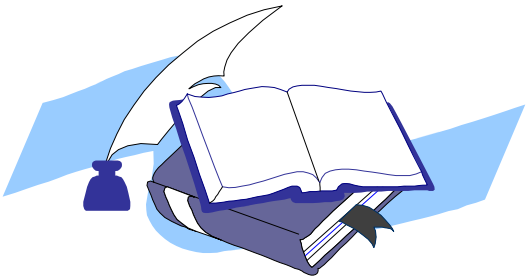
ІНФОРМАЦІЙНИЙ БЮЛЕТЕНЬ
№ 6, 2019



Інститут інформаційних технологій і засобів навчання НАПН України
Відділ компаративістики інформаційно-освітніх інновацій

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КОНФІДЕНЦІЙОСТІ ЯК АСПЕКТ ЦИФРОВОЇ КОМПЕНТНОСТІ УЧНІВ ТА ВЧИТЕЛІВ В УМОВАХ КОНС В ПРОЦЕСІ ВИХОВАННЯ ГРОМАДЯНИНА: ДОСВІД НІДЕРЛАНДІВ

Пріоритетами освіти і виховання громадянина у сучасному суспільстві, які визнані більшістю європейських країн та Україною, є цінності, проголошені Радою Європи, а саме: верховенство права, демократія та права людини. Освітні процеси сьогодні відбуваються у інформаційному цифровому світі і вимагають від педагогів компетентностей як у використанні ІКТ, так і у галузі громадянської освіти, які безпосередньо пов'язані з відповідальним ставленням, повагою до приватного життя, толерантністю та ін. У розвинених країнах Європи, а зокрема Нідерландах, існує певний досвід щодо розв'язання проблеми інформаційної безпеки та конфіденційності використання цифрових технологій, які застосовуються у школі. Найбільш гострі питання, що піднімаються голландськими освітянами, з якими стикається школа, це: обмін персональними даними, політика щодо паролів, кодекс поведінки для безпечного використання цифрових ресурсів та персональних даних, угоди про соціальні медіа, тощо. У звіті Національного конгресу з питань інформаційної безпеки та конфіденційності в галузі освіти, що пройшов у м. Ньювейген, Нідерланди, у 2019р., наголошується, що аспект інформаційної безпеки та конфіденційності – те , на чому має зосередитися сучасна школа. Як зазначають

експерти, легковірно та недостатньо відповідально поводяться у Інтернеті не тільки діти, а й вчителі, що пов'язане з недостатньою обізнаністю, технологічними аспектами та впровадженням політики школи щодо інформаційної безпеки та конфіденційності. Фішинг, який є однією із форм шахрайства в Інтернеті, визнаний учасниками конгресу найбільшою проблемою школи сьогодні. Прості паролі доступу, неуважність при натисканні кнопок, відкриваючи електронні листи чи посилання, надання особистої та фінансової інформації підробним веб-сайтам становить реальну загроза я особисту, так і для всієї школи. Результати Моніторингу інформаційної безпеки та конфіденційності, 2019р. продемонстрували, що 80% хакерських нападів спроможні зламати електронну шкільну мережу. Отже, демократичність, прозорість і доступність освіти, відкритість і вільний доступ до інформації у цифровому світі, вимагають від вчителів та учнів набувати і розвивати громадянську та ІК компетентності.

Організація інформаційної безпеки та конфіденційності починається зі створення рамкових умов у вигляді політики та встановлення відповідальності. З метою забезпечити ефективне та безпечне функціонування шкіл у цифровому середовищі, фонд Kennisnet (https://www.kennisnet.nl) у 2019 р. запропонував оновлений підхід до формування і впровадження політики інформаційної безпеки та конфіденційності, розроблений завдяки плідній співпраці фонду з Радою в галузі середньої освіти (https://www.vo-raad.nl/), Радою в галузі початкової освіти (https://www.poraad.nl/) та Радою з питань охорони здоров'я. Для реалізації оновленого підходу також створено наповнений інструментарієм єдиний веб-портал з інформаційної безпеки для шкіл та забезпечено умови комфортного переходу на нього з попередніх шкільних сайтів. Ефективне впровадження ІК технологій у навчальне середовище, в якому застосовуються хмарні сервіси, цифрові ресурси і засоби, забезпечується рекомендаціями, що розроблені фахівцями у вигляді покрокового плану, які можуть допомогти школі запровадити політику інформаційної безпеки та конфіденційності навчального закладу. Покроковий план

