виконувати при яскравому освітленні чи на свіжому повітрі.

ВПРАВИ ДЛЯ ОЧЕЙ ПІСЛЯ РОБОТИ ЗА КОМП'ЮТЕРОМ НА 10 ХВИЛИН

Повторюйте кожну вправу 2–4 рази.

- 1) Тримавши голову нерухомо, по черзі спрямовуйте погляд вліво — вправо, потім угору — униз.
- 2) Переміщайте очі по діагоналі, хрест-навхрест спочатку вгору, потім униз.
- 3) Вправа «косоокість». Очима подивіться на кінчик носа.
- 4) Праву руку підніміть до рівня плеча вгору, після максимально перемістіть її вліво, долоня при цьому ніби окреслює півколо. Очима весь час слідкуйте за долонею. Те саме повторіть з іншою рукою.
- 5) На віконному склі поставте позначку на рівні очей або приклейте аркуш невеликого розміру. Відійдіть від нього на відстань 1 метр. По черзі дивіться очима то на аркуш/позначку, то крізь скло вдалину.

Зверніть увагу: відмінно працює для тренування очей ігри в теніс, волейбол, бадмінтон та інші, які пов'язані зі зміною положення предмета. Очі фокусуються на м'ячі або вола-ні, який постійно рухається, і це чудово тренує очні м'язи.

ШВИДКА РУХАНКА

- 1) Кожні дві години в процесі роботи за комп'ютером на 5–10 хвилин спрямовуйте погляд удалечинь.
- 2) Закрийте очі на 1–2 хвилини, постарайтеся максимально розслабитися.
- 3) Виконайте 4–5 вправ для розслаблення м'язів тіла.

Дітям віком 12–14 років рекомендується робити руханки кожні 45 хвилин, віком 15–17 років — щогодини з перервою не менше 15 хвилин.

ВПРАВИ BATES

(за методикою американського офтальмолога Вільяма Бейтса)

- 1) Сидячи за столом, зіпріться ліктями об стільницю.
- 2) Струсніть руками, розслабте пальці й зап'ястя.
- 3) Сильно потріть долоні одну об одну, щоб вони зігрілися.
- 4) Упираючись головою в основу долонь, закрийте пальцями очі так, щоб пальці перетиналися на лобі. Руки при цьому мають бути розслаблені. Сильно тиснути на очі не треба.
- 5) Потрібно постаратися відчути темряву. Вона сприяє синтезу родопсину у світлочутливій сітківці органів зору. Якщо вдалося сконцентруватися на темряві, значить, очі розслабилися добре. Суть вправи в тому, що саме в темряві очі можуть отримати максимально глибоке розслаблення, що дуже важливо для їх відновлення.
- 6) Тепер уявіть, що погляд спрямований на щось темне, наприклад, нічне небо або воду, і воно наповнює все поле зору й передається в головний мозок по зоровому каналу. Через якийсь час перед очима знову почнуть з'являтися образи — чинити опір цьому не треба, очі поступово повернуться в реальність. Очі мають бути закритими. Приберіть руки з очей, ви відчуєте зміну температури і яскравості. Сильно примружтеся, потім відкрийте очі. Ці вправи для очей від втоми після роботи за комп'ютером рекомендується виконувати щодня.

КОМП'ЮТЕРНІ ПРОГРАМИ ДЛЯ ОЧЕЙ

Eyes Relax — передбачає вправи для очей, які самі з'являються на екрані через певний час, заданий вами, перериваючи роботу. Потрібно просто дивитися на зображення, які сприяють відпочинку та відновленню органів зору.

NI Glaz — безкоштовна програма, яка контролює тривалість роботи користувачем за комп'ютером. Ця програма видає повідомлення у звичайному діалоговому вікні про

необхідність відпочити чи почати роботу через попередньо задані інтервали часу. Після запуску програми з'являється значок у системному вікні з указівкою тривалості роботи й часу на відпочинок. Налаштування англійською і російською мовами. Офіційний сайт програми — www.kivlab.com.

EyeLoveU — буде через якийсь час нагадувати, що потрібно зробити перерву.

NEWBaRest — працює у фоновому режимі та із заданою періодичністю нагадує про необхідність відпочинку чи короткої перерви. Зручний та ефективний інтерфейс програми.

Orbis — програма, призначена для дослідження гостроти зору. У перекладі назва означає коло, круг. Метод передбачає використання кілець Ландольта — простого у використанні інтернаціонального опто типу. Користувач повинен визначити, з якого боку є розрив кільця. Програма має три рівні, зручна у використанні, доступна всім користувачам. Як скрінінговий метод корисна для вчасного виявлення проблем із зором. Якщо гострота нижче 1.0, варто звернутися якнайшвидше до офтальмолога.

Workrave — містить максимум установок, призначених для захисту органів зору.

EyeLeo — програма, яка працює таким чином: миле левеня пропонуватиме зробити перерву й виконати вправи для очей.

МАСАЖ ОЧЕЙ ПІД ЧАС РОБОТИ ЗА КОМП'ЮТЕРОМ

Закрийте очі, розслабтеся, подушечки вказівних пальців розташуйте на внутрішніх куточках очей. Далі, не відриваючи пальця, його кінчиком виконуйте кругові рухи то в один, то в інший бік.

Те саме виконуйте із зовнішнім куточком ока.

Виконуйте легкі постукування подушечками вказівних пальців по зімкнутих верхньому і нижньому повіках. Вони робляться ніби з описом півкола від зовнішнього кута ока до внутрішнього і навпаки.

Потім виконайте легкі натискання на очні яблука при попередньо закритих очах. Такий масаж виконується в поєднанні з гімнастикою.

МАСАЖ І ВПРАВИ ДЛЯ ШИЇ

Вони допомагають розслабитися і зняти напругу після роботи за комп'ютером.

Краще виконувати їх після водних процедур або прямо під час них. Корисні заняття в басейні, які розслаблюють м'язи. Можна також виконувати самомасаж у поєднанні з фізичними вправами для м'язів шиї. Для масажу можна використовувати спеціальні масажери.

Перед початком масажу змастіть шкіру шиї і рук кремом або звичайним вазеліном. Поєднуйте погладжування, розминання м'язів шиї руками, постукування по ній ребром долоні.

Виконуються також нахили шиї в боки, вперед і назад, повороти голови, оберти шиї по черзі в різні боки, вправи з опором.

ЗАГАЛЬНІ ПОРАДИ

Комп'ютерне місце потрібно організувати так, щоб правильно падало світло. Кращим вважається розсіяне, непряме освітлення, без відблиску на монітор.

У вашому зоровому полі не повинно бути сильного перепаду яскравості, вікна краще затінити.

Важливим є рівномірний розподіл штучного світла, тому небажано використовувати тільки настільну лампу, краще, звичайно, стаціонарне світло.

Слідкуйте за чистотою монітора комп'ютера, а також лінз окулярів, якщо їх носите. Для протирання дисплея використовуйте спеціальні серветки для оргтехніки.

Верхня частина екрана має розташовуватися нижче рівня очей, а нижня його частина має бути злегка нахилена вперед. Це допоможе зменшити навантаження на зоровий нерв, зважаючи на оптимізацію зорової осі.

Відстань від очей до екрана має бути не більше 50–60 см. Якщо ви погано бачите зображення на такій відстані, потрібно збільшити шрифт.

Працюючи в текстовому режимі, використовуйте чорне кольорове підсвічення, а тло робіть світле. Кращий варіант — біле тло, чорні літери.

Якщо ви працюєте з рукописами, то рукопис тримайте поряд із монітором. Так не буде потреби робити різкі рухи.

Намагайтеся додати в раціон продукти, які зміцнюють судини сітківки ока (чорниця, чорна смородина, ожина, лохина, зелень, печінка тріски, натуральний зелений чай, заварені сушене листя і плоди глоду).

Найкорисніший продукт для підтримки здоров'я очей усіх користувачів — це терта сира морква з вершками або рослинною олією.

10. КІБЕРБУЛІНГ — ІДЕНТИФІКАЦІЯ ТА ЗАПОБІГАННЯ

Кібербулінг (англ. Cyberbullying) — умисне й повторюване заподіяння шкоди із використанням сучасних електронних технологій та засобів електронної техніки: комп'ютерів, мобільних телефонів та інших пристроїв.



Молодь використовує сучасні електронні технології (електронні пошти, формули, чати тощо) з метою переслідування, погроз, приниження однолітків. В основному інциденти виявляються в надсиланні образливих текстів іншим або поширенні принизливої інформації за допомогою смартфонів чи планшетів. Таку інформацію може бути поширено в усіх соціальних мережах, на платформах прямого ефіру, профілях або через приватні повідомлення та анонімні програми.

Характерною для кібербулінгу є систематичність, тобто шкідлива інформація поширюється не одноразово чи епізодично, а має певну систему повторень. Своєрідне «цькування» досить часто може відбуватися одночасно в реальному житті та в інтернет-мережі. Це робиться з метою залякування, приниження, пригнічення тих, кого переслідують. Інтернет-залякування залишає цифровий слід — записи, що є доказами і в подальшому допоможуть припинити

заякування. Поширеними формами прояву кібербулінгу можуть бути:

- видавання себе за іншу особу;
- відправлення непристойних повідомлень від чужого імені;
- поширення фейкової інформації;
- розміщення непристойних фотографій у соціальних мережах тощо.

Кібербулінг трапляється в різних місцях і засобах масової інформації в кіберпросторі, адже найчастіше це відбувається там, де підлітки масово спілкуються в мережі. Більшість молоді приваблюють соціальні медіа (Instagram, Snapchat, TikTok та Twitter), голосовий / текстовий чат у популярних іграх (Roblox, PUBG, Overwatch, Call of Duty Black Ops, Fortnite, God of War), обмін відео, потокове передавання та сайти спільнот (наприклад YouTube, Discord та Twitch). Підлітки також націлюються на розміщення шкідливого вмісту інформації в чужому профілі. Інші можуть погрожувати або неодноразово переслідувати через приватні повідомлення.

ПИТАННЯ, ЯКІ НАЙЧАСТІШЕ ВИНИКАЮТЬ ПРО ЗАЯКУВАННЯ В ІНТЕРНЕТ-МЕРЕЖІ

- Як зрозуміти, що мене переслідують?
- Як можна відрізнити травлю від жарту?
- Які наслідки кіберзаякування?
- Чи є покарання за травлю в інтернеті?
- Хто несе відповідальність за онлайн-безпеку?
- Які методи з попередження знущання в інтернет-мережі?
- Як зупинити кібербулінг, не відмовляючись від доступу до інтернету?
- Як допомогти своєму другу у випадку кіберзаякування?
- З ким поговорити, якщо хтось заякує мене в інтернеті?
- Я боюся розказати батькам про це. Як мені поговорити з ними?

ВІДПОВІДІ НА ПОШИРЕНІ ПИТАННЯ ВІД МІЖНАРОДНИХ ЕКСПЕРТІВ ІЗ КІБЕРЗАЛЯКУВАННЯ ТА ЗАХИСТУ ДІТЕЙ СПЕЦІАЛІСТІВ ЮНІСЕФ

Як зрозуміти, що мене переслідують?

Для розуміння переслідування в інтернет-мережі слід звернути увагу насамперед на свій психологічний та емоційний стан. Якщо виникає відчуття дискомфорту, образи, підвищеної уваги з боку широкого кола людей — це кіберзалякування.

Якщо вам погано та це не припиняється, слід негайно звернутися по допомогу. Кожен заслуговує на повагу як у реальному житті, так і в соціальних мережах. Кожна людина почувається щасливою, коли її розуміють та поважають.



Як можна відрізнити травлю від жарту?

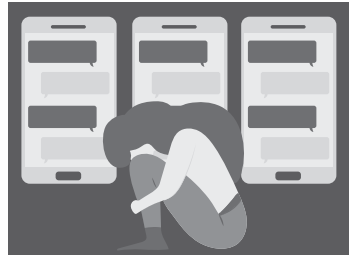
Діти, підлітки люблять жартувати та веселитися. Друзі завжди жартують між собою, іноді важко сказати, це розваги чи образи. Коли друг говорить: «Не переймайся, це просто жарт», «Не сприймай це серйозно» або «Я просто шуткую», здається, немає приводу для образ. Але якщо ви почуваетесь ображеним, пригнобленим, коли з вас сміються інші люди, коли на прохання припинити не реагують, значить жарти зайшли занадто далеко, і це є знущанням. Такі дії можуть відбуватися як у реальному житті, так і в інтернет-мережі. Де б це не було, якщо це вам не подобається, ви не маєте це терпіти. Звертайтеся по допомогу!



Які наслідки кіберзалякування?

Звичайно погрози та переслідування (кіберзалякування) мають для людини будь-якого віку негативні наслідки. Коли знущання відбуваються в інтернеті, може здаватися,

що на вас нападають усюди, навіть у вашому власному будинку. Узагалі будь-які знущання можуть мати серйозні фізичні та психологічні наслідки, зокрема для дитини. Цькування спричиняє страх, депресію, проблеми з поведінкою тощо.



Кіберзалякування може мати руйнівні наслідки. На відміну від традиційних знущань, кіберзалякування може відбуватися в будь-який час вдень і вночі та здійснюватись анонімними особами. Через це кібербулінг більш жорстокий та безжалісний.

Кіберзалякування є дуже серйозним фактором стресу в житті дитини. Оскільки кіберзалякування відбувається в кіберпросторі, онлайн-знущання здається безкінечним. Діти почуваються беззахисними та пригніченими, намагаючись усамітнитися.

Якщо неприємні пости або тексти передаються великій кількості людей, це викликає сильне почуття приниження.

Коли відбувається кіберзалякування, батьки можуть забороняти підлітку користуватися комп'ютером і телефоном. А для багатьох дітей використання гаджетів є одним із важливих способів спілкування з однолітками та друзями. Отже, обмеження дитини в користуванні засобами зв'язку означає припинення її спілкування зі своїм світом, що викликає ізоляваність.

Багато хто з жертв кіберзалякування обурені ситуацією, яка з ними відбувається. Гнів є найбільш частою реакцією на кіберзалякування, що спричиняє розлади поведінки та занепокоєння. Деякі, ставши жертвами, можуть планувати помсту та брати участь у покаранні.

Жертви кіберзалякування часто не можуть почуватися в безпеці. Вони вважають себе вразливими та безсилими. Жертві може здаватися, що кіберзалякування скрізь, що виходу немає. Крім того, оскільки хулігани можуть залишатися анонімними, це усвідомлення лише посилює відчуття

страху. Ефект може тривати довго і по-різному впливати на людину, зокрема, спричиняти:

- відчуття смутку, збентеженості, злості, пригніченості, гніву та розчарування;
- почуття сорому та втрати інтересу до улюблених речей;
- втому (безсоння) або такі симптоми, як біль у животі й головний біль.

