Міністерство освіти і науки України
Сумська обласна рада
Комунальний заклад Сумський обласний інститут
післядипломної педагогічної освіти

КІБЕРБЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ

Методичні рекомендації

Суми – 2024

УДК 378.046.4

Рекомендовано до друку та практичного використання
вченою радою комунального закладу Сумський обласний інститут
післядипломної педагогічної освіти
протокол № 10 від 28.06.2024 року

Рецензенти:

О. О. Подліняєва,	к. пед. н, доцент кафедри освітніх та інформаційних технологій комунального закладу Сумський обласний інститут післядипломної педагогічної освіти, доцент;
Л. І. Симоненко,	директор КУ Сумська гімназія № 1, вчитель вищої категорії, старший вчитель, Відмінник освіти України.

Укладачі:

І. М. Павленко,	старший викладач кафедри освітніх та інформаційних технологій Комунального закладу Сумський обласний інститут післядипломної педагогічної освіти;
Т. О. Шевченко,	старший викладач кафедри освітніх та інформаційних технологій Комунального закладу Сумський обласний інститут післядипломної педагогічної освіти.

Кібербезпека учасників освітнього процесу : методичні рекомендації / уклад.: І. М. Павленко, Т. О. Шевченко. Суми : НВВ СОІППО, 2024. 76 с.

Методичні рекомендації розкривають сутність кібербезпеки освітнього закладу, знайомлять з нормативно-правовою базою з даного питання та описують вплив кіберзагроз на учасників освітнього процесу. Автори пропонують кроки захисту інформаційних систем та мереж закладу освіти, а також методи кібергігієни для організації безпечного навчання.
Методичні рекомендації призначені для вчителів та керівників закладів освіти, які прагнуть розвинути цифрову грамотність та освоїти професійні компетенції у сфері інформаційної безпеки (кібербезпеки).

Зміст

ВСТУП

В епоху інформаційного суспільства, де цифрові технології проникають у всі сфери життя, з'являються й нові виклики – кіберзагрози.

Кібербезпека стає невід'ємним елементом загальної системи безпеки, адже вона гарантує конфіденційність, цілісність та доступність даних.

Педагоги, стикаючись у своїй роботі зі спамом, вірусами, комп'ютерними атаками та іншими кіберзагрозами, мусять не лише вміти оперативно реагувати на них, а й запобігати їх появі.

Тому в сучасній освіті актуальною стає потреба в постійному оновленні знань про інформаційні технології та методи забезпечення кібербезпеки. Педагог, володіючи цими знаннями, зможе не лише захистити інформаційні ресурси, а й навчити учнів безпечного користування ними.

Цифровий світ, де інформаційні технології пронизують всі сфери життя, несе в собі й нові виклики – кіберзагрози.

В сучасних школах комп'ютерні технології застосовуються практично на всіх уроках. Тому вдосконалення професійної підготовки педагогів у сфері інформаційних технологій, а отже, й кібербезпеки, стає вкрай актуальною потребою.

Педагог, який володіє знаннями про сучасні цифрові технології та методи забезпечення кібербезпеки, зможе не лише захистити інформаційні ресурси закладу, а й навчити учнів безпечного користування ними.

Кібербезпека – це сукупність технічних та соціальних засобів, стратегій, принципів для забезпечення захисту суспільства від загроз та впливів з небажаними наслідками, що походять від інтернет-середовища.

Кібербезпека – це процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних.

Кібербезпека покликана захистити дані на етапі їх обміну та збереження.

В законі України «Про основні засади здійснення кібербезпеки України» [52] кіберпростір визначається як «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі «Інтернет» та/або інших глобальних мереж передачі даних», а кібербезпека, 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 і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». У зв'язку з цим велике значення набуває проблема культури безпечної поведінки у кіберпросторі.

Закон України «Про основні засади здійснення кібербезпеки України» [52] зазначає, що розвиток безпечного, стабільного і надійного кіберпростору має полягати в тому числі і завдяки «підвищенню цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту».

Розділ 1. Кібербезпеки та її значення в освітньому процесі Кібербезпеки та її значення в освітньому процесі

1.1. Поняття кібербезпеки

Кібербезпека є найважливішим питанням сьогодення, оскільки в сучасному цифровому світі кіберзагрози та атаки зустрічаються все частіше. Кожного дня ми чуємо, що зламали чиюсь сторінку у соціальній мережі і розсилаються з нею повідомлення, що у когось з картки пропали гроші, що хтось розсилає повідомлення з вашої електронної пошти. Зловмисники тепер використовують складніші методи для націлювання на системи. Піддаються їхньому впливу усі: люди, малий бізнес або організації і установи. Таким чином, усі ці організації, чи то IT, чи не IT-компанії, усвідомили важливість кібербезпеки і зосередилися на вжитті всіх можливих заходів для боротьби з кіберзагрозами. Оскільки нам подобається все підключати до інтернету, це також збільшує ймовірність вразливостей, порушень та недоліків.

Минули часи, коли паролів було достатньо для захисту системи та її даних. Ми всі хочемо захистити наші особисті та професійні дані, тому Cyber Security – це те, що ми повинні знати для забезпечення захисту даних. Під'єднання до електронної інформаційної мережі стало невід'ємною частиною нашого повсякденного життя. Усі організацій, установи, в тому числі і освітні, використовують цю мережу для ефективного функціонування. Електронна інформаційна мережа використовується для збору, обробки, зберігання та обміну великою кількістю цифрової інформації. Чим більше цифрової інформації збирається і чим частіше вона спільно використовується, тим важливішим стає захист цієї інформації забезпечення національної безпеки та економічної стабільності.

Кібербезпека – це сукупність технічних і соціальних засобів, стратегій, принципів для забезпечення захисту суспільства від загроз і впливів з небажаними наслідками, що походять від інтернет-середовища.

Кібербезпека в цілому – це дуже широкий термін, але він ґрунтується на трьох фундаментальних поняттях, відомих як «CIA»: конфедеційність, цілісність, доступність. Ця модель призначена для керівництва організацією політиками кібербезпеки у сфері інформаційної безпеки (InfoSec). Конфіденційність, цілісність і доступність – це запорука ефективного захисту даних та безпеки інфраструктури організації. Ці три поняття – основоположні принципи для впровадження плану InfoSec.

Інформаційна безпека — це гарантія того, що співробітники організації зможуть переглядати та редагувати потрібні їм дані, при цьому не дозволяючи нікому більше отримати доступ до них.

При розгляді безпеки інформаційних систем звичайно виділяють дві групи проблем: безпека комп’ютера і мережева безпека.

До безпеки комп’ютера відносять всі проблеми захисту даних, що зберігаються і обробляються комп’ютером, який розглядається як автономна система. Ці

проблеми вирішуються засобами операційних систем та програм, таких як бази даних, а також вбудованими апаратними засобами комп'ютера.

Під мережевою безпекою розуміють всі питання, пов'язані з взаємодією пристроїв в мережі, це перш за все захист даних у момент їх передачі по лініях зв'язку та захист від несанкціонованого віддаленого доступу в мережу. І хоча часом проблеми комп'ютерної і мережної безпеки важко відокремити один від одного, настільки тісно вони пов'язані, цілком очевидно, що мережева безпека має свою специфіку.

Автономно працюючий комп'ютер можна ефективно захистити від зовнішніх замахів різноманітними способами:

- авторизовані користувачі завжди будуть отримувати доступ до даних,
- гарантія збереження даними правильних значень, цілісність,
- секретні дані будуть доступні дозволеним користувачам.

Комп'ютер, що працює в мережі, за визначенням не може повністю відгородитися від світу, він повинен спілкуватися з іншими комп'ютерами, можливо, навіть віддаленими від нього на велику відстань, тому забезпечення безпеки в мережі є завданням значно складнішою. Логічний вхід чужого користувача у ваш комп'ютер є штатною ситуацією, якщо ви працюєте в мережі. Забезпечення безпеки в такій ситуації зводиться до того, щоб зробити це проникнення контрольованим – кожному користувачеві мережі повинні бути чітко визначені його права щодо доступу до інформації, зовнішніх пристроїв та виконання системних дій на кожному з комп'ютерів мережі. Крім проблем, що породжуються можливістю віддаленого входу в мережеві комп'ютери, мережі за своєю природою схильні до ще одного виду небезпеки – перехоплення та аналізу повідомлень, переданих по мережі, а також створення «помилкового» трафіку. Більша частина коштів забезпечення мережної безпеки спрямована на запобігання саме цього типу порушень.

Питання мережевої безпеки набувають особливого значення зараз, коли при побудові корпоративних мереж спостерігається перехід від використання виділених каналів до публічних мереж (інтернет, frame relay). Постачальники послуг публічних мереж поки рідко забезпечують захист даних користувача при їх транспортуванні по своїх магістралях, покладаючи на користувачів турботи по їх конфіденційності, цілісності та доступності.

Безпечна інформаційна система – це система, яка, по-перше, захищає дані від несанкціонованого доступу, по-друге, завжди готова надати їх своїм користувачам, а потретє, надійно зберігає інформацію і гарантує незмінність даних.

Таким чином, безпечна система має властивості конфіденційності, доступності та цілісності.

