Міністерство освіти і науки України
Дніпровський педагогічний коледж КЗВО
«Дніпровської академії неперервної освіти
Дніпропетровської обласної ради»

Навчальний предмет Інтегрований курс «Громадянська освіта»

Тема Приватність та конфіденційність у віртуальному світі.

Лекція

Галузь знань: 01 Освіта

Рівень підготовки – базова загальна середня освіта

Дошкільне відділення. *Спеціальність 012 Дошкільна освіта*

Шкільне відділення. *Спеціальність 013 Початкова освіта*

Музичне відділення.

Спеціальність 014.13 середня освіта (музичне мистецтво)

Розроблено викладачем: О. С. Коваль
Розглянуто та затверджено
на засіданні циклової комісії суспільних дисциплін
Протокол № ___ від _____ р.
Голова циклової комісії ____В. В. Золотарьова

Міністерство освіти і науки України
Дніпровський педагогічний коледж КЗВО
«Дніпровської академії неперервної освіти
Дніпропетровської обласної ради»

Навчально – методична карта заняття № 25-26

Назва та № спеціальності 012 Дошкільна освіта, 013 Початкова освіта, 014.13 середня освіта (музичне мистецтво)

Рівень підготовки базова загальна середня освіта

Навчальний предмет Громадянська освіта

Тема **Приватність та конфіденційність у віртуальному світі.**

Тип заняття: **Лекція**

Мета заняття ***навчальна*** – розкрити поняття віртуальний світ, приватність, конфіденційність, зазначити сфери використання віртуальної реальності; охарактеризувати шляхи захисту своєї приватності, конфіденційної інформації; ***розвиваюча*** – розвивати мислення, навички критичного мислення, мовлення, пам'ять студентів, увагу та вміння сприймати лекційний матеріал; ***виховна*** – виховувати взаєморозуміння, терпимість, поважне ставлення до людської гідності, поглядів, засобів передачі інформації.

Забезпечення заняття:
**** роздатковий матеріал***
підручники, інформаційні технології

**** ТЗН***
Ноутбук, мультимедійний проектор, екран

ХІД ЗАНЯТТЯ

І. ВСТУПНА ЧАСТИНА

- організація студентів;
- повідомлення теми та мети лекції;
- запис теми, плану, літератури.

ІІ. ОСНОВНА ЧАСТИНА

Мотивація навчальної діяльності.

Є такий афоризм: ***«Ми повинні знайти баланс між недоторканністю приватного життя і використанням даних в рамках громадської безпеки. Інтернет є одним з найбільших глобальних продуктів. Якщо ми знищимо його, ми знищуємо багато чого з нашого економічного майбутнього.»***

Сатья Наделла, головний виконавчий директор корпорації Microsoft

Викладення матеріалу за планом

1. Поняття та характеристика віртуального світу.
2. Сфери використання віртуальної реальності.
3. Як правильно захистити свою приватність. Поради, які допоможуть зберегти Вашу конфіденційну інформацію.

Література

Базова

1. Бакка Т. В., Марголіна Л. В., Мелещенко Т. В. Інтегрований курс Громадянська освіта. Підручник для 10 класу заладів середньої освіти. Рівень стандарту. – Київ: Оріон, 2018.
2. Васильків І. Д., Кравчук В. М., Сливка О. А., Танчин І. З., Тимошенко Ю. В., Хлипавка Л. М. Громадянська освіта. Інтегрований курс, рівень стандарту: підручник для 10 класу закладів середньої освіти. – Тернопіль: Астон, 2018. - 296 с. : іл.
3. Громадянська освіта. Інтегрований курс. 10 клас. І семестр / Л. І. Валентій. – Харків: ВГ «Основа», 2018. – 112 с. (Серія «Мій конспект»)

Додаткова

1. http://isearch.kiev.ua/en/-searchpractice-en/-internetsecurity-ru/1777-online-safety-tips-to-help-keep-your-sensitive-information

ІІІ. ЗАКЛЮЧНА ЧАСТИНА

- закріплення вивченого матеріалу;
- відповіді на запитання студентів;
- підбиття підсумків;
- завдання для самостійної поза аудиторної роботи

СТРУКТУРА ЛЕКЦІЇ

Тема Приватність та конфіденційність у віртуальному світі.