Крім того, дослідження доводять, що кібербулінг впливає на самооцінку людини, спричиняє депресію, тривогу, проблеми в сім'ї, академічні труднощі, правопорушення, шкільне насильство тощо. Відчуття, що над ними сміються або ображають, може перешкодити людям висловитися або спробувати вирішити проблему. У крайніх випадках кіберзалякування може навіть призвести до суїцидальних думок та спроб самогубства. Інтернет-цькування може по-різному впливати на дитину, але це можна подолати, повернути впевненість у собі та відновити здоров'я.

Чи є покарання за цькування в інтернеті?

У більшості закладів загальної середньої освіти досить серйозно ставляться до знущань та вживають відповідних заходів щодо протидії їм. Якщо дитина зазнає кібербулінгу з боку інших учнів, обов'язково треба повідомити про це керівництво школи!

Люди, які стали жертвами будь-яких форм насильства, включаючи знущання та кіберзалякування, мають право на правовий захист і на притягнення винних до відповідальності. Законодавство щодо відповідальності за залякування, особливо кіберзалякування, відносно нове та існує не в кожній країні. Тому більшість держав покладаються на інші відповідні закони, що визначають відповідальність, наприклад за переслідування, кіберхуліганство.

У країнах, де діють спеціальні закони про кібербулінг, поведінка в інтернеті, що навмисно викликає серйозні емоційні розлади, розглядається як злочинна діяльність.



За вчинення кібербулінгу до кривдника може застосовуватися цивільна адміністративна або кримінальна відповідальність.

Однак важливо пам'ятати, що покарання не завжди є найбільш ефективним способом змінити поведінку хуліганів. Краще зосередитися на усуненні шкоди. Наприклад, у Facebook є набір Стандартів спільноти, в Instagram є Принципи спільноти, яких мають дотримуватися всі співтовариства. Якщо виявляється контент, що порушує ці правила, наприклад, у разі залякування або переслідування, компанії Facebook та Instagram видаляють його. У разі помилкового видалення контенту або акаунта можна подати апеляцію до довідкового центру Facebook / Instagram.

Щодо Twitter, тут діють суворі правила для того, щоб усі люди вільно й безпечно могли брати участь у публічних обговореннях. Ці правила спеціально охоплюють ряд напрямів, включаючи такі теми:

- насильство;
- сексуальна експлуатація дітей;
- зловживання / домагання;
- агресивна поведінка;
- самогубство або фізичні ушкодження тощо.

У рамках цих правил уживають різних примусових заходів у разі порушення контенту, вони можуть стосуватися певного фрагмента контенту (наприклад, окремого твіту або особистого повідомлення), а також конкретного облікового запису.

Хто несе відповідальність за онлайн-безпеку?

Інтернет-компанії дедалі частіше звертають увагу на проблему онлайн-знущань. Більшість із них запроваджують механізми вирішення цієї проблеми і краще захищають своїх користувачів за допомогою нових інструментів

і способів повідомлення про зловживання в інтернеті. Багато молодих людей щодня стикаються з кіберзалякуванням та крайніми формами зловживань в інтернеті.



Технологічні компанії несуть відповідальність за захист своїх користувачів, особливо дітей та молоді. Вони мають бути залучені до відповідальності в разі невиконання своїх обов'язків.

Як зупинити кібербулінг, не відмовляючись від доступу до інтернету?

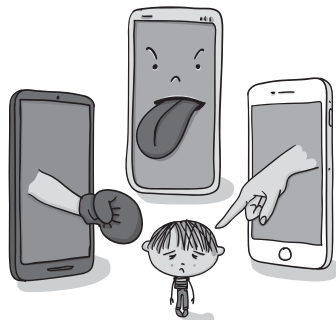
Всесвітня мережа інтернет має безліч переваг. Однак, як і багато інших речей у житті, це пов'язане з ризиком, від якого необхідно захиститися. Якщо ви зіткнулися з кібербулінгом, ви можете видалити певні програми або деякий час залишатися в автономному режимі, щоб дати собі час на відновлення. Але вихід з інтернету — це не довгострокове рішення. Ви не зробили нічого поганого, так чому ж ви повинні бути в невідгідному становищі? Це може навіть послати кривдникам неправильний сигнал, заохочуючи їх до негідної поведінки.

Усі прагнуть припинення кібербулінгу, а це важлива причина поширення інформації про кіберзалякування. Слід думати про те, що ми розповідаємо або говоримо, що може зашкодити іншим. Потрібно залишатися добрішими один до одного в інтернеті й у реальному житті. Все залежить від нас!



Які є методи з попередження знущання в інтернет-мережі?

- Подумайте двічі, перш ніж публікувати або ділитися чимось в інтернеті, оскільки це може залишитися в мережі назавжди, а згодом може бути використано вам на шкоду;
- не повідомляйте особисті дані (адресу, номер телефону, школу);
- використовуйте налаштування конфіденційності ваших улюблених програм для соціальних мереж;



- вирішуйте, хто може бачити ваш профіль, надсилати приватні повідомлення, коментувати ваші публікації;
- скаржтеся на образливі коментарі, повідомлення та фотографії й вимагайте їх негайного видалення;
- використовуйте функцію заблокування людей, щоб вони не могли бачити ваш профіль або зв'язуватися з вами;
- видаляйте небажаних друзів;
- обирайте функцію, щоб коментарі певних людей відображалися тільки для них;
- вчасно видаляйте повідомлення у своєму профілі або приховуйте їх від певних людей тощо.

Як допомогти своєму другу у випадку кіберзалякування?

Будь-хто може стати жертвою кібербулінгу. Якщо ви бачите, що це відбувається з кимось із ваших знайомих, ваші дії можуть бути такими:

- спробуйте запропонувати підтримку, оскільки важливо послухати друга та дати йому (їй) зрозуміти, що не потрібно нічого офіційно повідомляти, але дуже важливо поговорити з кимось, хто може допомогти;
- пам'ятайте про те, що ваш друг може відчувати себе безпорадним, тому будьте добрішими, гуманними, надійними;
- допоможіть другу продумати, що він (вона) може сказати і кому;
- весь час нагадуйте, що ви поруч та хочете допомогти;
- допоможіть знайти дорослу людину, якій ви довіряєте, яка допоможе впоратися із ситуацією;
- пам'ятайте, що в певних ситуаціях наслідки кіберзалякування можуть бути небезпечними для життя;
- пам'ятайте, що бездіяльність може викликати в людини відчуття, що все проти неї;
- знущання й домагання мають суто особистий характер, тому в багатьох випадках потрібно, щоб хтось повідомив про цю поведінку;



- повідомити своєму другові про інструмент в Instagram під назвою Restrict, за допомогою якого можна непомітно захистити свій обліковий запис, не блокуючи будь-кого, що може здатися суворим для деяких людей.

З ким поговорити, якщо хтось залякує мене в інтернеті?

Якщо ви вважаєте, що над вами знущаються:

- насамперед потрібно звернутися по допомогу, наприклад, до ваших батьків, близького члена сім'ї або іншого дорослого, якому ви довіряєте;
- у школі ви можете звернутися до вчителя, директора, психолога, спортивного тренера тощо;
- якщо вам незручно розмовляти зі знайомим, пошукайте телефон довіри, щоб поговорити з професійним консультантом.



Якщо знущання відбуваються в соціальній мережі, подумайте про те, щоб заблокувати хулігана й офіційно повідомити про його поведінку в самій мережі, оскільки ці компанії зобов'язані забезпечувати безпеку своїх користувачів. Корисно зібрати докази у вигляді текстових повідомлень або скрінів екрану з публікаціями в соціальних мережах, щоб показати те, що відбувається.

Щоб почуватися в безпеці, потрібно припинити знущання, повідомивши про нього поліції (102).

Пам'ятайте, у вас є право на безпеку!

Я боюся розказати батькам про це. Як мені поговорити з ними?

Якщо ви зіткнулися з кіберзалякуванням, то першим найважливішим кроком має бути розмова з вашими батьками. Розмовляти з батьками не всім легко. Але є деякі речі, які допоможуть цій розмові:



- виберіть такий час для розмови, коли увага батьків зосереджена на вас;
- поясніть, наскільки серйозною є для вас проблема;
- пам'ятайте, що батьки можуть бути не так добре обізнані з технологіями, як ви, тому допоможіть їм зрозуміти, що саме відбувається.

Батьки обов'язково допоможуть і знайдуть вихід із ситуації!

Facebook та Instagram постійно (24/7 по всьому світу на більш ніж 50 мовах) перевіряє анонімні звіти, публікації, коментарі, чим допомагає впоратися з проблемами кібербулінгу



ІДЕНТИФІКАЦІЯ ТА ПРОЯВИ КІБЕРБУЛІНГУ

- Приниження, ставлення людини в незручне становище.
- Погрози вбивства.
- Погрози заподіяння фізичної шкоди іншій людині.
- Публікація або повідомлення непристойного змісту.
- Сексуальне домагання.
- Видавання себе за іншу людину.
- Відправлення фото та відео без дозволу.
- Переслідування в цифровому вигляді.
- Розміщення, перегляд або запит дитячої порнографії.
- Злочини за ознакою раси, статі, сексуальної орієнтації, релігії.
- Зйомка або публікація фото не конфіденційно.
- Використання лайливих та образливих слів.

ПОРАДИ БАТЬКАМ ІЗ ПОПЕРЕДЖЕННЯ КІБЕРБУЛІНГУ

Хоча не існує надійного способу запобігти кіберзалякуванню вашої дитини, але є речі, які ви можете зробити разом, щоб знизити ймовірність цього. Це включає в себе певні заходи безпеки, а також постійні розмови про кіберзалякування. Вам необхідно обговорити, що це таке, які є ризики, пов'язані з кіберзалякуванням, та способи його

ескалації. Важливо поговорити зі своїми дітьми про те, як безпечно й відповідально використовувати соціальні мережі, а також про те, що їм слід робити, якщо над ними знуються в інтернеті.

Пам'ятайте, проблема не в технологіях та інтернеті. Справжня проблема — це люди, які використовують його на шкоду іншим. Постарайтеся не обмежувати доступ вашої дитини до онлайн-інструментів. Замість цього навчіть їх користуватися цими інструментами безпечно й відповідально:

- захистіть облікові записи та пристрої;
- використовуйте інструменти та налаштування конфіденційності;
- відразу сповістіть про кіберзалякування;
- отримуйте дозвіл перед тим, як поділитися фотографією;
- зберігайте в таємниці особисті дані (адресу пошти, номер телефону);
- управляйте передачею місця знаходження;
- навчіть дітей думати перед розміщенням публікації;
- проведіть аудит соціальних мереж;
- не відповідайте кібер-хуліганам та не контактуйте.

ЧОМУ КІБЕРБУЛІНГ Є ОСНОВНОЮ ПРОБЛЕМОЮ

Деякі підлітки можуть просто не усвідомлювати серйозності шкоди, якої вони завдають іншим. Вони чудово володіють технологічними ноу-хау, оскільки інструменти онлайн-спілкування стали повсякденною та важливою частиною життя молоді, і не дивно, що деякі використовують пристрої, програми та платформи, щоб загрожувати іншим.

Більшість дорослих не замислюється або просто не має часу для того, щоб відстежити, як підлітки використовують інтернет. У результаті дії агресора можуть бути не помічені та не контрольовані. На жаль, трапляється так, що коли ідентифікують тих, хто залякує, більшість дорослих не спроможні адекватно реагувати на цю ситуацію.

Фактом є те, що підлітки постійно зазнають кібербулінгу. Агресор може приховати свою особу, використовуючи анонімні акаунти та вигадані прізвища. Кібербулінг може стати вірусним, коли велика кількість людей (у школі, по

сусідству, у місті, у всьому світі) може брати участь у віктимізації цілодобово.

Проблемою запобігання кібербулінгу є те, що дорослі повільно реагують на нього, а також багато хто вважає, що негативних наслідків для їхніх дій майже немає. Незважаючи на те, що ця проблема існує вже понад два десятиліття, деякі люди все ще не бачать шкоди. Дехто намагається знехтувати кібербулінгом, тому що є «серйозніші проблеми, про які варто турбуватися».

На сьогодні існує багато проблем, які стоять перед підлітками, батьками, учителями та правоохоронними органами, але перш за все слід визнати та усвідомити, що кібербулінг — це одна з таких проблем, яка лише погіршуватиметься, якщо її ігнорувати. Інший виклик стосується того, хто готовий узяти на себе відповідальність за реагування на невідповідне використання технологій. Батьки часто кажуть, що у них бракує знань або часу і що школа повинна детально висвітлювати це під час уроків. Педагоги часто виконують свою роль через навчальні програми, тренінги та збори, але іноді не знають, коли і як можуть вплинути на поведінку дитини в інтернеті, коли це відбувається поза школою. Щодо правоохоронних органів, вони не поспішають втручатися, якщо немає чітких доказів злочинної діяльності чи значної загрози чийсь фізичній безпеці. У результаті інциденти з кібербулінгом розглядаються дещо формально (неофіційно).

Припинення кібербулінгу можливе, цього можна досягти спільними зусиллями, взаємно узгодженим порядком дій. Насамперед потрібно створити середовище, у якому молодь почуватиметься комфортно, розмовляючи з дорослими про цю проблему, і відчуватиме впевненість, що для вирішення ситуації буде вжито серйозних заходів. Від молоді, батьків, вихователів, радників, молодіжних лідерів, правоохоронних органів, компаній у соціальних мережах та суспільства в цілому очікують цілеспрямовані та всебічні зусилля, щоб домогтися суттєвого зменшення випадків кібербулінгу й уникнення ризиків, пов'язаних із ним.

Діти мають розуміти, що дорослі будуть втручатися в ситуацію раціонально та логічно, а не погіршувати

її. Наприклад, батьки повинні пояснити важливість призначення зустрічі з адміністрацією школи (або педагогом, якому вони довіряють) для обговорення питання безпеки дитини. Вони також можуть поспілкуватися з батьком чи матір'ю кривдника та /або співпрацювати з постачальником послуг інтернету, який для розв'язання проблеми має видалити користувачів, що порушують правила. Батьки мають бути впевнені, що дитина почувається в безпеці, надавати їй безумовну підтримку, демонструючи те, що безпека дитини є найцікавішою для них, вартує їхнього часу й зусиль.

Діти мають довіряти батькам, показувати їм, які сайти та програми вони використовують, і розповідати, чому вони їм подобаються. Вони повинні розповісти батькам, як вони захищають себе в інтернеті, дозволити мамі чи татові запропонувати інші стратегії. Звернення до дорослої людини має величезне значення для покращення ситуації, оскільки діти часто відчують себе безпорадними та потребують, щоб хтось прийшов їм на допомогу. Нарешті, самі вони ніколи не повинні прямо чи опосередковано сприяти негідній поведінці, передаючи образливі повідомлення, сміючись над невідповідними жартами чи змістом, виправдовуючи вчинок для того, щоб «вписатися» в соціум. Нарешті, підлітки мають приймати відповідальні рішення щодо того, що вони надсилають чи публікують в інтернеті, усвідомлюючи, що це може побачити кожен, включаючи і їхніх батьків.