1) Конфіденційність (confidentiality) – гарантія того, що секретні дані будуть доступні тільки тим користувачам, яким цей доступ дозволений (такі користувачі називаються авторизованими). Конфіденційність – це основний компонент InfoSec, який полягає в тому, що доступ до інформації можуть отримувати лише авторизовані користувачі. Шифрування даних, багатофакторна автентифікація та захист від втрати даних – це приклади інструментів, які

підприємства можуть використовувати для забезпечення конфіденційності інформації.
Що таке багатофакторна автентифікація. Багатофакторна автентифікація (БФА) додає ще один рівень захисту під час входу. Під час доступу до облікових записів або програм користувачі проходять додаткову перевірку ідентичності, наприклад сканують відбиток пальця чи вводять код із телефона. Багатофакторна автентифікація (БФА) за допомогою хмарної служби Azure Active Directory (Azure AD) допомагає захистити доступ до даних і програм, не ускладнюючи роботу для користувачів. Azure AD використовують для проходження багатофакторної автентифікації при доступі до ресурсів організації, наприклад таких як Microsoft 365. Додатковий етап перевірки посилює безпеку під час автентифікації, а сама перевірка відбувається простими й одночасно надійними методами.
2) Доступність (availability) – гарантія того, що авторизовані користувачі завжди будуть отримувати доступ до даних. Доступність говорить про те, що дані відкриті лише для тих, у кого є відповідні дозволи.
3) Цілісність (integrity) – гарантія збереження даними правильних значень, яка забезпечується забороною для неавторизованих користувачів будь-яким чином змінювати, модифікувати, руйнувати або створювати дані.
Будь яка організація має підтримувати цілісність даних протягом усього їхнього життєвого циклу. Організації з розвинутим компонентом InfoSec визнають важливість використання точних і надійних даних та не дозволять неавторизованим користувачам отримувати доступ до них, змінювати їх або керувати ними. Такі інструменти, як дозволи для файлів, керування ідентичностями й елементи керування доступом користувачів, забезпечують цілісність даних. Вимоги безпеки можуть змінюватися залежно від призначення системи, характеру використовуваних даних і типу можливих загроз. Важко уявити систему, для якої були б не важливі властивості цілісності та доступності, але властивість конфіденційності не завжди є обов’язковим. Наприклад, якщо ви публікуєте інформацію в інтернеті на Web-сервері і вашою метою є зробити її доступною для найширшого кола людей, то конфіденційність в даному випадку не потрібно. Проте вимоги цілісності та доступності залишаються актуальними.
Поняття конфіденційності, доступності та цілісності можуть бути визначені не тільки по відношенню до інформації, але і до інших ресурсів обчислювальної мережі, наприклад зовнішніх пристроїв або додатків. Існує безліч системних ресурсів, можливість «незаконного» використання яких може призвести до порушення безпеки системи. Наприклад, необмежений доступ до пристрою друку дозволяє зловмисникові отримувати копії, роздруковувати документи, змінювати параметри налаштування, що може призвести до зміни черговості робіт і навіть до виведення пристрою з ладу. Властивість конфіденційності, застосована до пристрою друку, можна інтерпретувати так, що доступ до пристрою мають ті і тільки ті користувачі, яким цей доступ дозволений, причому вони можуть виконувати тільки ті операції з пристроєм, що для них визначено. Властивість доступності до пристрою означає його готовність до використання кожного разу, коли в цьому виникає необхідність. А властивість цілісності може

бути визначена як властивість незмінності параметрів налаштування цього пристрою. Легальність використання мережевих пристроїв важлива, оскільки вона впливає на безпеку даних. Пристрої можуть надавати різні послуги: роздруковування текстів, відправлення факсів, доступ до інтернету тощо. Незаконне використання мережевих пристроїв завдає матеріальної шкоди організації (підприємству, установі), а також є порушенням безпеки системи.

Важливим поштовхом до впровадження компетентістного навчання став запуск штучного супутника Землі радянськими вченими у 1957 році. Реагуючи на цей виклик і розуміючи системні прорахунки своєї системи навчання уряд США розпочинає загальну реформу освітньої системи. На основі порівняльного аналізу систем народної освіти США та СРСР американський вчений А. Трейс опублікував свою відому роботу What Ivan knows that Johny doesn't», надавши потужний поштовх до системної перебудови освіти на основі компетентнісного підходу.

Подальший розвиток компетентністний підхід отримав у 70-ті роки XX століття у навчальних закладах Північної Америки та Європи. Зокрема наукове обґрунтування впровадження компетентінісного навчання у систему загальної підготовки здобувачів освіти було зроблено у роботах Д. Равена, Р. Уайта та інших.

Цінним для нашого дослідження є класифікація етапів розуміння поняття «компетентність» у «західній науці», яка була розроблена американським вченим П. Хаген.

Провівши аналіз наукових джерел було визначено, що у сучасній педагогічній науці немає узгодженої точки зору щодо поняття «компететність». Зокрема, у «Психологічній енциклопедії» компетентність ґрунтується на трьох основних аспектах [14]:

– ступені та здатності оволодіння необхідними знаннями, уміннями і навичками;
– юридичній відповідності (особи);
– досвідченості спеціаліста для займання конкретної посади (за фаховим спрямуванням).

Зазначимо, що в енциклопедії поняття «компетентність» може визначатися досить неоднозначно, тому що не надає чіткого ступеня рівня майстерності фахівця. Відповідно цей термін може використовуватися для визначення загальної кваліфікації фахівця.

Так, у Державному стандарті базової та повної середньої освіти поняття «компетентність» визначається, як «…набута у процесі навчання інтегрована здатність учня, що складається зі знань, умінь, досвіду, цінностей і ставлення, що можуть цілісно реалізовуватися на практиці». О. Іванова визначає термін компетентність як відповідну сукупність знань, умінь та навичок з наявністю певного досвіду їх використання у контексті реалізації потенційних можливостей особистості [6].

Таким чином, у психолого-педагогічній літературі надано низку визначень поняття «компетентність», визначено, що сам термін пройшов довгий шлях становлення від загального розуміння діяльності особистості до оволодіння індивідом системою інтелектуальних, моральних та соціальних якостей,

потрібних у житті, та здатності їх використовувати. Наступним кроком у розвитку й запровадженні компетентнісного підходу в освітній процес була розробка платформи ключових компетентностей у рамках програм ЮНЕСКО у 1996 р. [53]. Сьогодні ж у європейській освітній системі існує поділ компетентностей на дві значні групи:

– subject specific competences (фахові компетентності);

– generic competences (загальні компетентності).

Відзначимо, що група фахових компетентностей залежить від предметної галузі, саме вони визначають профіль освітніх програм та кваліфікацію майбутнього випускника закладу вищої освіти. Так, на противагу визначеній вище групі компетентностей існують й інші, не менш важливі компетентності, якими майбутній фахівець оволодіває в процесі отримання вищої освіти, але вони у своїй природі мають універсальний характер та не прив'язані до предметної галузі знань. Зокрема, можна виділити уміння вчитися, обізнаність в інформаційних технологіях, креативність у роботі, володіння іноземними мовами тощо [16].

У контексті впровадження компетентнісного підходу в вищу освіту України потрібно визначитися з тим, що ж саме є компетентнісний підхід (далі КП), і дати визначення цьому процесу. В. Химинець визначає КП (в освіті) як направленість освітнього процесу на формування та розвиток ключових і предметних компетентностей особистості. Відповідно КП у цьому контексті направляє освіту на формування цілісного набору здатностей, якими повинні оволодіти здобувачі освіти під час навчання у закладах освіти. Крім того, вчений акцентує увагу, що традиційна освітня система спрямовує основні зусилля на отриманні ЗУН (знання, уміння, навички) [21]. В. Химинець розглядає підготовку здобувачів освіти в контексті КП у двох аспектах: через оновлення змісту вищої професійної освіти, що передбачає її відбір і структурування з одночасним визначенням результативної складової освітнього процесу, а саме: набуття студентами певних компетентностей; потреба у навчанні цілеспрямовано формувати ключові та предметні компетентності.

Отже, основною ідеєю КП є компетентнісно орієнтована освіта, яка спрямована на комплексне засвоєння знань і способів їх практичного застосування, завдяки яким людина успішно реалізує себе в різних галузях своєї життєдіяльності [21].

Відповідно до численних викликів, які поставали перед освітою Європи, були сформульовані п'ять ключових компететностей «Молодого європейця» (що слугувало однією з перших спроб розробити компетентності з направленістю у законодавчому полі), серед яких говориться про компетентності, що пов'язані зі зростанням інформатизації та цифровізації суспільства, яка передбачає оволодіння людиною технологіями, розуміння особливостей їх використання, сильних і слабких сторін, здатність критично оцінювати інформацію, поширювану рекламою та засобами мас-медіа.

Цифрова компетентність займає ключове місце в системі професійних та загальних компетентностей, є основою для професійного становлення в будь-якій галузі діяльності сучасного фахівця. Наприклад, важливою характеристикою становлення майбутнього фахівця в галузі освіти є цифрова

компетентність, яка входить до складу десяти основних компетентностей, прописаних у Концепції «Нова українська школа» (2016). Отже, цифрова компетентність визнається як одна із ключових компетеностей сучасної людини і займає провідне місце у їх переліку.

У дослідженні «Цифрова компетентність на практиці: рамковий аналіз» («Digital Competence in Practice: An Analysis of Frameworks»), яке оприлюднила Європейська комісія, зазначено, що в Рекомендаціях Парламенту і Ради Європи від 18 грудня 2006 р. (Recommendation of the European Parliament and of the Council of 18 December 2006 on key competences for lifelong learning (2006/962/EU)) цифрова компетентність визнана однією з восьми ключових компетентностей для навчання впродовж життя Lifelong Learning (LLL) у країнах Європейського Союзу. Вона визначена як здатність упевнено, критично та творчо використовувати цифрові технології для досягнення цілей, що належать до галузі роботи, зайнятості, навчання, дозвілля, участі в житті суспільства. Ця компетентність розглядається як наскрізна, що сприяє досягненню інших компетентностей, які стосуються сфери мов, математики, вміння навчатись, культурної обізнаності тощо і належать до обов'язкових компетентностей XXI ст., відповідно, якщо громадянин хоче реалізувати себе у професійному та особистому житті та мати сучасні навички і знання для ефективного функціонування у суспільстві, він повинен розвивати власну цифрову компетентність.

Цифрова компетентність у своїй основі має знаннєвий та дієвий компоненти.