складається із п'яти розділів, що називаються: *політика та відповідальність, визначення обмежень та ризиків, прозорий обмін персональними даними, обробка та зберігання персональних даних та оцінка*. Розділ І Політика та відповідальність складається з таких тем: політика інформаційної безпеки та конфіденційність – та ролі та обов'язки. Кодекс поведінки щодо безпечного використання ресурсів та персональних даних ІКТ, політика щодо паролів та процедура повідомлення про інциденти з порушення безпеки – аспекти розділу ІІ Визначення обмежень та ризиків. Питання конфіденційності за замовчуванням та конфіденційності процесу розробки, угоди про соціальні медіа, обмін персональними даними та ін. розкриваються у розділі ІІІ Прозорий обмін персональними даними. Угоди про обробку та зберігання даних, правила та юридичне підґрунтя містяться у Розділ IV Обробка та зберігання персональних даних. Інструкції щодо процесів підзвітності та інформування містяться у розділі V Оцінка. До інструментарію, що забезпечує політику інформаційної безпеки та конфіденційності, також належить укладений глосарій, що визначає основні терміни та поняття, серед яких: анонімізація, псевдонімізація, аутентифікація, матриця авторизації, хмара, мінімізація даних, шифрування, хакер, аналіз ризиків, конфіденційність, конфіденційність за замовчуванням, шифрування та ін.

Молоді люди виростають в цифровому світі, який пропонує багато можливостей, та має й багато ризиків. Робота з молоддю, просвітницька діяльність у напрямі впровадження політики безпеки та конфіденційності у цифровому світі в Нідерландах здійснюється не тільки освітніми установами. Управління захисту даних Нідерландів, що забезпечує нагляд за дотриманням законів щодо захисту персональних даних та здійснює консультування та інформування громадян, окремо опікується освітньою галуззю. Фахівцями управління зазначається, що серйозна проблема полягає в питанні, чи розуміють молоді люди, які дані вони надають і як це відбувається. Задля розв'язання цієї проблеми було розроблено два навчальні пакети: для учнів під назвою "Ви керуєте своїм

телефоном?" *(«Ben jij je telefoon de baas?», нідер.*) та для вчителів, що називається «Конфіденційність» *(«Privacy», нідер.*). Навчальний пакет "Ви керуєте своїм телефоном?", що створений для учнів початкової та середньої школи, допомагає перевірити, на скільки відповідально і безпечно дитина користується своїм смартфоном, та набути необхідних знань і навичок. До складу цього навчального пакету входить гра https://autoriteitpersoonsgegevens.nl/, презентація якої була присвячена Тижню медіаграмотності, що пройшов у листопаді 2019 р.

Навчальна гра побудована на завданнях, що імітують ситуації, з якими стикається або може стикнутися дитина, користуючись своїм смартфоном для он-лайн ігор, спілкування в мережах та ін. Наприклад, дитині допомагають зрозуміти, що давши відповідь на запитання: «Кожного року на твій день народження ми будемо надсилати тобі у подарунок кролика. Скільки кроликів буде у тебе, коли тобі виповниться 18 років?» можна дізнатися про її особисті дані, а саме – рік її народження. Завдяки грі учні дізнаються, що через додатки, комп'ютерні ігри, сайти, соціальні мережі та ін. їх дані можуть потрапити до нечесної людини із сумнівними намірами, що зловмисники можуть отримати доступ до відеокамери і

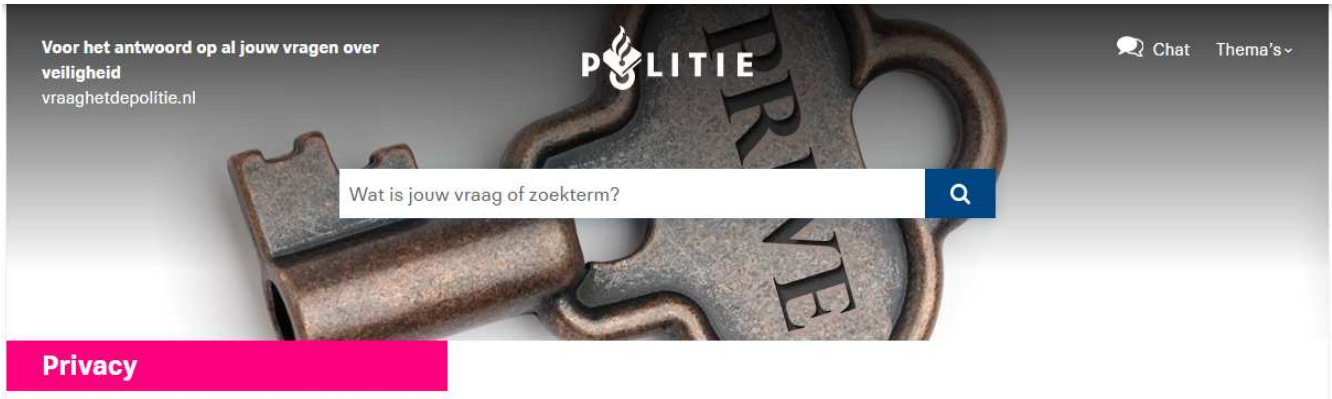
мікрофону, підслуховувати розмови чи непомітно робити фото, привласнити ім'я дитини і видавати себе за неї, та навіть отримати відбиток пальця, доступ до рахунків та здійснювати з них покупки та ін. https://autoriteitpersoonsgegevens.nl/. Виконуючи завдання навчальної гри учні дізнаються, з якими ризиками вони могли б зіткнутися, якщо не дотримуватись правил безпечної поведінки у цифровому світі та як цьому запобігти.