11. КРИТИЧНЕ МИСЛЕННЯ ДЛЯ ОЦІНЮВАННЯ ІНФОРМАЦІЇ

Критичне мислення є своєрідним продуктом когнітивної діяльності. По суті — це вміння активно, творчо, індивідуально сприймати інформацію, оптимально застосовувати потрібний вид розумової діяльності, різнобічно аналізувати інформацію, мати особисту незалежну думку та вміти коректно її відстоювати, уміти застосовувати здобуті знання на практиці.

Навчити людину мислити критично означає:

- навчити логічно формулювати запитання;
- зосереджувати увагу на ключових поняттях, термінах;

- робити логічні зв'язки в матеріалі, що вивчається, із вивченим попередньо;
- правильно ставити запитання;
- знаходити рішення через використання практик критичного аналізу ситуацій, діалогу, рольових та ділових ігор, мозкового штурму.

До педагогічних умов формування критичного мислення відносять:

- включення в освітні програми цілей формування критичного мислення та змісту, що сприяє умовам розвитку дивергентності розуму;
- окрім професійних компетенцій та системи умінь і навичок, логічно й критично мислити.

Середовище, створене вчителем на уроці, має спонукати учнів до критичного мислення, самостійних розумових операцій. «Критичномисляча» особистість — поняття динамічне, тому її треба формувати й розвивати, використовуючи для цього ефективні засоби, методи та прийоми розвитку критичного мислення дитини.

ПРАКТИКИ ФОРМУВАННЯ ДОСВІДУ КРИТИЧНОГО МИСЛЕННЯ

1) «Мозкова атака» («брейншторм»).

Ця методика допомагає систематизувати знання й знаходити творчі рішення. Для застосування методики вчитель записує посередині дошки певне поняття, а учні озвучують усе, що про нього знають. За допомогою рисочок, спрямованих від слова, учитель записує висловлювання дітей. У результаті утворюється своєрідна ментальна карта, доповнювати яку можна впродовж уроку та в кінці, щоб систематизувати знання учнів.

2) «Асоціативний куц».

На відміну від мозкової атаки, де висловлені думки стосуються інформації з приводу певної теми, метод «Асоціативний куц» спонукає учнів думати вільно та відкрито стосовно певного предмета, образу, теми, включаючи почуття, емоції, ставлення. Отже, цей метод стимулює нелінійну форму мислення — асоціативне мислення.

3) Кола Венна.

Цю методику доцільно використовувати для порівняння декількох понять або предметів. Її можна зобразити за допомогою схеми: два кола, що перетинаються між собою. Кожне коло означає окреме поняття, місце перетину — це спільні властивості обох понять. За допомогою цієї діаграми можна порівнювати літературних героїв, явища природи, величини тощо.

4) «Товсті» — «тонкі» запитання.

Учитель улаштовує опитування за певною тематикою (запитання готуються заздалегідь). «Тонкі» запитання передбачають відповідь лише «так / ні» і починаються, наприклад, так: «Хто...?», «Що...?», «Чи правда, що...?». «Товсті» запитання вимагають розгорнутої відповіді — з аналізом, синтезом, порівнянням, оцінкою. Наприклад, «Дайте три пояснення, чому...?», «Поясніть, чому...?», «У чому відмінність між...?».

5) «Відкриті» запитання.

Такі запитання дають змогу учням спиратися на здобуті знання та застосовувати те, про що вони дізналися раніше. Також це дозволяє їм вирішувати завдання швидше і підвищує їхню самооцінку перед однолітками. Учнім необхідно ставити такі запитання, які пробуджують «дослідницький рефлекс»: «Чому...?», «Як...?», «А як би...?», «А якщо...?». Ці та інші питання такого типу пробуджують і розвивають в учнів цікавість, захоплення, а також нестримне бажання досліджувати цей світ.

6) Практика приймати рішення.

Оскільки значна частина навичок критичного мислення передбачає застосування знань та прийняття рішень, то вчителі можуть максимально заохочувати учнів приймати рішення, тоді діти зможуть порівнювати плюси та мінуси прийнятих рішень, вирішити, які з них найкраще працюють.

7) Кероване читання з передбаченням.

Після ознайомлення з назвою тексту та його автором перед читанням ставлять дітям запитання, які дозволяють зробити припущення, про що саме буде текст (робота в парах чи групах).

Текст розподіляється на частини. Зупинки треба роботи на найбільш цікавих місцях, створити інтригу — ситуацію очікування. Після читання кожної частини учням ставляться запитання. Пропонується зробити передбачення стосовно того, що буде далі. А після читання наступної частини це передбачення аналізується й приймається певне рішення.

8) Робота в групах змінного складу.

Групові проекти та дискусії — ще один чудовий спосіб розвивати навички критичного мислення. Таке групове навчання розширює світогляд, дає осмислення, що немає єдиного правильного способу вирішення проблеми.

9) Активне слухання.

Вислуховування різних точок зору під час дискусії дасть можливість сформулювати єдину правильну думку й водночас дозволить учням ділитися власними поглядами з іншими учасниками навчального процесу.

10) Метод «прес».

На будь-якому етапі уроку пропонувати відповісти: «Наприклад...», «Отже...», «Таким чином...»

11) Читання з позначками.

Різновид роботи з підручником. Має на меті привчити учнів до осмисленого читання тексту з аналізом. Перед початком роботи пропонується виділяти в тексті інформацію чотирьох видів і позначати відповідними символами: відома інформація, це я знав раніше (+); нова інформація (–); суперечлива інформація, я так не думав (✓); недостатня інформація, про це хотілося б довідатися більше від однокласників (?).

12) Прийом палітри ідей.

Використання життєвих ситуацій для навчання критичного мислення. Наприклад, учитель може запитати учнів, чи знають вони, чому на шкільному подвір'ї не росте сад. Такі життєві запитання допомагають школярам розглядати різні можливі ситуації та інші рішення. Це допоможе їм застосовувати здобуті знання при виникненні непередбачуваних ситуацій у житті.

13) Можливість створювати щось нове.

Учні мають дуже розвинуте уявлення. А це, у свою чергу, сприяє успішному створенню ними навчальних проектів.

Вони можуть робити власні винаходи, писати історію чи вірш, придумувати гру, співати пісню, укласти живий підручник чи усну газету, формувати власні підкасти.

14) Практика порожнього часу.

Ми інколи відволікаємось і витрачаємо час на перекладування каналів телебачення, гортання стрічки соцмереж, самозвинувачування чи сум. Це не приносить продуктивного результату, задоволення. То краще використовувати цей час для розвитку критичного мислення. Наприкінці кожного дня можна проаналізувати самозвіт:

— про що я сьогодні думав(-ла) за день?

— коли я мислив(-ла) при цьому про несуттєве, а коли, навпаки, думав(-ла) продуктивно?

15) Один день — одна проблема.

Подумай, які проблеми перед тобою зараз стоять. Відкинь ті, на які ти не можеш впливати самостійно. Потім обери одну проблему, яка тобі під силу. Вивчи її з усіх боків. З'ясуй, яка інформація тобі потрібна для вирішення проблеми. Потім збери інформацію та продумай свої подальші дії.

16) Загугли тричі.

Перший крок — перевірити дані, які тобі подали, у пошуковій системі. У цьому випадку скористайся Google. Краще користуватися інформацію з офіційних сайтів, ресурсів мас-медіа. Достовірність інформації варто відстежувати. Якщо не менше трьох джерел указують те саме, то, зазвичай, така інформація є достовірною.

17) Перевір фото.

Традиційно до новин додають світлину. Її теж можна проаналізувати. Спробуй пошук за зображеннями від Google. Для того, щоб він спрацював, іноді достатньо віддзеркалити будь-яке зображення. Якщо ж картинка знайдеться, то пошуковик видасть усю наявну про неї інформацію.

18) Не йди за більшістю.

Інколи стрічка новин заповнена подібними репостами, або всі мережеві друзі масово почали додавати до своїх аватарок рамки «Я за...». Не поспішай долучатися до масового руху. Пошукай відомості про людину чи подію, яку підтримують. Поширюй інформацію та виказуй підтримку тільки

тоді, коли є впевненість у наслідках твоєї допомоги, участі й прогнозованих результатів.

19) Не пици (за А. Макаренком).

Не давай емоціям заволодіти собою. Кожна людина бачить те, що хоче бачити: ми охоче ретранслюємо інформацію, що вписується до нашого світосприйняття. Особливо варто бути розважливим у спілкуванні через соцмережі.

КОРИСНІ ПОРАДИ

- 1) Курс «Критичне мислення для освітян» (безкоштовно) https://courses.prometheus.org.ua/courses/course-v1:CZ+CTFT101+2017_T3/about
- 2) Ведіть інтелектуальний щоденник. Систематично (наприклад, щотижня) записуйте опис емоційно значущої ситуації, реакцію на неї, її аналіз та оцінку аналізу.
- 3) Працюйте над своїми сильними сторонами. Робота над собою є найефективнішою, бо результат із тобою завжди.
- 4) Зменшуйте рівень егоцентризму — несвідомий нахил на користь себе. Спостерігайте за собою в таких ситуаціях, коли думаєте егоцентрично. Зафіксувавши такі моменти, спробуйте вдатися до саморефлексії, поставивши собі таке запитання: а що би в такій ситуації відчувала та зробила раціональна людина?
- 5) Змініть свій погляд на речі, шукайте відповіді на запитання: «Для чого мені ця ситуація?», «Чому мене це дратує/засмучує тощо...». Знаходьте альтернативу психоемоційній стабільності в собі, а не зовні.
- 6) Працюйте зі своїми емоціями. Якщо ви відчуваєте негативні емоції, спитайте себе: які думки привели мене до цього? Як інакше я можу подумати про те, що мене так турбує? Якщо ви знайдете відповіді на ці запитання, ваші емоції неодмінно змінюватимуться.
- 7) Проаналізуйте вплив групи на ваше життя. Періодично запитуйте себе: як на вас впливає той чи інший колектив; якої поведінки від вас очікують; що забороняють робити? Часто групові норми можуть впливати на нас на несвідомому рівні, у результаті

чого ми можемо забороняти собі думати чи вчиняти певні речі.

- 8) Сповільніть темп. Ефективно викликати відповідати того, хто першим підніме руку. Так і урок не втрачає темпу, і можна встигнути розказати більше. Але якщо ви почекаєте 5–10 секунд після запитання, то, імовірно, помітите, що кількість учнів, готових відповідати, суттєво збільшиться. Додатково це спосіб розказати, що перша думка, яка виникає в голові після запитання, не завжди хороша, і що може потрібно ще подумати, аби зібратися. Аби уникнути недоречної паузи, можете сказати таке: «У вас є 10 секунд, щоб подумати, перш ніж відповідати». Або: «Я хочу побачити 10 учнів, що бажають відповідати, перш ніж когось викличу».
- 9) Придумайте запитання дня (уроку). Зверніть увагу на це запитання на першому уроці. Згадайте про це запитання в змісті хоча б одного уроку. Наприкінці навчального дня підбийте підсумок: поговоріть з учнями, чи змінилась їхня думка упродовж дня на це запитання?
- 10) Створіть коробку відповідей. Напишіть на дошці певне запитання (типу: «Які способи для вирішення проблеми ви бачите?»). Роздайте учням аркуші та попросіть написати відповіді. На виконання завдання виділіть дві хвилини. По завершенню пройдіть по класу та попросіть учнів скласти аркуші з відповідями в коробку. Перемішайте та діставайте їх по черзі, читаючи відповіді. Обговоріть результат, проаналізуйте позиції. Також це гарний варіант перевірки домашнього завдання. Поставте питання за темою попереднього уроку, дочекайтеся відповіді. Створіть систему бонусів усім, хто надав аргументовані та правильні відповіді.
- 11) Попросіть зайняти позицію однієї зі сторін. Прочитайте завдання, у якому було б дві протилежні думки: «Згодні ви з автором чи ні? Обґрунтуйте». Якщо є можливість, дозвольте дітям піднятися зі своїх місць та стати поряд з однодумцем. Фактично, клас буде розділено на дві частини. Спитайте, чому кожен із них обрав саме

таку сторону. Якщо хтось захоче змінити свою точку зору в процесі обговорення, він зможе перейти на іншу сторону.

- 12) Спитайте «Чому?». Коли ви стикаєтеся з проблемою в класі, можете допомогти вирішити її. Використовуйте принцип 5 запитань. Ідея в тому, щоб дійти до суті проблеми, яка виникла. Коли буде поставлене останнє питання, буде надана остаточна відповідь, зроблені висновки. Такий підхід можна використати й для вирішення шкільних конфліктів.
- 13) Використовуйте метод «Автостоп». На будь-якому предметі можна практикувати метод розвитку творчого мислення. Змодельуйте ситуацію словами чи візуально. Викладіть це на папері, наче стопкадр на екрані. Закріпіть папір на дошці. Допишіть на дошці кілька фраз, які б різнобічно висвітлювали ситуацію. Попросіть пояснити, як кожна з фраз пов'язана із зображенням на папері. Хваліть учнів, якщо вони починають взаємодіяти між собою.
- 14) Думки навиворіт. Корисний спосіб зосередитися на позитивному в складних ситуаціях — стратегія «Шиворіт-навиворіт». Якщо учень забув принести домашнє завдання, запитайте: «Що може із цього вийти? Що трапиться?». Попросіть дати кілька небуденних відповідей із натяком на позитивне мислення, наприклад: «Я подолаю звичайну вечірню рутину, зібравши портфель увечері, а не за п'ять хвилин до виходу до школи».
- 15) Проведіть сеанс запитань та відповідей. Ставте різні запитання один на один та групам, зверніть увагу, чого уникають та чому віддають перевагу учні. Фіксуйте це, щоб зрозуміти, чи досягаєте ви прогресу в бажанні навчити дитину критично мислити, а не відповідати, не думаючи з бажанням «аби все це швидше закінчилось».
- 16) Практика відповідати на запитання запитанням. Коли дитина питає, висуває гіпотези, шукає причини, вона мислить. На запитання «Чому?» відповідайте дитині запитанням «Як ти думаєш, чому?».

- 17) Відповіді в лоб. Задавайте питання на порівняння, протиставлення. Наприклад: порівняти перець і колесо.
- 18) Ставте питання, на які немає правильної відповіді.
- 19) Складайте історії про «що бачу».
- 20) Грайте в різноманітні ігри, коли дитині треба зробити самостійний вибір.