У зарубіжних системах освіти в межах поняття «цифрова компетентність» визначають низку понять, зміст яких у багатьох випадках ототожнюється.

Незважаючи на велику кількість наукових робіт, присвячених питанню цифрової компетентності, єдиного підходу до тлумачення терміна «цифрова компетентність особистості» на сьогодні не існує.

Проведений аналіз наукових джерел засвідчує, що питома вага досліджень, пов'язаних із різними аспектами впровадження цифрової компетентності в різні ланки суспільного життя набуває неабиякої популярності в науковому середовищі у наші дні. Не є винятком освітній процес. Так, у рамках впровадження «цифровізації» в сучасну освітню діяльність з'являється багато нових та оновлених понять і підходів, пов'язаних з упровадженням інформаційних та комунікаційних технологій в освіту.

Відзначимо, що основні дискусії навколо визначення поняття «цифрова компетентність» у минулому відбувались у межах розроблення відповідних документів міжнародними організаціями. Розбіжності, що мають місце у визначенні поняття «цифрова компетентність» стосовно формування і застосування сфери цифрових технологій, пов'язані з контекстом, у якому вони застосовуються. Наприклад, О. Овчарук, спираючись на звіти OECD, зазначає про такі тенденції, як трансформація суспільних відносин у контексті все більшого використання цифрових технологій у різних сферах його життєдіяльності: «нова економіка (new economy), е-економіка (e-economy), ІКТ-сектор (ICT sector), зумовлюють застосування різної термінології щодо сфери ІК-технологій, а це, у свою чергу, призводить до нечіткої термінології стосовно

поняття "цифрова компетентність"» [11]. Розвиваючи тему визначення поняття «цифрової компетентності» (далі ЦК) не можна не вказати й інші поняття, які використаються зарубіжними та вітчизняними вченими у значенні ЦК. До них можна віднести «цифрову грамотність» та «інформаційну грамотність».

Наприклад, Американська бібліотечна асоціація (ALA) на початку XXI століття, створила стандарти компетентності у сфері інформаційної грамотності («Information Literacy Competency Standards for Higher Education»), відповідно до яких освіченою людиною може вважатися та особа, яка вміє знаходити інформацію, необхідну для професійної та побутової діяльностей, знати, як користуватися цією інформацією, проводити аналіз, синтез та оцінку інформації та джерела її походження, використовуючи при цьому сучасні цифрові та комунікаційні технології. Учені А. Мартін та Й. Грудзієскі, описують цифрову грамотність як поінформованість, здатність людини до належного використання цифрових інструментів та засобів для виявлення, доступу, управління, інтеграції, оцінки, аналізу та синтезу цифрових ресурсів, конструювання нових знань, створення засобів масової інформації та спілкування з іншими людьми в контексті конкретних життєвих ситуацій з метою активізувати конструктивні соціальні сили особи.

Схожої точки зору дотримується Н. Сороко, визначаючи «інформаційну грамотність» через вміння і навички людини, направлені на дентифікацію інформації, здійснення її ефективного пошуку, аналіз та систематизацію, орієнтацію в інформаційних ресурсах та потоках. Цінною для нашого дослідження є робота американських вчених Н. Спірес та М. Бартлетт, які акцентують увагу свого дослідження «Digital literacies and learning: Designing a path forward» саме на цифровій грамотності здобувачів освіти, де цифрова грамотність повинна бути позицією для здобувачів освіти, яка підтримує їх повну участь у суспільному житті, в якому об’єднується громадське, культурне, політичне та фінансове життя в контексті їх все більшої інтеграції з цифровими технологіями.

Таким чином, на сучасному етапі розвитку цифрових технологій поняття «цифрова грамотність» має включати в себе низку таких аспектів, як організація роботи у цифровому просторі; безпека у цифровому середовищі; аналіз та синтез отриманої інформації, здатність використовувати отримані знання у професійному та приватному житті; комунікація та повага до всіх учасників процесу взаємодії у цифровому просторі.

Крім того, цифрова грамотність та кібербезпека стає основою для розвитку інформаційної культури людини. Тобто цифрова компетентність особистості на сьогодні може виступати у ролі «нової грамотності» сучасної людини, де переважна більшість суспільних відносин «переходить» у цифровий вимір.

Важливо зазначити, що «цифрова компетентність» як поняття, пов’язане з формуванням та застосуванням ІКТ, переживає трансформацію разом із поглибленням наукових розвідок у цій сфері. Варто підкреслити, що здебільшого науковці, які досліджують цифрову компетентність людини та її прояви в професійному та приватному житті зупиняються на суб’єктивній характеристиці цього поняття в контексті своїх досліджень. Тобто зміст визначення цього

складного поняття зводиться до цілей та потреб конкретного дослідника, що в свою чергу призводить до необ'єктивних та оманливих результатів, де саме поняття «цифрова компетентність» трактується занадто вузько чи занадто широко. Сьогодні такі колізії у визначені поняття «цифрова компетентність» надають ще більшої актуальності дослідженням, які ставлять за мету не підлаштування під отримані результати, а насамперед направлені на змістовий аналіз множинних визначень цього поняття та систематизації відповідно до теперішніх реалій розвитку освіти та техніки у цифровому просторі. Іншим важливим аспектом, пов'язаним із цифровою компетентністю та її формуванням, є її відображення у змісті освіти та системі ефективної підготовки здобувачів освіти, тому що не секрет, що зараз існує багато думок та позицій різних науковців щодо компете тності, пов'язаної з «цифровізацією» усіх ланок суспільного життя людини.

Далі розглянемо різні визначення цифрової компетентності провідними науковцями в галузі педагогічних та інших наук. О. Овчарук приводить консолідоване визначення цифрової компетентності як «доведену здатність працювати індивідуально або колективно, використовуючи інструменти, ресурси, процеси і системи, які відповідають за доступ до інформації (відомостей і даних) та її оцінювання, застосовувати таку інформацію для вирішення проблем, спілкування, створення інформаційно-спрямованих рішень, продуктів і систем, а також для отримання нових знань».

У дослідженні групи вчених під керівництвом М. Леннон цифрова компетентність була визначена як інтерес, ставлення та здатність людей до належного використання цифрових технологій і засобів комунікації для доступу, управління, інтеграції та оцінки інформації; конструювати нові знання; спілкуватися з іншими, щоб ефективно брати участь у суспільстві О. Жерновникова характеризує цифрову компетентність здобувача освіти як універсальні способи передачі, отримання, пошуку, обробки, надання, узагальнення, систематизації, перетворення інформації в знання.

О. Романовський під «цифровою компетентністю» розуміє комплекс знань, умінь, навичок і рефлексійних установок майбутніх учителів у взаємодії з інформаційним освітнім середовищем.

Група вчених під керівництвом М. Каравелло визначає ЦК як здатність бути в курсі швидких змін технологій, включаючи відповідні знання та вміння, здатність використовувати ІКТ належним чином для власних цілей, як особистих, так і професійних.

А. Добровольська у своїх дослідженнях акцентує увагу на підготовці майбутніх лікарів та провізорів медичного ЗВО та їх цифровій компетентності у межах навчання природничо-наукового циклу й називає знання, уміння навички та способи діяльності у процесі їх набуття «ІТ-компетентністю».

Цифрова компетентність передбачає впевнене, безпечне та критичне використання технологій інформаційного суспільства (анг. IST) для роботи, навчання, дозвілля та спілкування. Вона включає основні навички використання IST, а саме: використання цифрових пристроїв для отримання, оцінки,

зберігання, виготовлення, представлення, спілкування та обміну інформацією, а також для участі у соціальних мережах в мережі «Інтернет».
Схожої точки зору щодо визначення поняття цифрової компетентності особистості дотримується й М. Раньєрі. ЦК передбачає усвідомлене та критичне використання електронних медіа та цифрових ресурсів для професійної діяльності й особистих потреб. Ця компетентність пов'язана з логічним та критичним мисленням, навичками, високим рівнем управління інформацією у цифровому просторі та добре розвиненими навичками спілкування.
Особливо розгалуженим та повним є визначення ЦК, надане у роботі А. Феррарі, це визначення групується на низці міжнародних та національних проектів та грантів і включає в себе такі складові: здатності, стратегії, цінності та обізнаності в цифровому просторі, які потрібні в процесі використання сучасних ІК-технологій; ефективність вирішення проблем, які виникають при використанні ІК-технологій; роботу з інформаційними джерелами; створення контенту та його використання в межах правових відносин у кіберпросторі; забезпечення реалізації своїх прав у цифровому просторі; вміння комунікувати з іншими користувачами та поважати їх погляди.
Л. Іломякі та М. Канкаанранта визначають ЦК, як більш широку концепцію ІКТ компетентності. Вчені акцентують увагу на складових ЦК та включають до них базові навички з використання ІКтехнологій, а також розуміння та знання того, як використовувати цифровий пристрій та додатки в нових і нестандартних ситуаціях, які вимагають конкретної взаємодії з цировим середовищем для їх вирішення.
Визначення цифрової компетентності в освітніх рамках, наприклад, «The Digital Competence Framework 2.0» та навчальних програмах є життєво важливим, оскільки дає можливість відображати обґрунтування використання освітніх цифрових технологій в цьому процесі. Наприклад, Дж. Тондер та його колеги описали чотири обґрунтування, що лежать в основі впровадження цифрових технологій в життя суспільства: економічне, освітнє, соціальне та каталітичне.
Ці чотири позиції можуть визначати національну політику в галузі освітніх технологій і бути тісно пов'язаними розвитком навчальних програм у галузі формування цифрової компетентності здобувача освіти. Такі знання потенційно можуть ілюструвати основні напрямки та цілі національних навчальних програм і міжнародних рамок у цій сфері та підтримувати баланс між ними.
У «The Digital Competence Framework 2.0» визначено концептуальну модель цифрової компетентності особистості У контексті дослідження розглянемо визначення ЦК, надане скандинавським дослідником Р. Крумсвіком. У своєму дослідженні «Situated learning and digital competence» вчений розглядає ЦК педагогічного працівника в розрізі професійної здатності впроваджувати та застосовувати цифрові технології в освітньому процесі закладів освіти. Крім того, дослідник акцентує увагу на критеріях застосування цифрових технологій в освітньому процесі, а саме на важливості їх доцільного використання з урахуванням сучасних тенденцій освітніх наук та їх дидактичних можливостей, окремо наголошуючи на важливості використання цифрових технологій