План

1. **Поняття та характеристика віртуального світу.**
2. **Сфери використання віртуальної реальності.**
3. **Як правильно захистити свою приватність. Поради, які допоможуть зберегти Вашу конфіденційну інформацію.**

1. Поняття та характеристика віртуального світу.

Слово «віртуальний» походить від латинського virtus – римляни вживали його для позначення таких якостей воїна як мужність, хоробрість, рішучість. Нині ж англійське virtus означає доброчесність, чесноту.

Віртуальність **(**від лат. virtus – потенційний, можливий) – вигаданий, уявний (можливо, для деяких певних цілей) об'єкт, суб'єкт, ставлення, дія тощо, не присутній у цей час у реальному світі, а створений лише грою уяви людської думки, або зімітований з допомогою інших об'єктів.

Віртуальна реальність – штучно створене комп'ютерними засобами середовище, в яке можна проникати, змінюючи його зсередини, спостерігаючи трансформації і відчуваючи при цьому реальні відчуття.

Комп'ютерні технології відкрили перед людиною безпрецедентні можливості: розширення меж творчості, конструкторської діяльності, виникнення нових видів мистецтва, неможливих у фізичному світі. Використання комп'ютерних технологій значно полегшило трудову діяльність людини, забезпечило широкі можливості для самореалізації, освіти та самоосвіти. Завдяки мережі Інтернет людина вийшла за межі однієї країни, мови, культури. Виникла Homo Virtualis, людина, орієнтована на віртуальність, людина віртуальної культури.

2. Сфери використання віртуальної реальності.

Є велика кількість можливостей практичного використання цієї технології – віртуальної реальності (VR) в різних сферах. Хоча й окуляри віртуальної реальності зазвичай асоціюють саме з відеоіграми та розвагами, насправді їх застосовують навіть для лікування людей.

VR-можливості дуже широкі: абітурієнти можуть ознайомитися із своїми майбутніми університетами та прогулятися їхніми аудиторіями, навіть не виходячи з дому. Люди можуть на власні очі побачити точне відтворення квартир, які вони збираються придбати, та зайти в будь-яку кімнату ще до

початку будівництва. Будь-хто може стрибнути з парашутом або покататися на лижах, а діти навіть можуть опинитися в центрі самої казки перед сном та взаємодіяти з персонажами.

VR в медицині. Сьогодні за допомогою окулярів віртуальної реальності ви можете «пірнути» в людське тіло, ставши настільки маленьким, що зможете «зустріти» клітини. Ви можете побувати в будь-якому органі – наприклад, в мозку та вивчати його.

Є випадки, коли люди змогли подолати свій страх їздити в ліфті – вони робили це у віртуальній реальності, і потім самі були вражені, коли усвідомлювали, що без проблем можуть використовувати ліфт і в реальному житті.

VR в архітектурі та дизайні. Інколи навіть самі архітектори, дизайнери дивуються, побачивши свій проект «на власні очі» у віртуальній реальності і краще розуміють, що їм треба виправити чи переробити.

3. Як правильно захистити свою приватність.

Експерти стверджували, що у тих, хто використовував VPN для доступу до заблокованих соціальних мереж, були викрадені особисті дані, а VPN є не захистом приватності, а «дірою» у безпеці зберігання персональних даних. Незважаючи на блокування соціальних мереж, більше третини користувачів знайшли спосіб продовжувати користуватися цими ресурсами. Найбільш популярним варіантом обходу заборони стала технологія VPN.