Запропоновані способи для розвитку критичного мислення на уроках допоможуть учням навчитися сприймати явища, предмети чи події з різних точок зору, а також викличуть зацікавленість у вивченні й дослідженні світу. Навички критичного мислення залежать від уміння вчителя керувати навчальною діяльністю на уроці, розраховувати різноманітні можливості учнів, навчитися бачити й показати кожному учню його унікальність. У майбутньому це все узятє разом зможе сформувати з учнів успішних особистостей¹.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Які психологічні особливості підліткового віку можуть стати підґрунтям ризикової поведінки в мережевому просторі?
2. Які досягнення є опорою формування системи попередження і пропедевтики ризикової поведінки в підлітковому віці?
3. Перелічіть напрями психологічного супроводу і підтримки підлітків, схильних до ризикової поведінки.
4. Які основні характеристики комунікативної активності ви можете виокремити?
5. Назвіть детермінанти ризикової поведінки молоді у віртуальному світі.

ПРАКТИЧНІ ЗАВДАННЯ

1. Проаналізувавши презентовані в навчальному посібнику шляхи зміцнення психічного здоров'я підлітків, оберіть один із запропонованих і за його змістом розробіть просту листівку-порадник для дитини.

¹ Детальніше див: <https://buki.com.ua/blogs/yak-navchyty-myslyty-krytychno-uchniv-pochatkovoyi-shkoly/>.

2. Відкрийте свою персональну сторінку в соціальній мережі. Оберіть одну з груп, до якої входите. Перегляньте правила спілкування в групі. Виділіть, з яких причин дописувача чи учасника цієї групи можуть забанити. Сформулюйте відповідну коротку загальну пораду, зрозумілу підлітку.
3. Сформулюйте три поради, які допоможуть підлітку навчитися уникати флеймів у мережевому спілкуванні, візуалізуйте ці поради.

РЕКОМЕНДОВАНІ ДжЕРЕЛА

1. Курс із мережевого етикету й безпеки. [Електронний ресурс]. — Режим доступу : [g.co/ DigitalCitizenshipCourse](https://g.co/DigitalCitizenshipCourse).
2. Модельовання освітнього простору в умовах реалізації концепції «Нова українська школа» : методичні рекомендації / уклад.: Т. В. Деміракі; за заг. ред. В. В. Стойкової. — Миколаїв : ОППО, 2018. — 36 с.
3. Нова українська школа : поради для вчителя / за заг. ред. Н. М. Бібік. — Київ, 2019. — 208 с.
4. Обачність. Пильність. Захист. Ввічливість. Сміливість. Посібник із цифрового громадянства й безпеки / розробники: Google у співробітництві з Альянсом із захисту безпеки користувачів в інтернеті (Internet Keep Safe Coalition, iKeepSafe.org), 2017. — 42 с.
5. Проектування індивідуальної освітньої траєкторії професійного розвитку педагога : збірник тез Всеукраїнської науково-практичної конференції (м. Біла Церква, 13 червня 2019 р.); упоряд. Л. А. Литвиненко. — Київ : Всеосвіта, 2019. — 189 с.
6. Ройз С. Ресурсна скриня. — Київ : МФВ, 2021. — 52 с.
7. Цюман Т. П., Бойчук Н. І. Кодекс безпечного освітнього середовища : метод. посіб. / за заг. ред. Т. П. Цюман. — Київ, 2018. — 56 с.
8. Patchin, Ph.D, Justin. «2019 Cyberbullying Data.» <https://cyberbullying.org/2019-cyberbullying-data> (дата звернення 15.07.2021).
9. Hinduja, Ph.D, Sameer and Justin Patchin Ph.D. “Cyberbullying: Identification, Prevention, and Response.” <https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2018.pdf> (дата звернення 15.07.2021).

10. “Cyberbullying: Dealing with Online Meanness, Cruelty, and Threats.” MediaSmarts. http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/summary/YCWWI-II_Cyberbullying_ExecutiveSummary.pdf (дата звернення 15.07.2021).
11. Marcum, Catherine D. et al. “Battle of the Sexes: An Examination of Male and Female Cyberbullying.” *International Journal of Cyber Criminology*. <http://www.cybercrimejournal.com/marcumetal2012janijcc.pdf>. Anderson, Monica. “A Majority of Teens Have Experienced Some Form of Cyberbullying.” Pew Research Center. <https://www.pewinternet.org/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/> (дата звернення 15.07.2021).
12. “2015 National School Climate Survey.” GLSEN. https://www.glsen.org/sites/default/files/2015%20National%20GLSEN%202015%20National%20School%20Climate%20Survey%20%28NSCS%29%20-%20Full%20Report_0.pdf (дата звернення 15.07.2021).
13. “The Annual Bullying Survey 2017.” Ditch the Label. <https://www.ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-1.pdf> (дата звернення 15.07.2021).
14. John, FFPH, Ann. “Self-Harm, Suicidal Behaviours, and Cyberbullying in Children and Young People: Systematic Review.” *Journal of Medical Internet Research*. <https://www.jmir.org/2018/4/e129/> (дата звернення 15.07.2021).
15. “Safety Net: Cyberbullying’s Impact on Young People’s Mental Health: Inquiry Report Summary.” The Children’s Society. <https://www.childrenssociety.org.uk/sites/default/files/social-media-cyberbullying-inquiry-summary-report.pdf> (дата звернення 15.07.2021).
16. “Safety Net: Cyberbullying’s Impact on Young People’s Mental Health: Inquiry Report.” The Children’s Society. https://www.childrenssociety.org.uk/sites/default/files/social-media-cyberbullying-inquiry-full-report_0.pdf (дата звернення 15.07.2021).
17. “Stop Cyberbullying Before It Starts.” National Crime Prevention Council. <http://archive.ncpc.org/resources/files/pdf/bullying/cyberbullying.pdf> (дата звернення 15.07.2021).
18. “Cyberbullying: The Role of the Witness.” Media Smarts. <http://mediasmarts.ca/digital-media-literacy/digital-issues/cyberbulling/cyberbullying-role-witnesses> (дата звернення 15.07.2021).

1. ДОТРИМАННЯ ЕТИКЕТУ В МЕСЕНДЖЕРАХ

- Час для спілкування — із 09.00 до 19.00.
- Переконайтеся, що ваше питання заслуговує на увагу та час.
- Завжди вітайтеся, починаючи переписку.
- Звертайтеся до співрозмовника по імені.
- Намагайтеся уникати голосових повідомлень.
- Не використовуйте CapsLock, смайлики, меми.
- Не зловживайте значною кількістю повідомлень.
- Не телефонуйте в месенджері без попередження.
- Якщо співрозмовник не відповідає, нагадайте про себе пізніше.
- Якщо не можете відповісти відразу, повідомте про це співрозмовника.

2. TELEGRAM — ЦЕ ОДИН ІЗ НАЙПОПУЛЯРНІШИХ МЕСЕНДЖЕРІВ

Telegram дозволяє обмінюватися текстовими й відеоповідомленнями, а також здійснювати дзвінки.

Переваги Telegram

- Безліч серверів по всьому світу, що дозволяє досягти високої швидкості й безпеки. Завдяки цьому в «Telegram» найшвидша доставка повідомлень.
- Відкритий протокол, що дає можливість розробникам використовувати напрацювання команди «Telegram».
- Відправлення абсолютно будь-яких файлів і документів.
- Секретні чати та групи.
- Надійний захист від різних атак.
- Повністю безкоштовний і навіть без реклами.



2. Telegram — це один із найпопулярніших месенджерів

- Практично повна відсутність обмежень за розміром чату й файлів. В одному повідомленні можна відправляти скільки завгодно файлів розміром до 1,5 Гб.
- Групові чати до 30 000 учасників, а також тематичні канали на зразок груп у соціальних мережах.
- Легкість у використанні, мінімум споживаних ресурсів пристрою, а також повна кросплатформеність.
- Повідомлення самовидаляється. Можна задати проміжок часу, коли повідомлення буде автоматично видалено.
- Можна зберігати всі свої файли в хмарі. Тепер файли не будуть займати дорогоцінну пам'ять пристрою.
- Синхронізація повідомлень між усіма пристроями. Можна навіть почати набирати повідомлення на телефоні, а потім завершити на комп'ютері, або навпаки.
- Самостійне створення стікерів за допомогою бота.

Можливості TELEGRAM

- Додавання контакту. Якщо він доданий у список контактів вашого телефону, то автоматично відобразиться в додатку. Також список контактів автоматично синхронізується між усіма пристроями.
- Відправка вкладення. Можна відправити фото, відео, аудіо, будь-який файл, контактні розташування. Як це зробити? Біля поля введення у вікні листування натисніть значок скріпки, після чого виберіть, який тип вкладення ви хочете додати.
- Відправка голосового та відеоповідомлення. Біля поля введення є кнопка у вигляді мікрофона. Якщо натиснути на неї, можна перемикатися між режимом голосового та відеоповідомлення. Для самого запису утримуйте кнопку. Як тільки ви її відпустите, то повідомлення відразу ж буде надіслано.
- Створення групового чату або каналу. Групові чати дозволяють вести листування між величезною кількістю



людей (до 30 тисяч). Канали являють собою подоби груп у соціальних мережах. Їх теж можуть читати десятки й навіть сотні тисяч людей. Щоб створити канал або групу, виберіть відповідний пункт у меню програми.

- Створення секретного чату. Секретний чат — унікальна функція, якої немає в переважної більшості конкурентів. Уся переписка між двома користувачами повністю зашифрована наскрізним шифруванням, що означає, що її можуть прочитати тільки два користувачі. Вміст не видно навіть розробникам. Крім того, можна налаштувати при відправці, щоб через певний час повідомлення самознищилось.
- Дзвінок. Щоб зателефонувати комусь через «Telegram», знайдіть його в списку контактів, після чого у вікні чату натисніть значок у вигляді телефонної трубки. Таким само можна зробити дзвінок будь-якому учаснику групового чату.

3. ІНСТАГРАМ — ЦЕ СОЦІАЛЬНА МЕРЕЖА ДЛЯ ОБМІНУ ФОТОГРАФІЯМИ ТА ВІДЕОЗАПИСАМИ

Як створити обліковий запис в Instagram

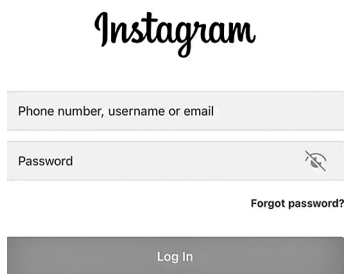
Якщо у вас є обліковий запис в Instagram, ви можете увійти в нього з будь-якого пристрою — вашого телефону, планшета або браузера на вашому комп'ютері. Усе, що вам потрібно, це ваші облікові дані для входу, такі як ваше ім'я користувача в Instagram, або номер телефону, або адреса електронної пошти, пов'язані з обліковим записом, а також ваш пароль. Також можна увійти в систему через Facebook, якщо ви підключили облікові записи.



3. Інстаграм — це соціальна мережа для обміну фотографіями та відеозаписами

Як увійти в Instagram на мобільному пристрої

Вхід до свого облікового запису Instagram на смартфоні або планшеті однаковий, незалежно від того, чи використовуєте ви додаток Instagram на пристрої iOS або Android. Як правило, Instagram дозволяє вам увійти в систему, використовуючи свій номер телефону або адресу електронної пошти, пов'язані з обліковим записом, тому введіть будь-який із цих трьох елементів. Після цього введіть свій пароль і натисніть «Увійти».



Як увійти в Instagram за допомогою Facebook

Якщо ви зв'яжете свій обліковий запис Instagram з Facebook, ви не тільки зможете легко ділитися своїми постами в Instagram на Facebook, але також зможете використовувати свої облікові дані Facebook як простий спосіб входу в Instagram.



Щоб зв'язати свої облікові записи Facebook і Instagram, відкрийте додаток Instagram на своєму мобільному пристрої, клікніть меню з трьома смугами й натисніть «Налаштування». У розділі «Рахунок» перейдіть у розділ «Спільне використання з іншими додатками» і підключіть Instagram до свого облікового запису Facebook.

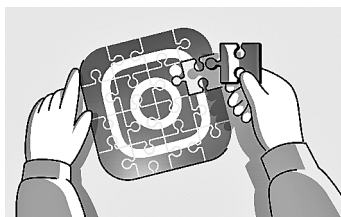
Підключіть свій обліковий запис Facebook до Instagram, якщо ви хочете мати можливість входити в систему, не запам'ятовуючи свої облікові дані Instagram. Після підключення цих двох облікових записів ви можете ввійти в Instagram за допомогою Facebook — на сторінці входу ви можете натиснути «Увійти за допомогою Facebook».

Що робити, якщо не виходить увійти в Instagram

Якщо ви втратили або забули пароль, можливо, вам доведеться його скинути. Процес по суті той самий, незалежно

від того, чи є у вас iPhone, пристрій Android або ви використовуєте веббраузер на комп'ютері:

- 1) На екрані входу в систему під полями імені користувача і пароля натисніть «Виправити це для мене» при вході в систему (якщо ви використовуєте телефон Android) або «Забули пароль?» (на iOS або в браузері).
- 2) Уведіть адресу електронної пошти, номер телефону або ім'я користувача та натисніть «Далі» (якщо ви використовуєте Android) або «Надіслати посилання для входу» (у веббраузері). Якщо ви використовуєте iPhone, виберіть, яку вкладку ви хочете використовувати — «Ім'я користувача» або «Телефон», і введіть облікові дані, пов'язані з вашим обліковим записом, потім натисніть «Далі».
- 3) Ви отримаєте повідомлення з інструкціями щодо скидання пароля. Також, можливо, ви не пам'ятаєте ім'я користувача або іншу інформацію, пов'язану з вашим обліковим записом, або ввели її неправильно. Ось кілька речей, які варто спробувати:
 - переконайтеся, що ви правильно пишете ім'я користувача або адресу електронної пошти;
 - не вмикайте символ @ при введенні імені користувача;
 - попросіть кого-небудь, хто може бачити сторінку вашого профілю, зробити знімок екрана або записати своє ім'я користувача за вас.



Як відключити обліковий запис Instagram від Facebook

- 1) На мобільному пристрої або планшеті відкрийте додаток Instagram.
- 2) Відкрийте сторінку свого профілю, потім торкніться трьох горизонтальних ліній у верхньому правому куті екрану, щоб відкрити меню параметрів.
- 3) У нижній частині меню параметрів натисніть «Налаштування».

3. Інстаграм — це соціальна мережа для обміну фотографіями та відеозаписами

- 4) На сторінці «Налаштування» знайдіть параметр «Рахунок» і натисніть його.
- 5) У розділі «Рахунок» знайдіть параметр «Пов'язані облікові записи». На цій сторінці ви побачите Facebook, виділений ім'ям, зазначеним у вашому профілі Facebook.
- 6) Щоб від'єднати, торкніться параметра Facebook і натисніть «Скасувати зв'язок з обліковим записом».
- 7) З'явиться попередження, у якому вас попросять підтвердити свій вибір для скасування зв'язку між вашими обліковими записами та повідомити, що це ускладнить відновлення доступу до Instagram, якщо ви будете заблоковані.
- 8) Натисніть «Так, від'єднати», щоб завершити процес.