навчання у тісному зв'язку зі специфікою дисципліни, яка викладається, особливостями групи здобувачів освіти, конкретної теми навчального заняття.
Цінними для нашого дослідження є нормативні документи в галузі освіти, розроблені в Європейському Союзі (ЄС). Розглянемо більше детально Європейську рамку е-компетентності (European e-Competence Framework, E-CF). Створення цієї рамки стало можливим після консультацій з країнами-членами CEN (The European Committee for Standardization), E-CF став європейським стандартом і був опублікований у 2016 році офіційно як Європейська норма (EN).
Новий формат EN надав великі можливості для подальшого розповсюдження та подальшого прийняття рамки у всіх країнах Європейського Союзу. E-CF є ключовою складовою цифрової програми Європейської комісії, направленої на використання будь-якою організацією, що займається ІКТ плануванням людських ресурсів та розвитком відповідних компетентностей. Зазначимо, що E-CF підтримує основні положення програми ЄС «The Digital Skills and Jobs Coalition», яка має на меті об'єднання зусиль провідних організацій, які направляють свої зусилля на покращення цифрових навичок громадян у Європі. У E-CF провідне місце відводиться визначенню поняття цифрової компетентності та цифровим навичкам особистості як основі їх формування в процесі навчання. Так, ЦК в освіті визначається як знання відповідних педагогічних підходів і методів організації навчального процесу, а також включає такі навички, як здатність правильно обирати цифрові ресурсів та навчальні матеріали, вміння розробляти навчальні плани та програми з використанням цифрових технологій, вміння ефективно аналізувати отримані результати вносити своєчасні зміни в процесі навчання [25].
Аналізуючи різні визначання ЦК у роботах вітчизняних та зарубіжних вчених, можна часто зустріти споріднене поняття «інформаційнокомунікаційна компетентність», що значною мірою збігається з узагальненим визначення цифрової компетентності як здатності працювати з цифровими джерелами інформації та сучасними технологіями, проте ми вважаємо, що ці поняття хоча і мають багато спільного, але потребують розмежування, що можливо буде зробити у подальших дослідженнях. З огляду на це, вважаємо за необхідне проаналізувати і таке поняття, як «інформаційно-комунікаційна компетентність» (ІКТ-компетентність) в його освітньому значенні. В. Браздейкіс розглядає ІКТ-компетентність як знання, вміння, ставлення, цінності, а також індивідуальні риси особистості, які направлені на ефективне використання інформаційно-комунікаційних технологій в освітньому процесі [23]. У своєму дисертаційному дослідженні «The educators' competence of applying the information and communication technologies and its evaluation strategies» [23] В. Браздейкіс розділяє ІКТ-компетентність вчителя на два рівні: базовий та інтегральний, а також включає до них низку компонентів.
С. Прохорова вказує на те, що цифрова компетентність педагога визначається як його здатність ефективно та результативно використовувати ІКТ у своїй професійній діяльності з метою розвитку. Вчена відносить до складових елементів цифрової компетентності низку допоміжних якостей педагога:

– технічні навички роботи з цифровими технологіями;
– здатність застосовувати цифрові ресурси в освітньому процесі;
– здатність планувати, аналізувати та керувати освітнім процесом за допомогою ІК-технологій;
– критично оцінювати ресурси та бути добре ознайомленим із соціальними та етичними аспектами їх використання.
С. Прохорова акцентує особливу увагу на коректному «підборі й аналізі матеріалів та інструментів», урахуванні специфіки навчального заняття, на якому будуть застосовуватися цифрові засоби навчання [13].
С. Скотт розкриває поняття «цифрової компетентності» як здатність особистості використовувати цифрові ресурси, усвідомлювати та критично оцінювати різні аспекти отримання контенту у цифровому просторі та ефективно комунікувати в умовах цифрового простору. Вчений виділяє низку складових частин ЦК особистості: ефективно та безпечно використовувати технологічні можливості ПК та інших гаджетів для вирішення різноманітних задач; цифрова грамотність в інформаційному та медійному полі направлена на пошук, обробку та зберігання інформації, створення цифрового контенту; онлайн комунікація з учасниками кіберпростору.
Цифрова компетентність є великим та складним конструктом, її зміст складається з багатьох складових й утворює загальну модель, яка складається з інструментальних умінь і знань, ставлення (у багатьох проявах) та розвинених умінь і знань, що в своїх дослідженнях приводить К. Ала-Мутка.
Крім того, працюючи з різними нормативно-правовими актами Європейського Союзу в галузі освіти вчена дійшла до висновку, що рушійною силою розвитку ЦК особистості є її цифрові знання й уміння, які проявляються в когнітивному, технологічному та інших компонентах.
Освітні перетворення пов’язані з упровадженням цифрових технологійта більш технологічних засобівпередачі інформації змушують реформувати і вітчизняну систему освіти. Надмірна бюрократизація, притаманна нашій освітній системі, уповільнює ці процеси, але, не дивлячись на це, з’являються нові підходи та концепції розвитку освіти. Наприклад, вже більше трьох років триває реформа шкільної освіти під назвою «Нова українська школа» (НУШ), де однією з ключових компетентностей здобувача освіти є ЦК. Ці зрушення мають позитивний характер та направлені на розвиток сучасної дитини.
На сьогодні поняття ЦК особистості розвивається і доповнюється, проте у вітчизняній освітній думці воно ще приживається і нерідко можна зустріти неоднозначне тлумачення та розуміння цього поняття. Слушною є думка вчених про те, що поняття ЦК являє собою найбільш доцільне вираження компетентності людини в галузі ІК-технологій.
За визначенням Л. Гаврилової, найбільш уживаним означенням ЦК виступає інтегрована здатність особистості, до складу якої входять знання, уміння, досвід, цінності та ставлення, що можуть бути реалізовані в загальному вигляді на практиці [1].
Цінним для нашого дослідження є узагальнене бачення необхідних

складових ЦК, яке дала О. Сисоєва, спираючись на дослідження зарубіжних та вітчизняних фахівців у галузі цифрової освіти [18].

Таким чином, провівши аналіз різних точок зору вітчизняних та зарубіжних вчених, організацій та структур щодо визначення суті поняття ЦК особистості, ми дійшли висновку, що ЦК в своїй основі має низку базових елементів, таких як знання та уміння працювати в цифровому середовищі, здатність взаємодіяти та комунікувати з різними суб'єктами у кіберпросторі, уміння шукати та аналізувати інформацію, здатність довідповідальної поведінки в процесі створення та розповсюдження цифрового контенту, знання операційних і технологічних можливостей техніки, з якою необхідно взаємодіяти. Крім того, потрібно чітко окреслити важливість ЦК в освітній діяльності, тому що сучасне покоління здобувачів освіти має незрівнянно більші можливості для розвитку свої умінь у цифровому середовищі порівняно з тією ситуацією, що була навіть 10 років тому, стрімкий розвиток соціальних мереж і їх трансформація в платформи для створення онлайн-ідентичностей та майданчиків для просування важливих ідей і тенденцій стає дієвим інструментом взаємодії між педагогом та здобувачем освіти. Іншою важливою функцією ІК-технологій в освіті стає побудова принципово нової моделі навчання, де питома вага пошукової діяльності значно збільшується та в перспективі зможе значно збагатити навчальний процес, проте існують і ризики, пов'язані з розривом у розумінні важливості цифрових технологій між поколіннями. Адже, як зазначалося вище, сучасні здобувачі освіти вже змалечку інтегровані в інформаціно-цифровий простір, що потребує відповідного підходу в процесі передачі знань від старшого покоління до молоді.

Варто відмітити, цінність цифрових технологій для розвитку критичного мислення та творчості. У першому випаду сучасна молодь має найбільший доступ до інформації за всю історію людства, тому важливо приділяти особливу увагу процесу критичного сприйняття отримуваної інформації. З метою розвитку цих вмінь можна впроваджувати спеціальні предмети (покликані дати знання та вміння в галузі аналізу й використання отриманої інформації) в закладах освіти. Щодо розвитку творчості здобувачів освіти, сучасні цифрові технології та засоби навчання створюють можливості для креативності, розбудови і втілення власних ідей без вкладання значних ресурсів, на сьогодні майже кожний має гаджети, які можуть задовольнити ці потреби, їх розумне використання в освітньому процесі може значно збагатити арсенал ефективних шляхів розбудови вітчизняної освіти. Говорячи про перспективи застосування цифрових технологій у вітчизняних суспільних відносинах, чи-то економіка чи освіта, потрібно чітко розуміти, які є сильні або слабкі сторони цього складного утворення, які є ресурси для їх розвитку тощо. У контексті вищезазначеного, розглядаючи питання, пов'язані з ЦК особистості, варто згадати такий важливий показник готовності країни до розвитку та впровадження інформаційно-комунікаційних технологій в суспільні відносини, як Індекс мережної готовності (WEF-INSEAD Network Readiness Index (NRI)). Починаючи з 2001 року, в рамках Всесвітнього Економічного Форуму (ВЕФ) видається щорічна доповідь «Глобальні інформаційні технології», метою якої є, вимірювання рушійних факторів

розвитку в ІК-технологій в усьому світі, використовуючи Індекс мережевої готовності (NRI).