Будь-яка відкрита точка доступу Wi-Fi мережі може призвести до потрапляння особистих даних до чужих рук. Підключаючись до публічної мережі, користувач не думає про те, що поруч може перебувати людина, яка зчитує дані з його гаджета. Рядовому користувачу може здаватися, що його приватна інформація навряд чи комусь потрібна, але практично кожен стикався зі зломом сторінок у соціальних мережах заради розсилки спаму. Тож, це не параноя – шахрайство в інтернеті стало реальною загрозою.

Механізм роботи. Основний принцип роботи VPN – це створення особистого віртуального «тунелю» в Інтернеті, який захищає канал передачі ваших даних від будь-якого зовнішнього втручання. Дані шифруються за певним алгоритмом, який практично неможливо зламати. Кожному користувачу замість реального, присвоюється IP-адресу іншої країни і всі сервіси розпізнають користувача за присвоєною VPN-ом геолокацією.

Основною програмою стеження за користувачами є програма Агентства Національної Безпеки США. Низка найбільших інтернет-компаній: Yahoo, Google, Facebook – співпрацюють у рамках цієї програми зі спецслужбами.

Захист власних даних, листування і приватності – це право на недоторканність приватного життя, яке є конституційним.

Приватність — це недоторканність приватного життя особи, невтручання в її особисту сферу. Як фундаментальне право людини, право на приватність закріплене в міжнародних і національних правових актах. Поряд із поняттям «приватність», «приватне життя», у них уживаються синонімічні терміни «***конфіденційність***» (лат. confidentia — довір'я) для позначення того, що не підлягає розголошенню, «таємниця особистого життя», «недоторканність приватного життя» та деякі інші.

Поради, які допоможуть зберегти Вашу конфіденційну інформацію.

Ввімкніть приватний перегляд. Багато інтернет-сайтів використовують такі технології, як cookie, щоб захопити IP-адреси конкретних комп'ютерів перед збиранням інформації про діяльність в Інтернеті.

Аби вирішити зростаюче занепокоєння з приводу того, що наше приватне життя під загрозою, основні веб-браузери, такі як Internet Explorer, Google Chrome і Mozilla Firefox мають функцію "приватний перегляд" в налаштуваннях своїх останніх релізів для забезпечення online безпеки.

Іншими словами, Ви можете запобігти зберігання cookie (а також інших деталей, таких як перегляд історії і тимчасові інтернет-файли) на своїх комп'ютерах, і тим самим зменшити ймовірність несанкціонованого збору інформації про те, як Ви подорожуєте в Мережі.

Така функція безпеки була надана в Safari 2.0 з 2005 року, Mozilla Firefox 3.1 і Google Chrome 1.0 в 2008 році та Internet Explorer 8 з 2009 року. Ввімкніть приватний перегляд в браузері (навіть на смартфоні) і це буде першою лінією оборони online безпеки.

Приховайте свою IP-адресу. У певному сенсі, Ваша IP-адреса як найчіткіший відбиток пальця в онлайн всесвіті. Для того, щоб скрити Вашу IP-адресу є сенс розглянути питання про використання веб-проксі, наприклад, таких сервісів як HideMyAss або відкритого інтернет-браузера Tor. Ці сервіси приховують інформацію, щоб Ви не залишали жодних слідів, незалежно від того, які сайти відвідуєте. Але треба мати на увазі, що деякі з таких веб-проксі мають сумнівну політику online безпеки і можуть самі мати доступ до даних, які Ви намагаєтесь приховати. Зробіть власне дослідження перед їх використанням. Бонусом веб-проксі або Tor є те, що Ви можете відвідувати сайти, які заблоковані Вашим інтернет-провайдером.