Зверніть увагу, що відключення ваших облікових записів Facebook і Instagram не обов'язково має бути постійним. Ви можете повторно пов'язати свій обліковий запис у будь-який час за допомогою тих же параметрів меню, які використовувалися для відключення. Якщо ви вирішите це зробити, вам потрібно буде повторно ввести дані для входу й дозволити Instagram доступ до вашого профілю Facebook, щоб повторно включити перехресну публікацію між двома платформами.

Ще недавно здавалося, що правила поведінки в соціальних мережах уже склалися: не ображай, не критикуй думку, висловлену автором на своїй сторінці, не засмічуй чужі сторінки смайлами й картинками не по суті, не показуй власну перевагу, поважай чужі кордони. Однак у міру зростання популярності Instagram можна спостерігати появу нових традицій мережових взаємин.

Цей майданчик дає можливість знайти швидку популярність і заробити на ній. Для прибутку необхідна активність на сторінці або каналі блогера, тому останні не цураються ніяких засобів, щоб цю активність організувати. Це впливає на поведінку передплатників. Уже зовсім не соромно перервати дискусію несуттєвим коментарем, потривожити абсолютно незнайому людину питанням із серії «Де брали?». А також без кінця відправляти смайлики, оскільки це активність, а активність — це популярність і прибуток. Усе б нічого, але зі сфери соцмереж нова етика переходить у життя та змінює традиції спілкування.

Будь-яка соціальна мережа, якщо займатися нею серйозно, вимагає великої праці й значної кількості часу. Якщо людина веде сторінку в одній соцмережі для власного задоволення, це не вимагає глобальних зусиль, якщо в декількох, — це складніше, якщо ж вона стає блогером з великою кількістю передплатників — це однозначно непросто.

Правила етикету в Інстаграм

- Не використовуйте багато хештегів.
- Пишіть грамотно.
- Будьте обережні з лайками й репостами.
- Поважайте чужий час.
- Звертайтеся до незнайомих людей на «Ви».
- Не зловживайте емодзі.
- Не дробіть повідомлення.
- Увімкніть самоцензуру та не ставте й не лайкайте пости, які можуть вас скомпрометувати.
- Не використовуйте CapsLock.
- Не множьте одну й ту саму фотографію.
- Не викладайте фотографії з друзями без їхнього дозволу.
- Не спамте.

Не варто публікувати в соціальних мережах:

- тексти, зображення та відео на тему національностей;
- контент, який висміює релігії;
- інформацію про фашизм і тероризм.

Ваші повідомлення та пости — індикатор вашої освіченості!

Як зібрати побільше лайків і поменше хейтів в Інстаграм

- Оптимальний ритм публікації — одна-дві фотографії на день.
- Публікуйте фотографію в той день, коли вона була зроблена.
- Робіть фото без сторонніх додатків.
- Ніч не найкращий час для повідомлень.
- Реагуйте на повідомлення та коментарі.

3. Instagram — це соціальна мережа для обміну фотографіями та відеозаписами

Як Instagram змінює життя блогерів

- **Проблема перша: робити цікаву сторінку складно.** Бути блогером — теж складно. Це тільки здається, що якщо сидіти й просто розповідати щось на камеру, станеш відомим і збереш велику аудиторію. Ні! Це величезна праця, що вимагає таланту, розуму та часу. І неважливо, у який саме соцмережі людина веде блог, це складно скрізь.
- **Проблема друга і головна: активність.** Головна проблема для блогера в Instagram — це необхідність постійно бути активним, тобто щось публікувати. Більш того: недостатньо наповнювати сторінку тільки цікавим матеріалом, блогеру треба розповідати про себе і своє життя.



Споживачі хочуть активності від блогерів, чекають оновлень новинних стрічок, хочуть, щоб ці оновлення були цікавими. Якщо довго немає постів і Сторіс, люди починають відписуватися, що блогеру, звичайно, не подобається.

Біда блогерів у тому, що вони починають залежати від своїх сторінок, у них починаються якісь нав'язливі стани: п'ять годин минуло, а я нічого не постив! Це відбувається у тих, хто вкладає у розвиток блогу всього себе. Як правило, починається все невинно: людина хоче ділитися чимось цікавим і корисним, але через деякий час вона вже й не помічає, що стежить за охопленням аудиторії, числом передплатників, рівнем активності й т. ін. Бачить Instagram з іншого боку: не як соцмережу з гарними фотографіями, а як графік, який або радує, або показує, що він погано працює.

- **Проблема третя: зайва відвертість.** Блогер починає бути дуже відвертим у Сторіс або прямих ефірах з людьми, про яких нічого не знає. Часом від ступеня відвертості коробить навіть читачів або глядачів. Таке враження, що відкрив чужий щоденник і читаю те, що мені не призначене. Чому так виходить? Людина сидить в кімнаті наодинці з камерою, записує ефір

або пост, і у нього враження, що він сам. Але з іншого боку екрану зібралось кілька десятків людей, багатьох з яких не варто запрошувати в потаємні сфери свого життя. Треба намагатися застерегти своїх друзів, якщо складаються такі ситуації. Зрозуміло, що комусь буде все одно, але є ті, хто прислухається.

- **Проблема четверта:** *не разом, а поруч*. Не раз доводилося бачити, як хлопець і дівчина гуляють, і кожен знімає Сторіс у свій інстаграм. Може, я чогось не розумію, але коли закохані зайняті своїми блогами, а не один одним, це якось дивно.
- **Проблема п'ята:** *тролінг і хами*. Кожен блогер неодмінно стикається з хамством і неадекватними коментаторами. Чим більше передплатників — тим більше негативу. Причому зараз видаляти негативні коментарі не варіант, тому що людина, побачивши це, прийде і залишить ще п'ять. Так що ті, хто веде блог, повинні бути готові до цього. В ідеалі добре, щоб блогом займалося кілька людей, тоді простіше зберегти психіку здорової.

Як необхідність активності впливає на наші відносини

Блогеру недостатньо регулярно публікувати пости і Сторіс, треба ще й постійно лайкати коментарі, відповідати на них хоча б смайликом-сердечком. Раніше нас вчили, що не слід відволікати всякою нісенітницею зайнятих людей. А тепер виявляється, що навіть дріб'язкова реакція цінна, тому що це підвищує твій рейтинг і створює необхідну активність на сторінці. Люди просять, щоб їх передплатники хоч як-небудь реагували на їхні пости. Це ще більше руйнує кордони між людьми, тому що постійні відвідувачі Instagram звикають, що втручання в чуже життя — це норма, це корисно і добре.

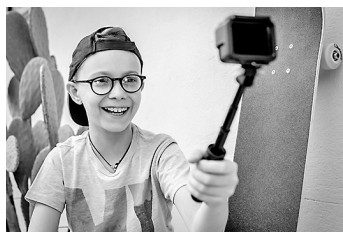
Чому це так популярно? Колосальна популярність Instagram пояснюється тим, що в безлічі молодих людей є бажання наслідувати своїх улюблених зірок, бути такими ж крутими. Ну, і це хороша можливість заробити, якщо блог отримає популярність. Якщо ваша дитина цілодобово сидить у телефоні й у свої чотирнадцять-п'ятнадцять років мріє стати блогером-мільйонником, нехай. До вісімнадцяти років

3. Інстаграм — це соціальна мережа для обміну фотографіями та відеозаписами

Йому це обридло, бо у всьому цьому є якась несправжність. Зрештою йому захочеться нормального спілкування, а значить, доведеться вийти з квартири та побачити очі людини, якого він до того десять років бачив тільки на екрані. Прямі ефіри й конференц-зв'язок не рятують: вони виснуть, фонують і взагалі незручні. Так що я сподіваюся, що поступово підлітки перехворіють соцмережами й підуть у реальність.

Діти-блогери

Це велика біда. Тут виникає багато питань до батьків, які все це допускають. На жаль, дитяче блогерство — це, як правило, реклама. Заробляє у такий спосіб зараз чимало дітей. Вірніше, чимало батьків, які все це організовують і підтримують. До того ж, часто це дуже фальшиво й непрофесійно.



Можна знайти хороші дитячі блоги, але все одно, як правило, така діяльність таїть багато небезпек. Батькам, які підтримують її, треба чесно відповісти на питання: чи не ламають вони психіку своїх дітей? Чи не намагаються змусити робити те, що їм насправді нецікаво? Чи не віднімають вони в дітей дитинство? Мало кому подобаються десятки дублів і промовляння примітивних рекламних текстів. Чи не прийде такий блогер через кілька років зі звинуваченнями, що йому скалічили життя?

Як Instagram змінює життя передплатника

У передплатників теж поступово утворюється залежність від улюблених блогерів. Людина звикає спостерігати їхнє життя, якимось чином навіть брати участь у ній — лайками, коментарями. Часом доступність зірок людину розбещує: вона втрачає відчуття кордонів, переходить межі дозволеного. Зверніть увагу, як просто зараз люди переходять на «ти»!

Відкритість і прозорість інтернету призводить до панібратства. Пояснити це легко: люди автоматично вважають близьким власника популярної сторінки, оскільки залучені в його життя. Звичайно, самі блогери в цьому винні. Що

взяти з передплатників, якщо блогер проводить рум-тури (тобто тур по квартирі), показуючи, де й що в нього! Він таким чином або намагається привернути увагу до себе, або рекламує меблі, якісь речі. А передплатник, віртуально побувавши вдома в зірки, відчуває себе з ним мало не приятелем. Тим більше, що він уже знає, які млинці той їсть на снідачок, де відпочиває, яким шампунем користується і так далі.

Знову ж таки, як можна засуджувати передплатників за настирливість і втручання в життя, якщо блогери самі просять: пишіть, коментуйте, ставте лайки, «зворотний зв'язок нам дуже важливий»? Насправді їм неважливі ваші лайки та сердечка. Ці заклики означають тільки одне: у них на сторінці підключена монетизація, тобто вони просто заробляють за допомогою цього. Або ж вони вклалися в рекламу, і їм треба ці гроші відбити. А нам здається, що ми робимо важливу справу, підтримуємо свого улюбленого блогера.

Будьте обережні в соцмережах, уважні до себе й оточуючих. Думайте, чи потрібно впускати у своє життя тих, кого ви впускаєте, чи варте воно того. Не забувайте, що в житті повинна бути частина, яка належить тільки вам і вашим близьким людям. Instagram не поганий і не хороший — він такий, яким ми його робимо, а перекрутити можна навіть найкращі речі. Підписуйтесь на хороші сторінки та блоги — і у вас буде багато корисної інформації, нових знань і цікавих знайомств. Але пам'ятайте, що це тільки частина вашого життя.

4. ПРАВИЛА СПІЛКУВАННЯ У VIBER-ЧАТІ

- Не поширюйте неперевірену інформацію.
- Будьте відповідальними за те, що пишете або пропонуєте.
- Не давайте оцінку людині та не «вішайте ярлики».
- Турбуйтеся про стан та почуття співрозмовника.
- Не засмічуйте спілкування в месенджерах «дрібними» повідомленнями.
- Не переходьте на особистості.
- Не вживайте образливі фрази.



6. Безпека у використанні zoom

- Будьте чесними та уважними до співрозмовника.
- Ніколи не приховуйте свій статус.
- Будьте стриманими, а не гіперактивними.
- Пишіть співрозмовнику лише з одного месенджера.

5. ЗАХИСТ ВІД СПАМУ

Спам (англ. *Spam*) — це масове розси-
лання рекламних листів, повідомлень ко-
ристувачам, які не давали на це своєї згоди.

Використовується з метою залучення
в процес маркетингу власників електрон-
них пошт. Повністю захиститися від спаму
неможливо, але можна звести до мінімуму ймовірність його
потрапляння до особистої електронної пошти.



- Не повідомляйте нікому електронну адресу.
- Не вказуйте e-mail в опитувальниках.
- Майте окремий e-mail для важливих справ.
- Не публікуйте e-mail у відкритому доступі.
- Приховуйте інформацію про себе.
- Налаштовуйте параметри приватності.
- Умикайте антиспам системи.
- Забороніть спливаючі вікна в браузері.

6. БЕЗПЕКА У ВИКОРИСТАННІ ZOOM

Zoom — хмарна платформа для орга-
нізації відеоконференцій, онлайн-зустрічей,
вебінарів, онлайн-заходів.

Щоб почуватися безпечно, слід дотри-
муватися певних правил.

- Реєстрація під справжнім прізвищем та ім'ям.
- Проведення ідентифікації перед початком.
- Використання функції «зала очікування».
- Установлення пароля до конференції.
- Заборона на публікації паролей та посилань.
- Надання права адміністратора учасникам заборонено.



- Використання кнопки «Управління учасниками».
- Видалення небажаного учасника.
- Використання зворотного зв'язку.

7. ЯК ВИЗНАЧИТИ, ЩО НА КОМП'ЮТЕРІ Є ВІРУС

- Комп'ютер відчутно уповільнює роботу.
- Комп'ютер самостійно перезавантажується.
- Ваші друзі отримують від вас повідомлення, яких ви не писали.
- Відбувається несанкціонований запуск програм.
- Зростає споживання трафіку.
- Комп'ютер часто «висне».
- Браузер поводить себе неадекватно, у довільному порядку відкриває вікна, їх неможливо закрити.
- Виникають системні помилки.
- На екрані з'являються незвичні повідомлення.
- При включенні комп'ютера операційна система не завантажується.
- При виключенні комп'ютера система видає повідомлення про спробу закрити певні програми.
- Спалахує індикатор доступу до жорсткого диску, хоча ви не запускали жодної програми.



8. ЯК ВИДАЛИТИ КОМП'ЮТЕРНИЙ ВІРУС

- 1) Завантажте та встановіть антивірусний сканер.
- 2) Відключіться від інтернету.
- 3) Перезавантажте комп'ютер у безпечному режимі.
- 4) Видаліть усі тимчасові файли.



10. Поради з безпечного з'єднання в публічних wi-fi мережах

- 5) Включіть сканування комп'ютера на віруси.
- 6) Видаліть віруси або помістіть їх у карантин.
- 7) Перезавантажте комп'ютер.

9. КОРИСНІ ПОРАДИ ДЛЯ БЕЗПЕЧНОЇ ПРОФЕСІЙНОЇ КОМУНІКАЦІЇ

- 1) Для навчальних взаємодій між працівниками школи, учнями, батьками чи іншими зацікавленими у якості освіти особами завжди використовувати шкільну електронну пошту.



- 2) Бажаємо сформувати звичку в учасників освітнього процесу: у стінах навчального закладу в навчальний час краще не контактувати на платформах, які не мають відношення до навчального процесу в цьому закладі освіти в конкретний час.
- 3) Месенджери використовувати тільки в тому випадку, якщо ви не можете взаємодіяти наживо.
- 4) Установити разом з учнями прості й чіткі правила як для працівників, так і для учнів щодо проведення відеоконференцій, онлайн-занять: наприклад, правила, який вигляд має місце для проведення уроків, наявність фото профіля, підпис профіля державною мовою тощо.