З часом NRI еволюціонував і зараз оцінює стан мережевої готовності з використанням 53 індивідуальних показників для кожної із 139 економік, які в ньому індексуються. Отримані результати за допомогою NRI дозволяють визначити пріоритетні сфери розвитку, щоб більш повно використовувати ІК-технології для соціально-економічного розвитку держави. Важливо відзначити, що місце у цьому рейтингу може виступати індикатором готовності суспільства та держави брати участь у розвитку ІК-технологій. Україна у цьому рейтингу посідає 59 місце згідно з даними сайту KNOEMA (https://knoema.com/atlas/topics/World-Rankings/World-Rankings/Networked-readinessindex), що показує значну динаміку приросту порівняно з 2015 р. Але не дивлячись на позитивну динаміку впровадження цифрових технологій у вітчизняні суспільні відносини згідно з NRI, українське суспільство має докласти багато зусиль для подальшого впровадження цифрових технологій в усі сфери його життя.

До шляхів покращення ситуації можна віднести: удосконалення вітчизняної нормативно-правової бази, пов'язаної з функціонуванням та професійною діяльністю у цифровому просторі, що також потребує покращення та інтеграції з міжнародними правовими інституціями щодо права інтелектуальної власності, що дуже часто негативно впливає на мотивацію «виведення» цифрових продуктів на ринок; державну підтримку впровадження реально діючих цифрових продуктів через їх апробацію в державному секторі та в освіті зокрема; покращення потребує «реальне» навчання як ІТ-фахівців, так і звичайних користувачів, потрібно у зрозумілій формі пояснювати та мотивувати, покращувати власні цифрові навички, що у майбутньому можуть стати основою цифрової культури особистості. Відповідно до вищезазначеної доповіді ВЕФ розвиток інформаційно-цифрового середовища країни безпосередньо визначає її конкурентоспроможність в економічному плані та в цілому.

1.2. *Нормативно-правова база з питань кібербезпеки в освіті*

В Україні поки ще немає чітко визначеної нормативної бази, яка б регулювала безпеку роботи вчителів та учнів в інтернеті під час навчання, у тому числі, – безпеку роботи з персональними даними. Але ніщо не заважає нам використовувати на практиці ті норми законодавства, які ми вже маємо.

Положення про дистанційну форму здобуття повної загальної середньої освіти визначає, що під час дистанційного навчання освітній процес організовується з дотриманням вимог законодавства про захист персональних даних. У листі МОН від 02.11.20 № 1/9-609 "Щодо організації дистанційного навчання" наголошується, що всі учасники освітнього процесу мають дотримуватися вимог щодо захисту персональних даних учасників освітнього процесу в електронному освітньому середовищі.

Основним законом із питання захисту персональних даних в нашій державі є Закон України "Про захист персональних даних", і саме його потрібно брати за основу для роботи з персональними даними та їхнього захисту.

Міжнародний союз електрозв'язку визначає наступні рекомендації для закладів освіти:

- заклад освіти має забезпечити захищену та надійну 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;

– використання програмного забезпечення для фільтрації та моніторингу безпеки пристроїв;

– встановлення політику в межах закладу освіти, 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;

– організація для здобувачів освіти навчання з питань онлайнової безпеки;

– забезпечення достатнього рівеня підготовки усіх співробітників (зокрема, технічного персоналу), а також регулярне підвищення їхньої кваліфікації;

– призначення у закладі освіти спеціального координатора і створення можливості для обліку та реєстрації інцидентів, пов'язаних з онлайновою безпекою, щоб сформувати цілісне уявлення про наявні у школі проблеми та тенденції, що вимагають уваги;

– вживання заходів для того, щоб адміністративно–управлінський персонал та керівники були достатньо обізнані в питаннях онлайнової безпеки у закладі освіти;

– взяття до уваги потенційний вплив інтернету та онлайнових технологій на навчання та психіку здобувачів освіти.

Відповідно до Положення про дистанційну форму здобуття повної загальної середньої освіти, електронні освітні платформи, онлайн сервіси та інструменти, за допомогою яких організовується освітній процес під час дистанційного навчання, обирає та схвалює педагогічна рада закладу освіти. МОН наголошує на тому, що рекомендовано педагогам обирати для дистанційного навчання одну або дві освітні платформи, оскільки це полегшить учням, вчителям та батькам організацію навчання. Також використання мінімальної можливої для забезпечення освітнього процесу кількості платформ робить дистанційне навчання безпечнішим, оскільки зменшується ризик витоку персональних даних. Як у випадку з провайдером, рекомендуємо обирати перевірені платформи від офіційних виробників та не надавати зайвих персональних даних здобувачів освіти і вчителів для користування платформами.

Заклад освіти має повідомити учнів та батьків, які персональні дані будуть оброблятися під час використання тієї чи іншої платформи дистанційного навчання. Водночас закладам освіти необхідно звернути увагу на розробку певних правил поведінки та безпеки в онлайн середовищі і порядок реагування на інциденти. Спільне обговорення та прийняття цих правил з усіма учасниками освітнього процесу дозволить мінімізувати неприємні випадки, які періодично трапляються під час дистанційного навчання.

Рекомендації педагогічним працівникам для безпеки дистанційного навчання: необхідно слідкувати за безпекою та надійністю як домашніх так і робочих пристроїв, які ви використовуєте для проведення дистанційного навчання.

Для цього:

– переконайтеся в тому, що всі пристрої надійно захищені та на них встановлено пароль. Учителі настільки ж вразливі перед кібератаками, шкідливими програмами, вірусами та зламами, як і всі інші. Важливо, щоб усі пристрої, які ви використовуєте, захищалися надійним паролем. Онлайн-генератор надійних паролів – сервіс 2ip.ua (https://2ip.ua/ua/services/useful-service/password-generator) – блокуйте пристрої, завершуйте сеанс і виходьте з облікового запису, коли не використовуєте їх (наприклад, якщо виходите з кімнати або класу);

– встановіть антивірусне програмне забезпечення та брандмауер й регулярно їх оновлюйте. Також дотримуйтеся визначеної закладом освіти політики щодо використання мобільних технологій та інших електронних пристроїв. Важливо, щоб при використанні пристроїв вчителі подавали учням приклад правильної поведінки;

- забезпечте фільтрацію та моніторинг даних, що передаються через шкільне під'єднання до інтернету (під час дистанційного навчання вдома – через домашнє під'єднання до інтернету);

- здобувачі освіти не повинні отримувати доступу до шкідливого або неприйнятного контенту через ІТ-системи закладу освіти або домашнє технічне обладнання. Системи фільтрації мають щонайменше блокувати доступ до незаконного контенту, а також контенту, який вважається неприйнятним або шкідливим. Необхідно пам'ятати про власну онлайн-репутацію та цифровий слід, який залишаєте, про те, що ваші слова та дії в інтернеті можуть вплинути як на вашу власну репутацію, так і на репутацію закладу освіти. Також розповідайте дітям про важливість онлайнової репутації й про те, як правильно її формувати. Між приватним та професійним життям педагогів завжди має бути чітка межа, зокрема, й у цифровому середовищі;

- для будь-яких контактів між співробітниками закладу освіти та здобувачами освіти або батьками завжди необхідно використовувати корпоративну електронну пошту. Комунікаційна політика закладу освіти може забороняти будь-які контакти, не пов'язані з освітньою діяльністю, та контакти на платформах, що не мають стосунку до закладу освіти. На випадок проведення відеоконференцій або занять у віддаленому режимі, заклади освіти мають

установлювати чіткі приписи як для співробітників, так і для учнів (наприклад, що бажано підготувати місце для віддаленого заняття/сеансу зв'язку та подбати про тих, хто перебуває поруч – чи то вдома, чи то в класі).

Вчителі мають розуміти, чим інтернет може бути для учнів небезпечний і чим корисний. З рекомендаціями щодо захисту дітей в мережі «Інтернет» можна докладно ознайомиться у Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі, розробленими Міжнародним союзом електрозв'язку (МСЕ) та робочою групою авторів із провідних установ, що працюють у індустрії інформаційно-комунікаційних технологій (ІКТ) і переймаються проблемами захисту дитини (в цифровому середовищі), зокрема за посиланням https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za-initsiativi-mintsifripidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP-Guidelinesfor-Parents-Educators-UAfin.pdf.

Для безпеки педагогів експерти радять створити окремий обліковий запис або окремого користувача, якщо ділите вдома чи на роботі свій пристрій ще з кимось, і також розмежувати ваші власні електронні скриньки для особистого користування та для робочих питань. Необхідно також звертати особливу увагу на пересилання персональної інформації (власної або здобувача освіти) через соціальні мережі, різноманітні месенджери, електронною поштою.

Захист персональних даних – це спільна робота педагогів, батьків та учнів. Тому важливу роль у тому, чи буде дистанційне навчання успішним, якісним та безпечним для дитини, відіграють батьки. Батькам треба розповідати дітям про персональні дані, про небезпеку їхнього поширення і правила поводження з ними.

Рекомендації для батьків:

1. Спілкуйтеся зі своїми дітьми, цікавтеся, що вони люблять переглядати в інтернеті, спробуйте організувати спільно з ними будь-яку онлайнову діяльність.
2. Визначте, які технології, пристрої та послуги використовуються у вас вдома.
3. Встановіть на всіх пристроях брандмауер та антивірусну програму.

Поміркуйте над тим, чи будуть корисними та чи підходять для вашої родини програми фільтрації, блокування або відстеження. Розгляньте 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.

4. У колі родини домовтеся 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.
5. Поясніть 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'ятайте про недоторканність приватного життя вашої дитини!
6. Поясніть дітям, що не можна повідомляти свої паролі доступу друзям або братам і сестрам. Звертайте їхню увагу на те, коли і де вони повідомляють свою

персональну інформацію – наприклад, навчайте, що в загальнодоступному профілі краще використовувати деперсоніфіковані зображення як фотографії профілю і вказувати мінімум персональної інформації, такої як вік, школа та місце проживання.

