

Раніше люди взаємодіяли в кількох середовищах: земля, вода, повітря. З появою інтернету з'явився ще один вимір – кіберпростір. Ідеться про мережу взаємопов'язаних між собою пристроїв. Загалом безпека – це стан захищеності від зовнішніх і внутрішніх загроз. А безпека в кіберпросторі – ваша особиста захищеність та безпека ваших пристроїв.

Так тлумачить це поняття фахівець із кібербезпеки **Олексій Барановський**, який працює в ІТ-компанії Intellias.

Журналістка “Нової української школи” поговорила з Олексієм про те, які ризики існують для дітей в інтернеті, яких правил варто дотримуватися в кіберпросторі та про що саме варто говорити з дітьми з цієї теми і з якого віку.

РИЗИКИ ДЛЯ ДІТЕЙ У КІБЕРПРОСТОРІ

“Нині відключений від мережі пристрій – це ніщо, він не має сенсу. Цінність з'являється, коли він стає частиною загальної великої мережі девайсів / гаджетів із доступом до різноманітних сервісів. Усі вони спрямовані на покращення нашого життя чи задоволення певних потреб. Ідеться про мережу інтернет”, – починає Олексій.

Він пояснює: якщо з реальним життям ми взаємодіємо безпосередньо – за допомогою п'яти чуттів, то **в нового виміру є особливості – ми взаємодіємо з ним через посередника**. Наприклад, цю розмову ми вели через посередника – телефон. Звідси виникає хибне відчуття захищеності.

Найбільша проблема кіберпростору така: у пересічних громадян є відчуття, що у випадку загрози вони можуть просто розв'язувати цю проблему, вимкнувши цей-таки телефон чи комп'ютер. Утім, ця думка – хибна. Тож ми маємо розуміти правила поведінки в кіберпросторі та навчитися з цим жити.

“Насправді ми маємо перенести до кіберпростору ті самі правила, якими користуємося в житті. Наприклад, мити руки, не спілкуватися з незнайомими людьми, “не тицяти каку”, прибирати за собою, бути ввічливими, перевіряти перед тим, як купувати тощо”, – пояснює фахівець.

Єдина різниця між цими правилами у звичайному житті та кіберпросторі полягає в тому, що **доступність вас як об'єкта збільшилася**. Тобто, з одного боку, утворився новий цікавий простір, а з іншого – попри оманливе відчуття безпеки, ви стали доступними для всіх.

“Коли ви купуєте дитині телефон, уявіть, що вона поринає в цей уявний простір, а там – цукерки перемішані з брудом, безліч поганців та вірусів. І це все треба вміти фільтрувати. Сучасна людина має значно більше викликів у кіберсвіті. Зокрема, в інтернеті діти можуть піддаватися трьом найголовнішим

*загрозам: **шахрайству, вимаганню та цькуванню**”.*

З ЯКОГО ВІКУ ГОВОРИТИ З ДИТИНОЮ ПРО КІБЕРБЕЗПЕКУ ТА ЯКІ ПРАВИЛА ВСТАНОВИТИ

Олексій радить починати говорити з дітьми про кібербезпеку одразу, коли ви даєте їм користуватися телефоном чи комп'ютером. У когось це може бути в 3 роки, у когось – у 7. Однак треба врахувати, що дитина, яка не має гаджета, може контактувати з тими, у кого він є. І тоді про це також треба говорити.

“Залежно від віку, ми можемо розповідати дітям, які ризики є й чому вони саме такі. Кожен етап розповіді відповідатиме етапу розуміння дитини. Наприклад, коли дитина розуміє цінність грошей, можна говорити про інтернет-банкінг і чому треба ставити надійний пароль. Коли дитина розумітиме цінність приватної інформації, можна говорити з нею про це”, – радить Олексій.

Як учителі, так і батьки можуть обговорити з дітьми такі правила в кіберпросторі:

- **Ти спілкуєшся не з пристроями, а все ж таки з людьми через пристрій.** На іншому боці може бути хто завгодно, навіть якщо тобі пише хтось, хто здається знайомим.
- **Те, що ти розмістиш в інтернеті чи відправиш у повідомленні, автоматично стає не твоїм.** Тому треба донести дитині, що таке цінна інформація та чому її не варто нікому надсилати.

- **Усе, що ти отримав, але не очікував отримати, – підозріло.** Тебе можуть обманути.
- **Безплатний сир – лише в мишоловці.** Гроші просто так не даються. Якщо в тебе є потреба в грошах, краще скажи про це дорослим, яким довіряєш.
- Якщо ти в чомусь сумніваєшся, **проконсультуйся зі мною**, дорослим.
- Ще одним правилом може бути, наприклад, не натискати (або не тицяти) на сайти з доменом “.ru”.

“Це про культуру виключення. Лише вихованням і прикладом треба показати дитині, що це не міститиме для неї жодної цінності. “Ми тобі не забороняємо, а радимо””, – пояснює Олексій.

У деяких школах викладають предмети – кібербезпеку чи кібергігієну, і це – метод достукатися одразу до багатьох дітей. Також цю тему можна інтегрувати в інші предмети, як-от безпека життєдіяльності, окремі факультативи чи курси.

ПРО ВАЖЛИВІСТЬ ВЗАЄМИН У ТЕМІ КІБЕРБЕЗПЕКИ

Основою цих правил є довіра дитини до дорослого. Якщо дорослі не вибудували довірливі взаємини з дитиною, усе це не матиме сенсу.