10. ПОРАДИ З БЕЗПЕЧНОГО З'ЄДНАННЯ В ПУБЛІЧНИХ WI-FI МЕРЕЖАХ

- 1) Запам'ятати й прийняти істину: публічні Wi-Fi мережі не захищені, тож хакери можуть відносно легко отримати доступ до вашого пристрою (ноутбуку, смартфон).



- 2) Бажаємо використовувати VPN. Це технологія, яка дозволяє створити безпечне з'єднання через інтернет.

- 3) Використовувати гіперпосилання обережно. Інколи в посиланні може міститися небезпечний код, який відкриває доступ до вашого пристрою, завантажує вірус тощо.
- 4) У разі отримання листа-спам із призами, вигідними пропозиціями, проханнями від невідомих вам осіб про допомогу та благодійний внесок, краще його проігнорувати.
- 5) Захищати мобільний телефон так само, як і комп'ютер, інші цифрові пристрої.
- 6) Використовувати брандмауер.
- 7) Думати про те, із ким ви розмовляєте.
- 8) У мережі не все надійне і не всі чесні.
- 9) Ви повинні піклуватися про репутацію інших так само, як і про свою.

11. УВАЖНІСТЬ ПІД ЧАС ЗДІЙСНЕННЯ ПЛАТЕЖІВ

- 1) Коли заходите на вебсайт, щоб здійснити оплату (наприклад, в онлайн-магазині чи особистому кабінеті банку), слідкуйте, щоб адреса сайту починалася з **https**, а не **http**, та поряд із назвою сайту була позначка у вигляді замочку.
- 2) Пильнуйте: під час відвідування вебсайтів назви деяких із них мають помилки чи близькі за змістом до оригінальних назв. Таким способом шахраї можуть маскувати фальшиві вебсайти, які створюються з метою викрадання персональних даних.
- 3) Мобільні додатки завантажуйте тільки з офіційних ресурсів та після перегляду відгуків від користувачів.
- 4) Встановіть і систематично оновлюйте антивірусний захист мобільного пристрою.
- 5) Систематично оновлюйте операційну систему мобільного пристрою.



12. ПОРАДИ ВІД ЕМІ МАКРІДІ ДЛЯ БАТЬКІВ¹

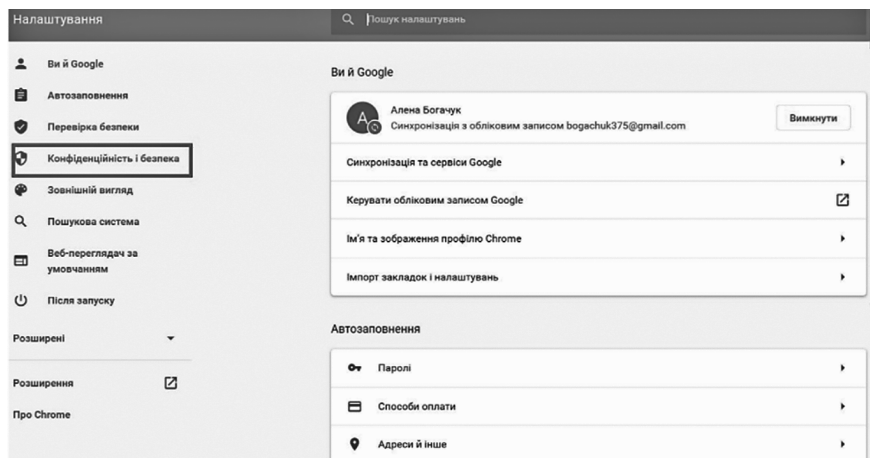
- Чітко визначте та повідомте дітей про обмеження технологій. Електронні прилади є своєрідними привілеями, яких дитину можна позбавити, якщо вона не дотримується правил.
- Порухення встановлених правил приведе до втрати права користування гаджетом, програмою.
- Встановіть часові обмеження для електронних пристроїв.
- Спальня та дитяча — без гаджетів.
- Не в мережі. Визначте час, вільний від гаджетів.
- Обговорюйте проблеми особисто, а не в мережі.
- Ніколи не соромте дитину в мережі.
- Знайдіть час для спільного навчання й прокачування цифрової грамотності.
- Ви не можете контролювати те, чого не розумієте.
- Просіть дитину навчити вас користуватися програмами та застосунками, які їй подобаються.



13. КОНФІДЕНЦІЙНІСТЬ ТА БЕЗПЕКА ВЕББРАУЗЕРУ GOOGLE CHROME

Для того, щоб налаштувати конфіденційність та безпеку веббраузеру Google Chrome, потрібно у верхньому куті екрана натиснути позначку ⋮ та обрати «Налаштування», а після зайти в розділ «Конфіденційність і безпека» (див. рисунок на с. 168.).

¹ <https://nashformat.ua/products/ya-ya-ya-yak-perevyhovaty-egoistychnu-dytynu-abo-ii-batkiv-709164>



У розділі «Конфіденційність і безпека» представлено такі можливості:

- «Очистити історію»

Дозволяє видалити всю історію сайтів, які ви відвідували.

- «Файли cookie та інші дані із сайтів»

Необхідно видалити файли, які використовують сайти для функціонування реклами (файли cookie).

- Безпека

Можливість обрати рівень захисту перегляду вебсторінок.

- «Налаштування сайтів»

Можливість переглянути або змінити дозволи для сайтів.

«Перевірка безпеки» допоможе вберегти від витоку даних сумнівних розширень, а також інших проблем із безпекою.

14. ЩО ТАКЕ ЗУМБОМБІНГ ТА ЯК ВІД НЬОГО ЗАХИСТИТИСЯ

Зумбомбінг — різновид кібератак, який став популярним у програмі Zoom, та являє собою захоплення відеоконференції. Користувачі розповідали про випадки, коли зловмисники малювали на екрані образливі зображення, показували непристойні



фотографії, викладали особисті дані учасників та погрожували учасникам зустрічей. Новий різновид кібератак став настільки популярним, що заслужив статтю у Вікіпедії. Інтернет-видання PCMag повідомило, що зловмисники обмінуються даними відеоконференцій на форумах; записують «зумбомбінг» та викладають у TikTok або YouTube. Швидко з'явилося безліч спільнот у Discord і Telegram, де «інтернет-тролі» діляться даними відкритих відеоконференцій. Як правило, вони використовують «ботів», щоб знаходити записи зустрічей та конференцій.

Інтернет-тролі — це люди, які хочуть провокувати та засмучувати інших у мережі заради власного задоволення.

Місця в інтернеті, де ви можете побачити онлайн-тролів:

- 1) анонімні онлайн-форуми, сайти, дошки оголошень;
- 2) Twitter також може бути анонімним, він став розсадником для інтернет-тролів. Часті методи тролінгу у Твіттері включають використання популярних хештегів і згадування популярних осіб у Твіттері для привернення уваги передплатників;
- 3) розділи коментарів у таких місцях, як YouTube та новинні сайти, також є популярними областями для годування тролів. Тут ви знайдете багато очевидних тролінгів, і вони часто викликають багато відгуків у злих читачів чи глядачів.



Ознаки тролінгу

- Зауваження не на тему.
- Відмова у визнанні доказів.
- Похмурий, поблажливий тон.
- Використання незв'язаних зображень або мемів.
- Забудькуватість.

Як захистити себе від зумбомбінгу

- 1) Не роби зустрічі публічними. У Zoom є можливість зробити зустріч приватною, щоб на неї потрапили тільки схвалені учасники. По-перше, ти можеш призначити пароль, який відправиш на пошту кожному учаснику (ніколи не викладай пароль разом із посиланням на загальний доступ). По-друге, ти можеш увімкнути функцію «Кімната очікування», щоб підключати лише схвалених гостей.
- 2) Увімкни вхід лише за доменом. Ти можеш увімкнути цю функцію, якщо всі учасники зареєстровані в програмі. Таким чином, випадкові (анонімні) люди не зможуть входити до відеоконференції. Крім того, є можливість повідомити порушення, щоб Zoom назавжди заблокувала користувача.
- 3) Не використовуй власний ідентифікатор конференції. У Zoom можна використовувати власний ідентифікатор конференції або унікальний ідентифікатор, який генерує програма випадково. Програма створює унікальний ідентифікатор кожної зустрічі. Це гарантія, що зловмисник не зможе увійти до конференції знову.
- 4) Переконайся, що використовуєш оновлену версію програми. Компанія продовжує працювати над безпекою. В останніх версіях з'явилися нові функції, які ускладнюють зумбомбінг (наприклад, «Кімната очікування»).
- 5) Закрий зустріч, коли всі учасники зібралися. Найнадійніший спосіб позбутися зловмисників — закрити зустріч. У програмі є функція Lock Meeting, яка не дає новим учасникам увійти в конференцію. Усі учасники зібралися — сміливо закривай зустріч для інших людей.
- 6) Вимкни спільний доступ до екрана. Найчастіше інтернет-тролі використовують екран, щоб малювати непристойні зображення або показувати фотографії та відео. Але цю проблему легко вирішити. Потрібно просто вимкнути цю можливість у налаштуваннях керування організатора конференції.

14. Що таке зумбомбінг та як від нього захиститися

- 7) Відключи можливість передавати файли і писати коментарі. Часто інтернет-тролі ображають учасників зустрічей у коментарях. На щастя, ти можеш заблокувати цю можливість. Це значно покращує безпеку зустрічей.



- 8) Заблокуй небажаних учасників. Якщо інтернет-тролі проникли на зустріч (таке іноді відбувається) просто заблокуй небажаних учасників. Для цього потрібно перейти до списку учасників, навести курсор на користувача та вибрати команду «Видалити».

1. ПЕРЕЛІК ОСВІТНІХ ПЛАТФОРМ ДЛЯ ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО ТА ЗМІШАНОГО НАВЧАННЯ В ЗАКЛАДАХ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ

- Портал **Дія. Цифрова освіта** (підвищення цифрової грамотності для громадян України);
- освітні серіали для вчителів **Карантин: онлайн-сервіси для вчителів** (формування цифрових навичок для педагогів);
- об'єднана всеукраїнська освітня мережа для вчителів, учнів, батьків **Щоденник.ua** (для впровадження сучасних комп'ютерних технологій у навчальний процес);
- громадська організація та тренінговий Хаб для вчительської спільноти **Освіторія** (курси й тренінги для вчителів);
- освітнє онлайн-середовище **MySchool.ua** (автоматизація документообігу шкіл, онлайн-бібліотеки з мультимедійними матеріалами для учнів, конспекти для вчителів з усіх предметів, тем для всіх класів і різних SMS-сервісів, облік шкільних підручників, конструктор електронних тестів, тематична соціальна мережа);
- освітня платформа **Prometheus** (комплекс розроблених лекцій, курсів, завдань із найрізноманітніших предметів);
- онлайн-школа **На Урок** (підвищення кваліфікації вчителів, всеукраїнські онлайн-курси, олімпіади та журнал для школярів, розробки уроків, тестового контролю тощо);
- освітня платформа **Доступна освіта** (вивчення навчальних предметів екстерном);
- освітня платформа **EdEra** (масові відкриті онлайн-курси із широким застосуванням інтерактивних лекцій та домашніх завдань);
- сайт освітніх новин **Osvita.ua** (каталог українських та зарубіжних закладів освіти, рейтинг шкіл та дистанційних курсів, корисний матеріал);

2. Сервіси та платформи для організації дистанційного та змішаного навчання

- освітня ініціативна платформа **Бумонлайн** (понад 30 сучасних тем для навчання, відеокурси, відеолекції);
- освітня платформа **Coursera** (у доступі навчальні курси, проекти провідних закладів освіти);
- платформа **Дистосвіта** (навчальні матеріали, конструктори тестів, завдань для вчителів інформатики);
- освітня платформа **Edx.org** (навчальні курси кращих університетів світу);
- універсальний усеукраїнський освітній портал **Parta.ua** (курси, майстер-класи, конкурси);
- портал інтерактивної дошкільної та шкільної електронної освіти **learning.ua** (програми, завдання для поглибленого вивчення предметів, онлайн-тести, інтерактивні завдання);
- платформа **Гіпермаркет знань** (повна шкільна програма для підготовки до відкритих уроків, контрольних робіт і практичних завдань, зібрання шкільних підручників, посібників та дидактичних матеріалів, завдань і вправи для самоперевірки практикумів, тренінги й домашні завдання);
- **Nus-english** (освітня платформа для вчителів з англійської мови);
- освітня платформа для вчителів, учнів, батьків **Nus.org.ua** (новини Нової української школи);
- електронна платформа для педагогів **Atoms.ua** (підвищення кваліфікації вчителів);
- поради від кращих учителів України за версією **Global Teacher Prize Ukraine**.

2. СЕРВІСИ ТА ПЛАТФОРМИ ДЛЯ ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО ТА ЗМІШАНОГО НАВЧАННЯ: МОЖЛИВОСТІ, ПЕРЕВАГИ, НЕДОЛІКИ

MOODLE

1. Можливості.

Формати. Moodle підтримує всі сучасні формати. SCORM, AICC і IMS підтримуються за замовчуванням, для xAPI потрібен плагін.



Інтеграція. Moodle легко інтегрується з іншими системами й сервісами. Якщо потрібно підключити CRM-систему, можна скористатися Arlo або Edwiser Bridge (підключає все необхідне для eCommerce).

Контент навчання. У Moodle можна завантажити будь-який тип контенту: текстовий (включаючи PDF і XLS), зображення, презентації (через плагін Presentation), тести та курси. Відео можна завантажити просто так або для зручності підключити Medial — стрімінговий відеосервіс. Можна формувати плани навчання (learning plans).

Мобільне навчання (смартфони, планшети) Moodle можна відкривати в мобільних браузерах Chrome і Safari або використовувати додаток Moodle Mobile.

Звітність. У Moodle можна вивантажувати будь-який вид звіту, але для цього потрібен плагін, який відповідає за дизайн.

2. Переваги.

- Для всіх типів закладів освіти;
- ведення форуму, чату, гейміфікація;
- створення якісних курсів для дистанційного навчання;
- керування курсами;
- потужний апарат тестування;
- різноманітність навчальних елементів;
- реалізація диференційованого навчання;
- налаштування варіантів керування доступом користувачів до курсу;
- відстеження прогресу учнів за допомогою візуалізації;
- публікації навчального контенту різного формату — аудіо, відео, текст та ін.

3. Недоліки.

- Для встановлення потрібен сервер (хостинг, доменне ім'я);
- непосильно для деяких ЗЗСО;
- потребує певних витрат часу на вивчення;
- потребує обслуговування та наявності адміністратора;
- споживає багато ресурсів.

2. Сервіси та платформи для організації дистанційного та змішаного навчання

EDPUZZLE

1. Можливості та переваги.

- Безкоштовний сервіс;
- створення відеоконтенту, інтерактивних онлайн-уроків;
- використання готового відеоконтенту, доступ до бібліотеки;
- організація поточного та підсумкового контролю знань здобувачів;
- синхронізація контактів.

2. Недоліки.

- Англomовний інтерфейс.