7. Зверніть 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.

8. Дізнайтеся, як повідомити про проблему на платформах, якими користуються ваші діти, і як видалити профіль або змінити зазначену в ньому інформацію.

9. Розкажіть про важливість персональної інформації. Поясніть 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. Нагадайте дітям, що в них є онлайн репутація, за якою необхідно стежити, а після того, як контент опубліковано, його може бути складно змінити або скорегувати.

10. Переконайтеся, що діти розуміють, що означає публікація світлин та відео в інтернеті, в тому числі їхніх власних та їхніх друзів. Поясніть дітям, що фотографії та відео можуть розкривати безліч персональної інформації. Діти повинні розуміти ризики, пов’язані з використанням камер та опублікуванням контенту. Бажано, щоб світлини інших людей не викладалися без їхньої згоди. Це також стосується і батьків, які роблять та публікують знімки своїх дітей. Крім того, важливо, щоб діти розуміли, що іноді інформацію може розкрити хтось із їхніх друзів або членів сім’ї, тому їм варто поговорити про це зі своїми друзями та родичами і розповісти про небезпеку надмірного розкриття інформації. Порадьте своїм дітям не викладати власні фото та відео або фото та відео друзів, на яких є елементи, що легко піддаються ідентифікації, наприклад, таблички з назвами вулиць, автомобільні номери або назва закладу освіти.

Всі учасники освітнього процесу повинні з повагою ставтеся один до одного, адже безпека як очного, так і дистанційного навчання залежить від педагогів, батьків, здобувачів освіти.

Правила інформаційної війни: як не нашкодити і бути корисним в інтернеті.

Національна гвардія України закликала громадян, які не можуть допомагати на полі бою чи займатися волонтерством, вступати у боротьбу з ворогом в інформаційній війні.

Для цього необхідно дотримуватись кілька правил на інформаційному фронті:

1. Інформація, котру ви поширюєте у мережах і серед знайомих повинна бути корисною. Корисна інформація виконує завдання, котрі пришвидшують нашу перемогу. Вона може підіймати бойовий дух наших воїнів, волонтерів і працівників галузей критичної промисловості. Вона може демотивувати ворога. Може підтримувати вимушених переселенців. Корисна інформація повинна мати ціль, а перед поширенням будь-якої інформації варто задати собі питання: а який ефект вона має спричинити? Якщо ви розумієте користь – тоді поширюйте.

2. Якщо ви хочете бути максимально корисними на інформаційному фронті, то не варто продукувати і ділитися великою кількістю матеріалів, котрі мають різні (часом протилежні) меседжі. Найкращий ефект буде тоді, коли ви методично і постійно будете популяризувати одну або кілька позицій, думок чи закликів. Наприклад, українці зі всього світу допомогли українським дипломатам добитися відключення Росії від системи SWIFT, тому що на порядку денному це питання було найпомітніше і про нього говорили і політики, і журналісти, і громадський сектор і звичайні громадяни. Якщо спільно тиснути в одну точку – це прискорить прогрес.

3. Будьте обережні з неперевіреною інформацією і фейками. Нам може здаватися, що якщо фейк пришвидшить нашу перемогу, то це корисний фейк, проте тут є певний підступ. Річ у тім, що ейфорія спричинена фейком дуже швидко може переростати у розчарування і недовіру. А недовіра - дуже добрий ґрунт для ворожої пропаганди. Важливу чи підозрілу інформацію краще перевіряти на офіційних сторінках командування і у якісних медіа.

4. На інформаційному фронті краще боротися групами. Зараз є безліч ініціатив, котрі працюють як на українську аудиторію, так і для людей за кордоном. Хтось через комунікацію з медіа, хтось через спілкування з іноземцями на пряму, хтось записує відео різними мовами, а хтось перекладає матеріали і збирає докази російських військових злочинів. Кожен може знайти собі застосування. Для пошуку найвідповіднішого для вас завдання використовуйте гештеґи. Це допоможе організуватися і знайти однодумців.

5. Не нашкодь. До інформації потрібно ставитися відповідально. Наші військові не раз просили не вести прямі трансляції обстрілів, бо це може допомогти ворогу у коригуванні вогню. Також пам’ятайте, що ваші фото мають зашиті в собі геолокацію, тому дуже обережно фотографуйте і діліться світлинами, котрі зроблені поруч з позиціями українських військових чи стратегічними об’єктами.

Розділ 2. Забезпечення кібербезпеки на рівні закладу освіти

2.1. Вплив кіберзагроз на учасників освітнього процесу

Кібербезпека – це безпека IT систем (обладнання і програм). Наскільки ваш комп'ютер або веб-сайт захищений від хакерської атаки – це саме і є питання кібербезпеки. Кібератака – це спроба реалізації загрози. Тобто, це дії кіберзловмисників або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Кібератаки – це загальна термінологія, яка охоплює велику кількість тем:

- порушення цілості систем і даних, що зберігаються всередині,
- несанкціонований доступ до конфіденційної інформації,
- порушення нормального функціонування організації,
- використання атак для шифрування даних і вилучення грошей у жертви.

Атаки становляться все більш інноваційними, що може порушити безпеку та взломати систему. Тому дуже складно подолати цю проблему та дати відсіч цим атакам. Більшість сучасних кібератак вважаються змішаними атаками. Змішані атаки використовують одразу кілька методів, щоб проникнути до системи і здійснити атаку. Коли атаці неможливо запобігти, завдання експерта з кібербезпеки полягає у зменшенні наслідків нападу. Щоб зрозуміти необхідність заходів кібербезпеки, коротко розглянемо типи загроз та атак.

I. **Віруси вимагачі** (Ransomware - англ. ransom — викуп і software — програмне забезпечення). Це шкідливе програмне забезпечення, яке блокує пристрій або шифрує його вміст, вимагаючи гроші у жертв. За певну плату оператори шкідливого коду обіцяють відновити доступ до інфікованої машини або даних. Серед сумнозвісних шифрувальників, які шкодили користувачам Windows – WannaCry, Bad Rabbit і Petya.

У більшості випадків програма-вимагач відображає на екрані повідомлення, що ваш комп'ютер заблокований, або додає текстовий файл (повідомлення) до відповідних папок. Багато сімейств програм-вимагачів також змінюють розширення зашифрованих файлів.

Як працює програма-вимагач? Оператори програм-вимагачів використовують багато різних технік інфікування:

- шифрування диску та блокування доступу користувача до операційної системи,
- блокування екрану користувача,
- шифрування даних на диску жертви,
- блокування пристроїв Android шляхом зміни коду доступу для заблокування пристрою користувача.

Загроза захована усередині іншого файлу або програми, яка виглядає настільки безвинно, що користувач спокійно їх відкриває: вкладення в електронні листи, відео зі сторінок сумнівного походження або навіть системні оновлення від особи надійних програм, таких як Windows або Adobe Flash. Після завантаження на комп'ютер шкідлива програма активується і блокує всю операційну систему,

після чого запустить попередження із загрозою і з зазначенням суми викупу, яку треба заплатити за «порятунок» всієї інформації. Ці повідомлення розрізняються залежно від типу шкідливої програми з якою Ви зіткнулися: піратський контент, порнографія, помилковий вірус. Щоб додатково налякати жертву, іноді додається IP-адрес, назви Вашого інтернет-провайдера або навіть фотографія, перехоплена з Вашої вебкамери. При цьому комп'ютер залишається працездатним, але всі файли користувача виявляються недоступними. Інструкцію та пароль для розшифрування файлів зловмисник обіцяє прислати за гроші. Однак немає ніякої гарантії, що кіберзлочинці виконають свою обіцянку (а іноді вони не можуть це зробити навмисно або через некомпетентне кодування).

Є декілька способів, які допоможуть захистити комп'ютер від здирників та інших шкідливих програм:

- Регулярне оновлення компонентів операційної системи.
- Тримати програмне забезпечення на комп'ютері в актуальному стані оновлюючи його.
- Тримати увімкненим мережевий екран.
- Не відкривати спам–повідомлення електронної пошти та не відвідувати підозрілі вебсайти.
- Використовувати відомі антивіруси для захисту від шкідливих програм та оновлювати антивірусні бази.
- Перед першим запуском нових програм перевіряти їх антивірусом.
- Періодично виконувати резервне копіювання важливих даних.

II. **Атаки ботнетов.** Ботнет — це мережа комп'ютерів, інфікована шкідливим програмним забезпеченням. Кіберзлочинці використовують ботнет-мережі, які складаються з великої кількості комп'ютерів для різних зловмисних дій без відома користувачів.

Деякі з атак ботнетів включають:

- Розподілені атаки типу «відмова в обслуговуванні» (DDoS – Distributed Denial of Service).
- Розповсюдження спам-листів.
- Крадіжка конфіденційних даних.
- Встановлення шпигунських програм.

Комп'ютер може потрапити в мережу ботнету через встановлення певного програмного забезпечення, без відома користувача.

Трапляється це зазвичай через:

- Інфікування комп'ютера вірусом через вразливість в ПЗ (помилки в браузерах, поштових клієнтах, програмах перегляду документів, зображень, відео).
- Недосвідченість або неуважність користувача — шкідливе ПЗ маскується під «корисне програмне забезпечення».

– Використання санкціонованого доступу до комп'ютера (рідко). – Підбір адміністративного пароля до мережевих ресурсів зі спільним доступом (наприклад, до $ADMIN, що дозволяє віддалено виконати програму) — переважно в локальних мережах.

Якщо комп’ютер став частиною ботнет-мережі, то це може негативно впливати на роботу комп’ютера. Обчислювальна потужність одного ботнету дозволяє здійснювати декілька зловмисних дій швидко та часто без виявлення.