Безкоштовний навчальний пакет "Конфіденційність" від Нідерландського управління захисту даних надає вчителю навчальні матеріали та он-лайн інструменти, за допомогою яких розкривається тема конфіденційності «Конфіденційність стосується всіх!».

Зміст навчального пакету висвітлює тему в новому ракурсі, виходячи від права на приватність. На 3 уроках тривалістю по 45 хвилин «Хто ти в Інтернеті?», «Оплатити своїми персональними даними», «Ви маєте право на приватність!» вчитель викладає матеріал з теми конфіденційності та захисту особистих даних. Учнів знайомлять з темінологією за темою, за допомогою практично орієнтованих завдань та заохочуючи до критичного аналізу запропонованих ситуацій, вони усвідомлюють, чому різні організації часто цікавляться їх даними та які права на конфіденційність вони мають. Вчитель разом з учнями обговорює теми: «Як Ви

робите пошук?», «Яку рекламу ви отримуєте?», «Чи всі отримали однакові результати під час пошуку?», «Мої особисті дані коштують багато», «Безкоштовно ?! Читаєте ви умови, перш ніж погодитися?», «Ваш цифровий слід» та ін.

Корисним та цікавим прикладом впровадження основ інформаційної безпеки та конфіденційності в Інтеренеті є спеціально створений Молодіжний веб-сайт поліції Нідерландів https://www.vraaghetdepolitie.nl, що надає інформацію та допомагає молодим людям вийти з небезпечних ситуацій або запобігти їм.



Сьогодні молода людина стикається з багатьма ризиками і інтернеті і потребує відповідей на запитання: чи може хтось шпигувати за мною через веб-камеру без мого відома? Як захистити свої дані в Інтернеті? Чи можу я дізнатися, чи надсилаю повідомлення анонімно? Як видалити фотографію в Twitter? У мене є фотографії, на яких я стріляю на стрільбу з пневматичної зброї. Чи можу я поширити його через соціальні медіа? Чи небезпечно зустрітись з людиною, яку ви знаєте лише з Інтернету? Чи правда, що інші можуть бачити мене через веб-камеру без мого відома? Чи може незнайомець отримати мою адресу через мою IP-адресу? Чи можу я довіряти модельному агентству, яке звертається до мене через Інтернет? Чи можу я просто дати кожному свій номер? Чи можна запобігти інтернет-аферам? Чому ви не можете просто довіряти всім в Інтернеті? Чому я маю бути обережним при поширенні власних фотографій в Інтернеті? Чому я повинен бути обережним із веб-камерою? На що слід звернути увагу на фотографії профілю? Що таке безпечний

пароль? Що можна і чого не можна розміщувати на профільних веб-сайтах? Хто мої друзі в Інтернеті? Чи є доказами зйомки камер? та багато інших. Знайшовши у переліку питання, яке потребує відповіді, користувач може натиснути на нього та перейшовши за посиланням, знайти поради і інструкції для його розв'язання.

Сучасний освітній процес відбувається технологічно насиченому середовищі, яке постійно розвивається і змінюється. Сьогодні це комп'ютерно орієнтоване та хмаро орієнтоване навчальне середовище, що ставить питання безпеки і конфіденційність на новий щабель, вимагає учасників освітнього процесу бути компетентними. Дані, які використовуються вчителем або учнем, зберігаються не тільки на власному комп'ютері, а все частіше розміщуються у хмарі, учасники навчально-виховного процесу користуються хмарними сервісами, спілкуються, співпрацюють, навчаються і розвиваються засобами соціальних мереж, блогів, форумів і чатів і т.і. Отже зарубіжний досвід і практичні розробки Нідерландів, зокрема, можуть стати у нагоді вітчизняним фахівцям.

Використані джерела:

1. Фонд Kennisnet, https://www.kennisnet.nl.
2. Радою в галузі середньої освіти, https://www.vo-raad.nl.
3. Радою в галузі початкової освіти, https://www.poraad.nl.

Матеріал підготувала: Гриценчук О.О., науковий співробітник.