CANVA

1. Можливості та переваги.

- Безкоштовний сервіс;
- український інтерфейс;
- зручне генерування посилання та доступ до різноманітних шаблонів створення інфографіки, презентації, плакатів, брошур, логотипів тощо;
- створення скрінкастів;
- запис відеоуроків, лекцій, інтерактивного відео.

2. Недоліки.

- Немає.



CLASSROOM

1. Можливості та переваги.

- Безкоштовний хмарний сервіс;
- просте створення завдань;
- автоматичне сповіщення учнів;
- контроль за виконанням завдань;
- інтеграція Google Classroom на Google;
- відтермінування виконання завдання;
- наявність журналу оцінок для кожного класу.

2. Недоліки.

- російськомовний інтерфейс.



PLAYPOSIT

1. Можливості та переваги.

- Безкоштовна платформа;
- використання за запитом відео на YouTube і Vimeo;
- організація поточного контролю шляхом створення завдань.

2. Недоліки.

- Англomовний інтерфейс.



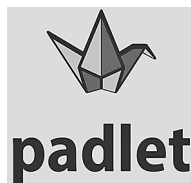
PADLET

1. Можливості та переваги.

- Безкоштовний сервіс;
- організація групової роботи;
- створення проєктів;
- розміщення навчального контенту;
- проведення інтерактивних вправ.

2. Недоліки.

- Англomовний та російськомовний інтерфейс;
- обмеження створення до 8 дошок у безкоштовній версії.



WIZER.ME

1. Можливості та переваги.

- Частково безкоштовна версія;
- можливість створення інтерактивних робочих листів;
- забезпечення формувального оцінювання;
- можливість використання готових робочих листів;
- урахування різних вікових та індивідуальних особливостей;
- автоматизована перевірка;
- економія часу;
- привабливий дизайн;
- спілка вчителів-предметників;
- інтуїтивно зрозумілий конструктор тестів.



3. Навчальний захід у режимі вебконференції

2. Недоліки.

- Англомовний та російськомовний інтерфейс;
- 14-денна пробна версія;
- обмежені можливості в безкоштовній версії.

MENTIMETER

1. Можливості та переваги.



- Безкоштовний сервіс;
- організація миттєвого опитування онлайн у реальному часі;
- створення питань із різними типами відповідей;
- анонімність відповідей;
- організація зворотного зв'язку;
- доступ із будь-якого пристрою.

2. Недоліки.

- Створення не більше двох питань у безкоштовній версії;
- англомовний інтерфейс.

3. НАВЧАЛЬНИЙ ЗАХІД У РЕЖИМІ WEBКОНФЕРЕНЦІЇ

Вебконференції дозволяють проводити онлайн-презентації, спільно працювати з документами й додатками, синхронно переглядати сайти, відео, файли та зображення.

Правила інформаційної безпеки під час проведення навчального заходу в режимі вебконференції

- Вебконференція в синхронному режимі організовується за умови неможливості опрацювання відповідного матеріалу в асинхронному режимі. Тривалість однієї сесії бажано обмежити до 40 хвилин.
- До початку конференції сформулюйте й ознайомте учасників із планом заходу, обговоріть необхідність попередньої підготовки, супровід заходу дорадчими інформаційними матеріалами.
- Заздалегідь підготуйтеся до вебзустрічі. Перевірте налаштування, протестуйте комп'ютер, інтернет, мікрофон, навушники та вебкамеру.

- У призначений час за 5 хвилин до початку увійдіть в онлайн-конференцію за отриманим посиланням від організаторів. Свій профіль назвіть своїм іменем і прізвищем.
- Організатору бажано використовувати «кімнату очікування», щоб уникнути приєднання до вебконференції сторонніх осіб.
- Запустивши вікно онлайн-конференції, закрийте інші.
- Заздалегідь визначтесь з організаторами щодо використання режиму аудіо чи відео, чи аудіо + відео. Режим спілкування для всіх учасників вебконференції однаковий.
- Без попередньої згоди не варто записувати вебконференцію.
- Перш ніж робити скрін екрана з учасниками, етично спитати дозволу.
- Дотримуйтеся правил проведення дискусії. За потреби натисніть на знак «підняти руку», спікер уведе вас в обговорення.
- Уникайте месенджерів під час конференції, адже багатозадачність виснажує.
- Під час виступу користуйтеся попередніми нотатками. Будьте лаконічними. Не витрачайте ресурс часу й уваги учасників вебконференції на загальні фрази.
- Дотримуйтеся лаконічного дрес-коду: однотонна сорочка, футболка.
- Заздалегідь потурбуйтеся про тло без сюрпризів. У Zoom можна не лише використати тло-заставку, але й застосувати розмитість навколо себе.
- Додайте актуальне фото у свій профіль. Це дасть ефект присутності, якщо вимкнено камеру.
- Для спілкування «не за темою» використовуйте внутрішній персональний чат.

Структура навчального заходу в режимі вебконференції

Підготовка: тема, мета, учасники дискусії, цільова аудиторія, спікери, формат зустрічі, заплановані застосунки. Укладання чек-листа із чітким таймінгом.

Основна частина: вступ, привітання, виступ — мотивація почесного гостя, повідомлення теми, мети зустрічі.

3. Навчальний захід у режимі вебконференції

Координувальна робота спікера в організації виступів і проведенні дискусії.

Підсумок: підбиття підсумків, резюме виступів і дискусії. Визначення перспектив теми вебконференції. Інформування учасників щодо сервісів і можливостей зворотного зв'язку.

Сервіси для проведення вебконференцій

1. Google+ Hangouts
2. Facebook Live
3. YouTube Live
4. Skype Group Calls
5. Cisco Webex
6. Blackboard Collaborate
7. GoToWebinar
8. Livestream
9. WebinarJam
10. EverWebinar
11. Zoom
12. ClickMeeting
13. Demio
14. Livestorm
15. WebinarNinja

Інформаційна безпека майданчиків зворотного зв'язку

Зворотний зв'язок (англ. — *feedback*) постійний, цілеспрямований процес взаємодії всіх учасників навчання, спрямований на отримання інформації про хід та результати навчальної діяльності та розробки на її основі коригуючих дій з удосконалення навчання.

Формати онлайн зворотного зв'язку

- Чат.
- Форум.
- Блог.
- Відеоконференція.
- Електронна пошта.

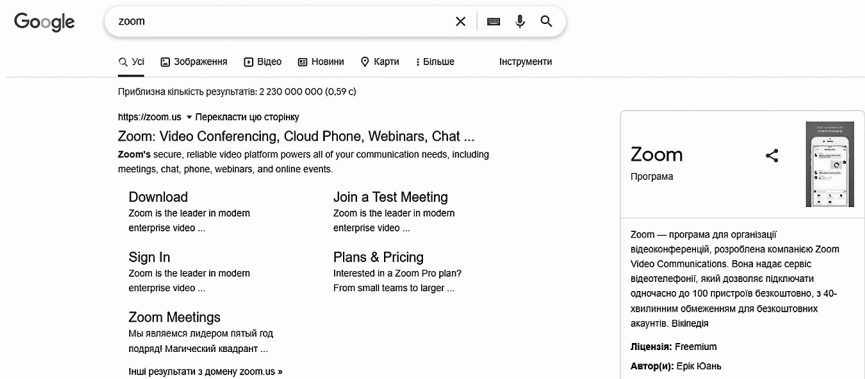
Поради з інформаційної безпеки

- Брати участь в обговоренні під своїм іменем.
- У коментарях бути лаконічним, відповідати суто за заявленою для обговорення темою.

- Перш ніж писати коментар-запитання, подумайте, чи можете самостійно знайти відповідь, аргумент, доведення. Якщо так, зробіть це, не відволікаючи увагу інших.
- Намагайтеся під час спілкування за допомогою чату зберігати стабільно врівноважений емоційний стан. Учїться стримуватися від емоційних коментарів.
- Під час участі в обговоренні теми форуму спершу перегляньте дописи учасників. Свій коментар залишайте за умови, якщо пропонуєте якісно нове бачення обговорюваної теми.
- Дописи краще писати безособовими, простими реченнями.
- Якщо не впевнені в цінності своєї думки для всіх, краще скористайтеся адресним меседжем.
- Не поширюйте неперевірену на достовірність інформацію.

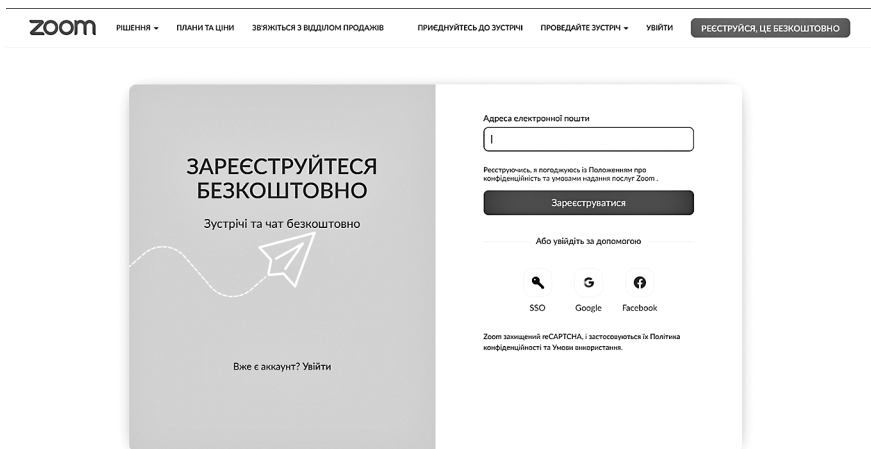
АЛГОРИТМ-ПРАКТИКУМ СТВОРЕННЯ ВІДЕОКОНФЕРЕНЦІЇ НА СЕРВІСІ ZOOM

Крок 1. У пошуковій стрічці GOOGLE написати ZOOM та перейти за першим посиланням <https://zoom.us/>. Завантажити програму можна на офіційному сайті Zoom. Платформа доступна для операційних систем Windows, MacOS, Android та iOS і має плагін, який дозволяє використовувати Zoom у браузерях Google Chrome та Mozilla Firefox.



3. Навчальний захід у режимі вебконференції

Крок 2. Натиснути в правому верхньому куті «Зареєструватися безкоштовно» та ввести свою адресу електронної пошти або увійти через акаунти Google, Facebook. Після реєстрації відкриється головна сторінка сервісу. Безкоштовна версія програми дозволяє проводити відеоконференцію тривалістю 40 хвилин. Можна використовувати додаток на комп'ютері, планшеті чи смартфоні.



Крок 3. На головній сторінці для створення нової відеоконференції натиснути →, після чого написати тему відеоконференції, обрати дату та час її проведення. Ідентифікатор конференції можна створювати автоматично або обрати власний (персональний). Після цього натиснути «Зберегти». Відеоконференцію можна запланувати заздалегідь, а також зробити посилання для постійних зустрічей у певний час.

До створеної відеоконференції можна підключитися за посиланням або ідентифікатором конференції. Для цього його потрібно скопіювати, натиснувши «Копіювати запрошення», та надіслати учасникам у будь-який зручний спосіб (Viber, E-mail, Telegram, Messenger), окрім загальнодоступних ресурсів.

Для уникнення підключення до конференції сторонніх осіб слід дозволяти приєднання лише зареєстрованим користувачам, користуватися налаштуванням «Кімната

очікування», оскільки організатор зможе підтвердити кожного учасника для приєднання до відеоконференції.

Надіслати запрошення на відеоконференцію її учасникам.

4. ШКОЛА В СМАРТФОНІ. ОСВІТНЯ ПЛАТФОРМА HUMAN

Усі учасники освітнього процесу, які підключені до HUMAN, можуть швидко зв'язатися один з одним, адже всі потрібні контакти автоматично з'являються у їхній базі. Їхнє спілкування здійснюється на безпечному рівні у єдиній захищеній системі школи. Сторонні особи не матимуть доступу до особистих даних дитини та не зловживатимуть їхньою довірою.

Доступ до платформи

Доступ до платформи здійснюється через вебсайт [id.human.ua], доступ до функціональних площадок може здійснюватися через вебсайт платформи¹.

Здійснивши реєстрацію на платформі шляхом надання необхідної для реєстрації інформації, у тому числі персональної, та висловлення своєї згоди з умовами та положеннями запропонованих до вашого обов'язкового ознайомлення документів, зазначених далі в реченні, підтверджуючи її встановленням позначки «галочка» та натисканням кнопки «Зареєструватися», ви підтверджуєте, що прочитали ці умови, додатки, а саме ліцензійний публічний договір, політику конфіденційності, політику файлів куки (Cookie) та прийняли їх положення, здійснюючи такі дії.

Якщо ви у будь-який момент не погоджуєтеся із цими умовами, ви не маєте права користуватися платформою і повинні негайно залишити її та видалити свій акаунт.

Платформа — сукупність пов'язаних між собою електронної (цифрової) інформації, спеціалізованого програмно-

¹ human Умови та правила використання. [Електронний ресурс]. — Режим доступу : <https://help-center.human.ua/en/articles/3840451> (дата звернення 15.07.2021).

го забезпечення, прикладних програм, виражених у вихідному та/або об'єктному кодах серверної частини (бек-енд), клієнтської частини (фронт-енд) та інших програмних частин, дизайну, графічних елементів, текстів, описів, схем, баз даних, комп'ютерних програм, що разом утворюють онлайн-платформу під назвою «Human», доступ та використання якої може здійснюватися лише на умовах, визначених ТОВ «Х'ЮМАН» — власником авторських та майнових прав, за допомогою вебсайту платформи [id.human.ua].

Користування платформою — усвідомлене та вільне волевиявлення користувача, що проявляється у використанні технічних можливостей та послуг платформи, не заборонених цими умовами.

Один із батьків або законний представник — фізична особа, яка відповідно до законодавства України визнається як така та має нести відповідні, установлені законодавством, обов'язки, щодо виховання та забезпечення дитини. Законним представником може бути особа, яка відповідає вимогам, установленим законодавством України, та має офіційний статус законного представника дитини, зокрема, один з її батьків, усиновлювачів, опікунів, піклувальників. Цей термін не позбавляє всіх батьків або законних представників дитини їхніх прав та обов'язків щодо своєї дитини на платформі, радше за все, цей термін установлює мінімальні вимоги згоди одного з батьків або законного представника, якщо це не суперечить чинному законодавству України.

Учень (може вживатися термін «дитина») — фізична особа, яка навчається та виховується в закладі середньої освіти; є відповідним користувачем онлайн-школи.

Профіль — створений Адміністратором обліковий запис всередині онлайн-школи, до якого підключається користувач за допомогою коду.

Код — унікальний та особистий набір знаків (код), який автоматично генерується при створенні адміністратором профілю та за допомогою якого відбувається підключення користувача до відповідного профілю, створеного адміністратором онлайн-школи.

Реєстрація акаунту

Для того щоб підключити профіль до акаунту користувача або створити онлайн-школу, вам треба спочатку створити акаунт. Ви приймаєте ці умови в момент створення акаунту.