Наприклад, у 2016 році ботнет був використаний для створення найбільшої DDoS-атаки в історії, яка спричинила збої у роботі таких сайтів як Twitter, Amazon та Netflix.

Щоб не стати частиною ботнету, важливо дотримуватися таких правил безпеки:

– Виконувати регулярне оновлення програмного забезпечення та виправлення помилок.

– Використовувати рішення для забезпечення безпеки в Інтернеті, до яких входить захист від ботнет–атак. Такі рішення виявляють та блокують загрози та використовують брандмауер (Брандмауер (Brandmauer) – це комп'ютерна програма, метою якої є захист комп'ютера від вірусів і хакерських атак) для фільтрації зв'язку між комп'ютером та інтернетом.

– Необхідно бути обережним, завантажуючи файли або програми та відкриваючи вкладення.

3. **Атаки соціальної інженерії.** Низка не технічних прийомів маніпулювання користувачами, які використовуються кіберзлочинцями під час атак. Соціальна інженерія – поширена тактика, яку використовують кіберзлочинці для збору конфіденційної інформації користувача. Вся інформація, яку вводить користувач, клонується та використовується для фінансових шахрайств, шахрайства з ідентифікацією тощо. Варто сказати про вірус ZEUS, який активний з 2007 року та використовується як метод соціальної атаки для крадіжки банківських даних жертв. Поряд із фінансовими втратами атаки соціальної інженерії здатні завантажувати інші руйнівні загрози для відповідної системи. Більшість методів соціальної інженерії не вимагають особливих технічних знань з боку зловмисників, а отже використовувати ці методи може будь-хто — від дрібних злодіїв до досвідчених кіберзлочинців. Існує багато методик, які підпадають під загальний термін соціальної інженерії в галузі кібербезпеки. Серед найвідоміших методик — спам та фішинг.

Спам — це масове розсилання небажаних листів. Найчастіше спам — це лист електронної пошти, який надсилається одразу на велику кількість адрес, але він також може бути доставлений через миттєві повідомлення, SMS та соціальні мережі. Власне, спам не є соціальною інженерією, однак в деяких кампаніях використовуються його види, такі як фішинг, цілеспрямований фішинг (spearphishing), вішинг (vishing), смішинг (smishing), а також поширення шкідливих вкладень або посилань.

Фішинг (саме слово є омофоном англійського слова «Fishing» (рибалка), оскільки техніка використовує ту ж логіку «вилову») — це форма кібератаки, під час якої злочинець намагається завойовувати довіру жертви для виманювання конфіденційної інформації. Для отримання даних зловмисники також створюють відчуття терміновості або застосовують тактику залякування. Варто зазначити, що фішингові кампанії можуть бути націлені на велику кількість випадкових користувачів або конкретну особу чи групу. Цілеспрямований фішинг — це форма фішингу, під час якої зловмисник надсилає повідомлення, спрямовані на конкретну групу людей, або навіть просто окрему особу з метою викрадення даних або маніпулювання ними в зловмисних цілях. Вішинг та смішинг — це методи соціальної інженерії, подібні до фішингу, але здійснюються не через електронну пошту. Зокрема, вішинг реалізовується через шахрайські телефонні дзвінки, а для смішингу використовуються текстові SMS-повідомлення, які містять шкідливі посилання або вміст.

Яскравий приклад — дзвінок нібито з банку. Зловмисники, вдаючи із себе співробітників банку, вигадують різні приводи для виманювання даних. Наприклад, кажуть, що відбулося блокування карти, і служба безпеки банку проводить звіряння особистих даних клієнтів для убезпечення їх від шахрайства. Іншим прикладом є схеми типу «Ваш родич потрапив в аварію чи поліцію». Найчастіше зловмисники здійснюють такого роду дзвінки вночі або рано вранці, коли людина сонна, погано міркує. Шахраї здебільшого розмовляють чітко, впевнено та помірно швидко, щоб не дати змоги жертві зважити ситуацію та поміркувати. При дзвінках «із поліції» шахраї роблять ставку на розгубленість жертви та застосовують методи психологічного тиску, змушуючи особу «вирішувати справу зараз і вже, оскільки немає часу зволікати». SMS-фішинг (смішинг) — різновид фішингу, який здійснюється через SMSрозсилки. Одним із яскравих прикладів є SMS-повідомлення нібито про виграш великої суми грошей або автомобіля. Однак, щоб отримати виграш, потрібно внести 10% за «оформлення» необхідної документації тощо. Також SMS-шахрайством є повідомлення від «банків». «Дорожнє яблуко» («road apple»), або «Троянський кінь», — це метод атаки, який передбачає підкинути співробітнику компанії чи установи фізичний носій інформації (флеш-накопичувач, диск) зі шкідливим програмним забезпеченням. Носій може мати логотип компанії чи надпис, що зацікавить співробітника, наприклад, «Список на звільнення», «Заробітна плата. Жовтень» тощо. Щойно співробітник вставить такий носій у комп'ютер, він запустить шкідливий код, який надасть хакеру віддалений доступ до мережі. Шкідливе програмне забезпечення, ціль якого викликати у жертви почуття страху чи тривоги та таким чином змусити її встановити небезпечний код на пристрій. Поширеними є випадки, коли користувачам відображалось повідомлення про нібито інфікування пристрою загрозою, для видалення якої необхідно завантажити антивірус (який, насправді, є шкідливим програмним забезпеченням).

«Зворотна соціальна інженерія» — це вид соціальної інженерії, за якої особа сама звертається до шахрая та повідомляє свої конфіденційні дані. Одним із можливих сценаріїв є, коли шахрай надсилає співробітникам компанії нібито

нові номери телефонів служби технічної підтримки. Цілком імовірно, що через певний час хтось із співробітників зателефонує і шахрай зможе вивідати інформацію, яка його цікавить. Складна атака через проміжну ціль («Supply chain attack») — це кількаступенева атака, в ході якої хакер атакує не напряму організацію, яка його цікавить, а менш захищену проміжну організацію чи установу, а вже через неї компрометує ту ціль, яка від самого початку його цікавила.

Наприклад, хакер обрав своєю ціллю банк, однак після його вивчення зрозумів, що установа має високий рівень захисту і просто так її не скомпрометувати. У такому разі хакер може сфокусуватися на атаці підрядників, наприклад, на невеликій компанії, яка розробляє або обслуговує сайт чи бази даних банку. Невеликі компанії зазвичай менш захищені, а тому скомпрометувати їх набагато простіше. Як здійснюються атаки з використанням соціальної інженерії? Існує декілька ознак, які допоможуть ідентифікувати таку атаку. Зокрема, одна з них — погана граматика та правопис. Ще однією ознакою є почуття терміновості, яке зловмисники намагаються створити для зменшення пильності жертви. Будь-який запит щодо конфіденційних даних також має викликати підозру: авторитетні компанії ніколи не просять відправити їм паролі або інші особисті дані електронною поштою або текстовими повідомленнями.

Деякі з ознак, які допоможуть виявити соціальну інженерію:

1. Граматика і лексика. Зазвичай, зловмисники не приділяють увагу деталям та надсилають повідомлення з помилками, пропущеними словами та поганою граматикою. Ще один мовний елемент, який може сигналізувати про можливу атаку — це формальні привітання та фрази.
2. Адреса відправника. Більшість зловмисників не витрачають час на створення правдоподібного імені або домена відправника. Отже, якщо електронний лист надходить з адреси, яка є набором випадкових чисел та символів, або одержувач взагалі невідомий, варто перемістити цей лист до папки спам.
3. Почуття терміновості. Злочинці часто намагаються залякати жертв за допомогою фраз, які викликають тривогу, наприклад «терміново надішліть нам свої дані, або ваша посилка буде скасована» або «якщо ви не оновите свій профіль зараз, ми його видалимо». Банки, компанії з доставки, державні установи і навіть внутрішні відділи, зазвичай, спілкуються нейтрально і лише констатують факт. Тому, якщо у повідомленні намагаються змусити одержувача діяти дуже швидко, це може бути ознакою атаки.
4. Запит на конфіденційну інформацію. Офіційні установи та навіть відділи компанії, зазвичай, не вимагають надсилання конфіденційної інформації електронною поштою або телефоном, якщо про це попередньо не домовлялися.
5. Щось звучить занадто добре, щоб бути правдою. Це стосується розіграшів подарунків у соціальних мережах, а також електронних листів з унікальними та обмеженими пропозиціями.

Способи захисту закладу від атак з використанням соціальної інженерії: 1. Регулярне навчання з кібербезпеки усіх працівників. Таке навчання повинно показувати та моделювати випадки з реального життя, оскільки методи

соціальної інженерії розраховані на користувачів з низьким рівнем обізнаності у кібербезпеці.

2. Здійснювати сканування на наявність слабких паролів, які потенційно можуть використати зловмисники для потрапляння до мережі вашого закладу. Крім того, створіть додатковий рівень захисту за допомогою двофакторної аутентифікації.

3. Впровадження рішення для захисту, які попереджають про можливі випадки шахрайства, а також повідомляють про виявлення спаму та фішингу.

4. Створення політики безпеки з чітким планом дій, які потрібно буде виконати працівникам, якщо вони стикнуться з проявами соціальної інженерії.

5. Використовувати рішення для централізованого управління корпоративною мережею, наприклад, ESET Security Management Center, щоб забезпечити повний огляд мережі, усіх рішень з безпеки та подій для виявлення та знешкодження потенційних загроз.

III. **Онлайн (online) та офлайн (offline)-ідентифікація.** Захист особистих даних. Інтернет — це невід'ємна частина нашого життя. Він є глобальною системою взаємозалежних комп'ютерних мереж. Інтернет є мережею мереж, що дає можливість створення кіберпростору, де відбувається онлайнова комунікація. Кіберпростір ще називають віртуальною реальністю. Віртуальна реальність — це ілюзія дійсності, створена за допомогою комп'ютерних систем, які забезпечують зорові, звукові та інші органи чуття. Чим більше часу ви проводите в Інтернеті, тим сильніше на ваше життя може вплинути ваша ідентичність як в Інтернеті, так і в офлайні.