Не забувайте виходити. Ось тривожний факт про Facebook. Як пише Business Insider, Facebook може відстежувати онлайн-активність користувачів, які залишаються авторизованими у своєму обліковому записі Facebook. Це означає, що якщо Ви закрили вкладку Facebook, не натиснувши кнопку «вийти», і продивляєтесь інші сайти, які містять кнопку «like», то ці сайти можуть відстежувати і обробляти дані про Вашу діяльність (навіть якщо Ви не натискуєте на неї).

Також, інтернет-активність може контролюватися на різних платформах, так як на Ваш обліковий запис Facebook можна увійти за допомогою будь-якого пристрою, підключеного до Інтернету.

Такі інтернет-гіганти, як Facebook, Amazon і Google мають великі прибутки від реклами та інформації про нас, яку вони захопили. Це ще одна причина бути обережним, так як вони можуть тонко відняти у нас наше приватне життя і використовувати це для своєї вигоди.

Отже, не забувайте виходити зі своїх аккаунів у соціальних мережах, поштових клієнтах та іншого.

Остерігайтеся відкритих Wi-Fi точок доступу. Якщо Ви знайшли відкриту Wi-Fi точку, я би не радила швидко підключатися до неї. За замовчуванням, відкриті джерела Wi-Fi в зонах загального користування не мають шифрування, а це означає, що будь-хто поруч з Вашим місцем розташування, може записувати такі дані, які Ви передаєте онлайн, як Ваші паролі, банківські рахунки та електронні листи.

Захистіть себе! Є деякі основні запобіжні заходи які можна вжити, якщо Ви не готові відмовитися від зручності цих безкоштовних з'єднань Wi-Fi:

1. Вимкніть обмін файлами на пристрої або комп'ютері
2. Уникайте сайтів, де Вам потрібно вводити персональні дані, щоб увійти в свій обліковий запис (сайти, наприклад, соціальних мереж, електронної пошти або онлайн-банкінгу)
3. Якщо Вам необхідно використовувати електронну пошту, шифруйте її з SSL (Secure Sockets Layer) або TSL (Transport Layer Security)
4. Переконайтеся в тому, що Ви підключені до захищених каналів (адреси, що починаються з "HTTPS").
5. Щоб отримати максимальну безпеку в Інтернеті, створіть VPN (віртуальну приватну мережу)

Не забувайте й про деякі додаткові заходи безпеки при роботі в Інтернеті, бо лише весь комплекс цих нескладних рекомендацій допоможе Вам залишатися в безпеці.

Правила безпечної поведінки в інтернеті

1. Нікому не надавати особисту інформацію: домашню адресу, номери телефонів, робочу адресу батьків, адресу школи тощо.
2. Не погоджуватися на зустріч з людиною, з якою ви познайомилися в Інтернеті.
3. Не посилати свої фотографії чи іншу інформацію незнайомим людям.
4. Не відповідати на грубі листи.
5. Не давати нікому свої паролі.
6. Не робити протизаконних вчинків і речей в Інтернеті.
7. Не шкодити і не заважати іншим користувачам.

Обговоріть ці правила. Прокоментуйте їх. Доповніть список правил своїми пропозиціями.

Отже, варто пам'ятати, що в разі ігнорування належних засобів безпеки хтось може отримати доступ до ваших персональних даних. Однак не тільки власна приватність важлива в Інтернеті, але і приватність тих, хто поруч. Тому інформацією про інших людей можна поділитися, тільки якщо вона вже є в публічному доступі, при цьому не несе шкоди й не містить образ, або з дозволу особи.

Підбиття підсумків. Вправа «Коло вражень»

1. *Що нового я відкрила для себе ?*
2. *Чого не зрозуміла ?*

Домашнє завдання

1. Вивчити конспект.
2. Читати параграф 33.
3. Наведіть приклади ризиків, які несуть неконтрольовані обсяги інформації в Інтернеті.
4. Проаналізуйте власну поведінку як відповідального користувача соцмереж. Виправте недоліки, якщо виявите загрози чи ризики порушення вашої приватності та безпеки.