У момент створення акаунту ви маєте ввести потрібну для реєстрації інформацію, яка має відповідати дійсності, а саме: ім'я, прізвище, електронну пошту, запропонований вами пароль, та прочитати й прийняти ліцензійний публічний договір, угоду й інші додатки та натиснути кнопку «Зареєструватися».

Діти не мають права реєструвати акаунт. Натомість один із батьків або законний представник дитини має зареєструвати акаунт замість дитини.

Кожен підключений користувач онлайн-школи має належати до категорії, що має відповідати його реальному статусу. Залежно від ролі такого користувача він/вона мають різні права та обов'язки, доступні послуги та технічні можливості на платформі.

Якщо через обставини в реальному житті роль користувача онлайн-школи змінюється або більше не підходить під опис однієї з ролей, такий користувач має повідомити про це адміністратора онлайн-школи не пізніше 7 календарних днів після такої зміни. Позбавлення будь-якої ролі не призводить до втрати акаунту.

Діти не мають права самотужки підключити профіль до свого акаунту. Натомість батьки або законний представник, зареєструвавши акаунт своєї дитини та підключивши відповідний профіль учня до акаунту за допомогою коду, що був наданий одному з батьків або законному представнику адміністратором після надання згоди на обробку та передачу даних адміністратору та виконання ним усіх необхідних додаткових супутніх дій, один із батьків або законний представник завершує процес підключення учня до онлайн-школи.

ТОВ «Х'ЮМАН» не несе відповідальності за реєстрацію та підключення до онлайн-школи дітей, яка була здійснена без відома та згоди одного з батьків або законних представників. ТОВ «Х'ЮМАН» не несе відповідальності за

отримання персональних даних від особи, яка не мала права самостійно надавати їх, натомість ви є цілком відповідальними за такі дії.

Кожний користувач, а у випадку дитини — її батьки або законні представники, є повністю відповідальними за збереженість коду користувача. Код, наданий адміністратором, є необхідним та достатнім для підключення профілю до акаунту користувача на платформі. ТОВ «Х'ЮМАН» не несе відповідальності за дії та їх наслідки, учиненні третіми особами, що в будь-який спосіб отримали код будь-якого користувача без провини ТОВ «Х'ЮМАН».

У разі виявлення помилки в заповнених адміністратором даних при генерації коду користувач або його законний представник має звернутися до адміністратора та попросити виправити помилку або помилки. Адміністратор має протягом 30 днів виправити помилки.

Права одного з батьків або законного представника на платформі:

- коментувати інформацію, пов'язану з процесом виховання та навчання в закладі освіти;
- перегляди домашнє завдання, оцінки, відвідуваність, розклад, результати навчання своєї дитини;
- звертатися за роз'ясненнями до вчителя;
- звертатися із запитом про зміну даних учня до адміністратора та працівників платформи;
- звертатися до платформи для отримання необхідної аналітики, пов'язаної з процесом здобуття освіти та виховання учня;
- мати доступ та користуватися всіма функціями доступних для них стрічок;
- користуватися всіма іншими можливостями, наданими платформою.

Права учня на платформі:

- коментувати інформацію, пов'язану з процесом виховання та навчання в закладі освіти;
- переглядати своє домашнє завдання, оцінки, розклад, відвідуваність, результати навчання;

- виконувати необхідні завдання курсів та здійснювати визначену вчителем діяльність із курсів;
- брати участь в опитуваннях, вікторинах та інших заходах, що відбуваються на платформі;
- мати доступ та користуватися всіма функціями доступних учневі стрічок;
- звертатися за роз'ясненнями до вчителя;
- користуватися всіма іншими, наданими платформою, функціями.

Діти можуть використовувати профіль користувача, створений адміністратором, відповідно до наданої попередньої згоди одного з батьків або законних представників та під наглядом одного з батьків або законного представника. У випадку, якщо ви дозволите вашій дитині використовувати платформу, її послуги та технічні можливості, ви розумієте та погоджуєтесь, що будете нести відповідальність за таке використання вашою дитиною в межах, визначених чинним законодавством України.

ТОВ «Х'ЮМАН» надає користувачу право в межах технічних можливостей платформи надавати, завантажувати, публікувати або будь-яким іншим способом робити доступними для платформи та користувачів, текстові, фото-, аудіо-, відеоматеріали та будь-яку іншу інформацію, включаючи пов'язані з послугами коментарі, відгуки, обмін ними між користувачами (надалі — «користувацький контент»). Формат та предмет завантаження користувацького контенту буде визначений ТОВ «Х'ЮМАН».

Користувач погоджується не надавати користувацький контент, який заборонений цими умовами та не відповідає законодавству України.

ТОВ «Х'ЮМАН» не надає гарантії, що весь користувацький контент буде опублікований на платформі, ТОВ «Х'ЮМАН» залишає за собою право, але не зобов'язує себе переглядати, моніторити або видаляти будь-який користувацький контент без повідомлення користувача, у тому числі у випадках, якщо такий користувацький контент може порушувати або порушує права інтелектуальної власності третіх осіб та законодавство України.

Використовуючи або отримуючи доступ до платформи або послуг, користувач погоджується, що ТОВ «Х'ЮМАН» може збирати й використовувати користувацький контент на платформі та відповідну інформацію згідно із цими умовами. Користувач також визнає та погоджується, що така інформація про нього може бути використана ТОВ «Х'ЮМАН» відповідно до цих умов, ліцензійного публічного договору та чинного законодавства України.

Усім користувачам заборонено такі форми користування платформою:

- порушувати чинне законодавство України;
- для будь-якої образливої, шахрайської та / або іншої незаконної діяльності;
- для булінгу, приниження людської гідності і дій, що можуть трактуватися як такі;
- для передачі, зберігання та/або публікації нелегальних матеріалів (включаючи матеріали, які можуть уважатися нецензурними);
- користуватися платформою в будь-яких комерційних цілях, якщо інше не встановлене цими умовами;
- видавати себе за іншу людину або свідомо розміщувати неправдиві дані;
- порушувати права та норми охорони інтелектуальної власності згідно із цими умовами та/або чинного законодавства України;
- давати в користування свій акаунт та / або акаунт будь-якій іншій особі, якщо інше не встановлено цими умовами, або без попередньої письмової згоди ТОВ «Х'ЮМАН»;
- чинити будь-які дії, що мають на меті отримання не-санкціонованого доступу до акаунту;
- чинити будь-які дії, що мають на меті заволодіння конфіденційною інформацією проти волі користувача;
- запускати будь-які форми автовідповідача або «спам»;
- запускати процеси «сканування» або «павутиння»;
- розміщувати та поширювати будь-яку інформацію або програмне забезпечення, яке може бути використане для

злому комп'ютерних систем або містить комп'ютерні віруси або інші компоненти, що прирівнюються до них;

- розміщувати та поширювати контент візуального характеру для перегляду учнями, який має загальну безперервну тривалість понад 20 хвилин (для учнів 2–4 класів) та 30 хвилин (для учнів 5–12 класів);
- будь-яким способом перешкоджати штатній роботі платформи;
- інші дії, які заборонені цими умовами, або такі, які не дозволені платформою, її послугами та технічними можливостями і є такими, які об'єктивно будуть суперечити цілям та предмету цих умов.

Вилучення або видалення профілю / акаунту з платформи

Користувач може бути вилучений із платформи на деякий час, що означає блокування можливості користування платформою, або назавжди шляхом видалення його акаунту.

Вилучення акаунту користувача з платформи на деякий час або назавжди можливе, якщо:

- користувач умисно надав недостовірну інформацію під час реєстрації на платформі;
- користувач неналежно користувався та / або користується платформою, як зазначено в Розділі VIII «Заборонене користування платформою»;
- здійснює будь-які інші порушення цих умов та/або ліцензійного публічного договору;
- у будь-яких інших випадках, якщо ТОВ «Х'ЮМАН» вважає такі дії як потрібні та обґрунтовані.

Видалення профілю користувача можливе, якщо:

- школа припинила своє існування;
- школа відмовилася від користування платформою;
- користувач неналежно користувався та / або користується платформою, як зазначено в Розділі VIII «Заборонене користування платформою»;
- персональні дані користувача були незаконно передані ТОВ «Х'ЮМАН», наприклад без відповідної згоди користувача.

Для того щоб редагувати чи видалити персональні дані, що стосуються вашого профілю, ви маєте звернутися до адміністратора з клопотанням про видалення, який є відповідальним за ведення та адміністрування персональних даних користувачів на платформі, як зазначено в згоді на передачу та обробку даних між вами та адміністратором. Адміністратор має видалити ваш профіль та всі ваші персональні дані протягом 7 днів із моменту вашого звернення. Якщо адміністратор не видалив ваш профіль вчасно, будь ласка, зверніться до ТОВ «Х'ЮМАН», написавши листа на [support@human.ua] для задоволення такого запиту.

Користувач може видалити свій акаунт у будь-який момент. Видалення акаунту будь-яким чином буде означати розірвання ліцензійного публічного договору.

Перед реєстрацією на освітній платформі Х'ЮМАН важливо ознайомитися з політикою конфіденційності.

5. КОРОТКИЙ СЛОВНИК ТЕРМІНІВ

Відеоконференція (Desktop Videoconferencing) — зустріч, методичне засідання або розмова партнерів, які перебувають у різних місцях та використовують відеотехнології як основний канал зв'язку. При цьому надається двосторонній звук та одно або двостороннє відео.

Віртуальний клас — це співтовариство двох або більшої кількості людей (здобувачів освіти й учителів / тьюторів), присутніх у віртуальному класі, які відповідно до обраної навчальної мети здійснюють навчальну діяльність (зокрема навчальні комунікації) у середовищі системи віртуального навчання.

Дистанційна форма здобуття освіти — це індивідуалізований процес здобуття освіти, який відбувається переважно за опосередкованої взаємодії віддалених один від одного учасників освітнього процесу в спеціалізованому середовищі, що функціонує на базі сучасних психолого-педагогічних та інформаційно-комунікаційних технологій.

Електронний підручник (посібник) — електронне навчальне видання із систематизованим викладом навчального матеріалу, що відповідає освітній програмі, містить цифрові об'єкти різних форматів та забезпечує інтерактивну взаємодію.

Електронні освітні ресурси з навчальних предметів (інтегрованих курсів) — засоби навчання на цифрових носіях будь-якого типу або розміщені в інформаційно-телекомунікаційних системах, які відтворюються за допомогою електронних технічних засобів і можуть застосовуватися в освітньому процесі під час вивчення окремих освітніх компонент (інтегрованих курсів).

Контент (з англ. *content* — зміст) — це інформаційне наповнення сайту, медіа та текст (різноманітна інформація) у різних форматах. Для користувача дистанційного курсу це все, що є на сайті: текстовий зміст, зображення, аудіо, відео та інші файли будь-яких розширень. Для користувача контент може бути представлений для перегляду, скачування або інших дій.

Мобільне навчання — це можливість отримувати навчальні матеріали на персональні пристрої та виконувати за їх допомогою певні дії з навчальним матеріалом для його засвоєння.

Онлайн — стан суб'єкта чи об'єкта, який в конкретний момент має доступ до інтернету в режимі реального часу. Переклад українською: «на лінії», «на зв'язку», «у мережі», «наживо», «вмережно».

Офлайн (англ. *offline*) — використовується в значенні «відключений, автономний». Це стан, коли відсутня можливість відкритого двостороннього спілкування користувачів або служб. Наприклад, офлайн може бути периферійне устаткування, що не підключене до вашого комп'ютера або поза зоною доступу для зв'язку з іншими користувачами. Тобто, не підключаючись до інтернету (у режимі офлайн), можна подивитися інформацію дистанційного курсу, що була заздалегідь завантажена із сайту на власний комп'ютер (у режимі онлайн).

Суб'єкти дистанційного навчання — здобувачі освіти та педагогічні працівники, які беруть участь в освітньому процесі за дистанційною формою здобуття освіти та / або з використанням технологій дистанційного навчання.

Технології дистанційного навчання — комплекс освітніх, інформаційно-комунікаційних (цифрових) технологій, що дають можливість реалізувати процес дистанційного навчання в закладах освіти.

Тьютор (tutor — учитель) — особа, що веде індивідуальні або групові заняття, наставник.

Цифрове освітнє середовище — сукупність умов навчання, виховання та розвитку здобувачів, що забезпечуються за допомогою сучасних освітніх, інформаційно-комунікаційних (цифрових) технологій.

Навчальне видання
ДОЦЕНКО Світлана Олексіївна,
ВОРОЖБИТ-ГОРБАТЮК Вікторія Вікторівна,
СОБЧЕНКО Тетяна Миколаївна

Навчально-методичний посібник
**«Онлайн-безпека учасників освітнього процесу
в умовах дистанційного і змішаного навчання»**

Схвалено для використання в освітньому процесі

Видано за рахунок державних коштів. Продаж заборонено

Редактор *О. В. Костіна.*
Технічний редактор *С. В. Яшиш.*
Коректор *Н. В. Красна.*

Підписано до друку 06.12.2021. Формат 60×90/16.
Папір офсетний. Гарнітура Шкільна.
Друк офсетний. Ум. друк. арк. 12,00. Обл.-вид. арк. 7,40.
Тираж 43 702 прим. Зам. № 2111-2021.

ТОВ Видавництво «Ранок»,
вул. Кібальчича, 27, к. 135, Харків, 61071.
Свідоцтво суб'єкта видавничої справи ДК № 5215 від 22.09.2016.
Адреса редакції: вул. Космічна, 21а, Харків, 61165.
E-mail: office@ranok.com.ua. Тел. (057) 701-11-22.

Навчально-методичний посібник
надруковано на папері українського виробництва

Надруковано у друкарні ТОВ «ТРИАДА-ПАК»,
пров. Сімферопольський, 6, Харків, 61052.
Свідоцтво суб'єкта видавничої справи ДК № 5340 від 15.05.2017.
Тел. +38 (057) 712-20-00. E-mail: sale@triada.kharkov.ua

ОНЛАЙН-БЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ В УМОВАХ ДИСТАНЦІЙНОГО І ЗМІШАНОГО НАВЧАННЯ

Онлайн-безпека в інформаційному суспільстві є одним з основних напрямів фундаментальних досліджень у сфері інформаційних технологій, які використовуються під час вивчення практично всіх шкільних дисциплін.

Отже, сучасний учитель повинен знати основні принципи безпеки у професійній діяльності, уміти користуватися засобами кібербезпеки електронних освітніх ресурсів для навчання з урахуванням психолого-педагогічних особливостей учнів.

Запропоновані в цьому посібнику теоретичні матеріали, інструкції, лайфхаки, практичні завдання допоможуть учителям захиститися від кібератак.

ВИДАВНИЦТВО
РАНОК



ISBN 978-617-09-7625-3



9 786170 976253



i Інтернет-
підтримка

за QR-кодом
або посиланням
mnk.com.ua/100862