“Треба розуміти, що кіберсвіт пришвидшив певні процеси. Раніше, навіть якщо дитина не довіряла батькам, не було таких ризиків, варіантів, небезпек. Тому питання довіри зараз стає значно важливішим, ніж раніше”, – говорить Олексій.

Також роль грає приклад дорослих. Якщо батьки показуватимуть приклад, які паролі ставити, як бути захищеними, чому не можна натискати на ті чи інші посилання, дитина братиме з них приклад.

Ще одна важлива річ у взаєминах у темі кіберпростору – **дорослі мають визнавати свої помилки та пояснювати все на реальних прикладах.** Можна обговорювати цю тему з дитиною, застосовуючи власні приклади.

“Наприклад, визнавати, що я перейшов за якимось посиланням, мій браузер зламали й кожне наступне натискання вело мене на заборонений контент.

Або так – людина натиснула на неперевірене посилання, й у неї вкрали гроші. Або під час війни дітей використовують як навідників чи людей, які ставлять мітки.

Наприклад, нам у школі в 90-х роках розповідали про “Біле братерство” – це релігійна секта, у яку набирали людей, зокрема дітей. Саме так учителька нас попереджувала. Тобто попереджений – озброєний”, – говорить Олексій.

До того ж дитина має переживати будь-яку тему через те, що для неї має цінність. Наприклад, якщо це маленька дитина – через історію з улюбленою іграшкою.

ПРО ЗАБОРОНИ

Соцмережі та месенджери мають вікові обмеження, які батьки часто ігнорують. Наприклад, до 13 років діти мали б дивитися YouTube Kids, у Telegram можна реєструватися з 16 років, у Viber – з 13 тощо.

“Ігнорувати запобіжники й думати, як убезпечити дитину від кіберпростору, – це наче думати, як вберегти дитину від алкоголізму, якщо батьки самі їй наливають. Буває, штучний інтелект моніторить активність, підозрює, що дитині менше дозволеного віку і блокує її обліковий запис. Однак я вважаю, якщо батьки не можуть опікуватися дитиною, це має робити суспільство. Можна жалітися на такий обліковий запис. Якщо ви побачите дитину, яка п’є горілку надворі, ви ж зробите їй зауваження чи захочете поспілкуватися з її батьками”, – говорить Олексій.

Також він розповідає про програми так званого батьківського контролю чи інші додатки, у яких батьки бачать активність дитини в інтернеті. Однак це, знову ж таки, діє лише на основі довіри.

“Батьківський контроль працюватиме, якщо дитина це сприйме та їй пояснять, чому це саме так і чому це треба. Адже діти можуть вигадати мільйон методів, як обійти батьківський контроль. Треба донести дитині важливість. Мовляв, дивись, ми не хочемо тебе обмежити – ми хочемо тебе попередити й убезпечити”, – говорить фахівець.

ЯКІ МАТЕРІАЛИ МОЖУТЬ ДОПОМОГТИ НАВЧИТИ ДІТЕЙ ПРАВИЛ КІБЕРБЕЗПЕКИ

У пригоді стануть:

1. **Блог “Хакер, що біжить”**, який веде експерт із кібербезпеки **Володимир Стиран**. Він ділиться досвідом і дає корисні поради. Наприклад, [тут](#) і [тут](#) він описує загальні та детальні правила, як не стати кібержертвою.

Ідеться про підозрілі посилання та пристрої, як вигадати надійний пароль, чому його варто тримати в секреті, навіщо потрібна двофакторна автентифікація, які месенджери безпечні, як працює шифрування даних, чому потрібно встановити антивірус, навіщо робити резервні копії, що таке мобільна безпека та як із нею бути тощо.

0. **Онлайн-курс “Основи кібербезпеки для школярів”**, створений CRDF Global в Україні у співпраці з ГО “Смарт Освіта” та Technomatix. Він повністю безплатний та скоро буде у відкритому доступі. Слідкуйте за оновленнями на сайті “Нова українська школа” – ми повідомимо, як тільки він стане доступним.

Цей курс допоможе відрізнити правду від фейків, розкаже, з ким спілкуватися в інтернеті безпечно, а хто – насправді кіберзлочинець.

А ще під час проходження курсу діти дізнаються про те, як захистити гаджет, як шукати безпечні відео та інформацію в інтернеті, якою інформацією можна ділитися, про SMS-шахрайство, цифрові сліди, онлайн-ігри та офлайн-проблеми, безпеку комп’ютера, фейки і як їх розпізнати, як захистити інформацію, про що розповідають акаунти, більше про соціальні мережі, загрози інформаційного простору, соціальну інженерію, заробіток в інтернеті, онлайн-ігри, основні помилки користувачів та можливі наслідки, типи шкідливих програм, основні правила захисту інформації, що робити, якщо кіберзлочин усе-таки стався, та багато іншого.

Уся інформація подається через цікаві слайд-шоу, відео, інтерактиви, вправи та практичні завдання, максимально наближені до реальних ситуацій. Курс поділений на групи: для дітей 1–4, 5–6, 7–9 і 10–11 класів. Наприкінці учасники отримають сертифікати, що засвідчить їхні знання з кібербезпеки.

Марія Марковська, “Нова українська школа”

Титульне фото: автор – [NatashaFedorova](#), [Depositphotos](#)

Курс “Основи кібербезпеки для школярів” розроблено CRDF Global в Україні у співпраці з ГО “Смарт Освіта” та технічними експертами компанії Technomatix, за підтримки Державного департаменту США (Офіс із координації допомоги Європі та Євразії).