Офлайн-ідентичність – це ви самі, особа, з якою ваші друзі та сім'я взаємодіють щодня вдома або на роботі. Оточуючі знають ваші персональні дані, а саме ваше ім'я, вік або місце проживання. Ваша ідентичність в інтернеті - це ви у кіберпросторі. Ваша онлайн-ідентичність – це те, як ви представляєте себе іншим в інтернеті. Ця онлайн-ідентичність має розкривати лише мінімум інформації про вас. Будьте обачні, обираючи ім'я користувача або псевдонім для себе в інтернеті. Ім'я користувача не повинно містити жодної особистої інформації. Це має бути щось доречне і прийнятне. Ім'я користувача не повинно давати привід стороннім людям подумати, що ви є легкою ціллю для кіберзлочинців або хочете привернути небажану увагу. У віртуальному світі інтернету ми постійно стикаємося з проблемою забезпечення приватності. Згідно зі статтею 8 Європейської конвенції з прав людини, приватність закріплюється як окремий аспект приватного життя. Ніхто не має права збирати та поширювати інформацію про наше приватне життя. Особиста інформація, якою ми не хочемо ділитися, має залишатися конфіденційною, не підлягати розголосові. Питання збереження приватності в мережі «Інтернет» є актуальним, оскільки віртуальне спілкування практично ніколи не буває приватним. Інформація, що поширюється в режимі онлайн електронною поштою, соцмережами тощо легко може бути доступна іншим. Від неї також неможливо повністю позбутися. Недостатня захищеність інформації та своїх профілів створює ризик доступу до неї інших людей і її використання без дозволу. Користувачі інтернету самі несуть відповідальність за захист відомостей про своє життя. Будь-яка інформація про вас може вважатися вашими персональними даними. Ця персональна інформація

може однозначно ідентифікувати вас як особистість. Ці дані містять фото та повідомлення, якими ви обмінюєтесь з родичами та друзями в Інтернеті. Інша інформація, така як ім'я, номер соціального страхування, дата і місце народження або дівоче прізвище матері, відома лише вам і використовується для встановлення вашої особистості. Такі відомості, як медична, освітня, фінансова інформація та дані про працевлаштування також можуть бути використані для ідентифікації вас в інтернеті.

Відповідно до Закону України «Про захист персональних даних»: **Персональні дані** – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Зокрема, прізвище, ім’я, по батькові, адреса, телефони, паспортні дані, національність, освіта, сімейний стан, релігійні та світоглядні переконання, стан здоров’я, матеріальний стан, дата і місце народження, місце проживання та перебування тощо. Незаконне отримання та оприлюднення (поширення) чужої особистої інформації є злочином.

Підраховано, що кожна п'ята людина віком від 18 років ставала жертвою кібератаки в соціальних мережах або через мобільні пристрої. Найчастіше метою отримання особистих даних є доступом до банківських рахунках. Ваші дані в Інтернеті завжди мають певну цінність для кіберзлочинців.

Важливо! За порушення недоторканості приватного життя, а саме за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації винна особа притягується до кримінальної відповідальності (стаття 182 Кримінального кодексу України) Комп'ютерні пристрої зберігають ваші дані та є порталом до вашого онлайн-життя.

Навіщо та кому можуть знадобитися ваші особисті дані?

– Ними можуть скористатися рекламодавці (для збільшення кількості розсилок).

– Чужі особисті дані використовуються для отримання кредитів та крадіжок коштів із банків.

– Дані можуть бути викрадені з хуліганських спонукань (оприлюднити листування, наприклад).

– Дані можуть бути викрадені для подальшого перепродажу.

– Витік даних можливий з комп'ютера, ноутбука, мобільного пристрою. При цьому дані потрапляють до кіберзлочинців через інтернет, електронну пошту.

– Цінність для зловмисників є і облікові записи електронної пошти. Адреса електронної пошти може бути використана для підтвердження реєстрації на інших вебсайтах. Цікаво, що поняття «витік персональних даних» в англійській мові відповідає Identity theft (крадіжка особистості). Запровадження дистанційного навчання на початку пандемії спонукало педагогічних працівників швидко шукати способи, інструменти та електронні канали комунікації для його проведення і

взаємодії з учнями та батьками. Цифровізація освітнього процесу й робота з технологіями дистанційного навчання вже помітно вплинула на те, як відбувається освітній процес. З одного боку значно розширилися і продовжують розширюватися можливості педагогів проводити навчання, а учнів – навчатися. З іншого – використання цих методів, технологій та інструментів тісно пов'язане з безпекою роботи, зокрема, використанням та обробкою персональних даних учасників освітнього процесу. Способи захисту особистих даних:

1. Створення складних паролів. Як правило, ми маємо більше ніж один обліковий запис в інтернеті, і для кожного з них слід використовувати унікальний пароль. Таким чином, доводиться пам'ятати багато паролів. Проте, нехтування правилом використання сильних та унікальних паролів залишає дані вразливими для кіберзлочинців. Використання однакового пароля для усіх облікових записів в інтернеті – це те саме, що й використання одного ключа для замикання усіх дверей. менеджери паролів допоможуть генерувати складні та унікальні паролі для кожного сайту та тримати їх в одному місці. Менеджери паролів допоможуть генерувати складні та унікальні паролі для кожного сайту та тримати їх в одному місці. Менеджер паролів (1password, LastPass, KeePass) допомагає автоматично входити до облікових записів в Інтернеті, потрібно лише пам'ятати майстер-пароль, щоб отримати доступ до менеджера паролів і керувати всіма обліковими записами та паролями. Онлайн-сервіси, такі як Google, Facebook, Twitter, LinkedIn, Apple та Microsoft, використовують двофакторну аутентифікацію для забезпечення додаткового рівня захисту при вході до облікових записів.

Крім імені користувача та пароля, або особистого ідентифікаційного номера (PIN) чи шаблону, для двофакторної аутентифікації іноді потрібен додатковий токен безпеки, такий як:

– Фізичний об'єкт – кредитна картка, телефон або ключ–брелок.

– Біометричне сканування - відбиток пальця, відбиток долоні, розпізнавання обличчя або голосу.

Навіть якщо використовується двофакторна аутентифікація хакери можуть отримати доступ до ваших облікових записів в інтернеті через такі атаки, як фішинг, зловмисне програмне забезпечення та соціальна інженерія.

2. Шифрування повідомлень. Шифрування – це процес перетворення інформації у форму, в якій неавторизована сторона не зможе її прочитати. Більшість месенджерів вже використовують шифрування. Наприклад, WhatsApp пропонує шифрування з 2016 року. Це означає, що ніхто не зможе побачити ваше повідомлення, окрім отримувача. Крім того – в месенджерах є секретні чати. Але експерти більше довіряють Telegram. А найзахищеніший і зовсім непопулярний в нас месенджер – Signal.

3. Не підключатися до громадського WiFi. Громадські мережі не завжди захищені паролем. Підключатись до відкритого WiFi – погана ідея. Хакери можуть створитимережу – двійника із такою ж назвою та перехопити дані.

Публічні Wi-Fi точки доступу (hot spot) дають змогу отримувати доступ до особистої онлайн-інформації та мандрувати Інтернетом. Тим не менш, краще не підключитися і не надсилати будь-яку важливу особисту інформацію через загальнодоступну бездротову мережу.

4. Використання протоколу HTTPS. Цей протокол більш безпечний, ніж HTTP, він шифрує всю інформацію та захищає від атак. Необхідно слідкувати, аби HTTPS обов'язково був в адресному рядку сайтів, де ми залишаємо дані банківської карти.

IV. **Захист організації.** Міжмережний екран (фаєрвол, брандмаурер) – це стіна або перегородка, яка призначена для запобігання поширенню вогню з однієї частини будівлі в іншу. Міжмережевий екран (МЕ) виявляє та блокує мережевий трафік на основі попередньо визначених або динамічних правил. Вони захищають мережі та пристрої від вторгнення потенційно небезпечних кіберзлочинців, які можуть інфікувати пристрої та використовувати їх у зловмисних цілях. МЕ служить захисною стіною між локальною мережею та зовнішньою мережею і запобігає будь-яким загрозам. Він призначений для контролю вхідного і вихідного трафіку на комп'ютері або в локальній мережі, дає змогу припиняти практично всі види мережевих атак, вирізати рекламу, відключати банери, рекламні скрипти, вспливаючі вікна та інше, не надсилати іншим «чужим» серверам інформацію про ваш комп'ютер, робить даремною роботу програм-троянів і засобів віддаленого адміністрування. Робота МЕ полягає в аналізі структури і вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і в залежності від результатів аналізу пропускає пакети у внутрішню мережу (сегмент мережі) або повністю їх відфільтровує. Головна функція брандмауера — фільтрація шкідливого та потенційно небезпечного контенту та з'єднань.

Розрізняють два типи МЕ: апаратний і програмний. Апаратний являє собою пристрій, який фізично підключається до мережі. Цей пристрій відслідковує всі аспекти вхідного і вихідного обміну даними, а також перевіряє адреси джерела і призначення кожного оброблюваного повідомлення, що забезпечує безпеку, допомагаючи запобігти небажаним проникненням в мережу або комп'ютер. Програмний виконує ті ж функції, але використовує не зовнішній пристрій, а програмний продукт, який запущений на кінцевому комп'ютері або шлюзі. Найбільшого розповсюдження отримав програмний тип реалізації МЕ.

Існує кілька типів брандмауерів із різними видами фільтрування трафіку:

- Брандмауер першого покоління працює як пакетний фільтр, порівнюючи основну інформацію, таку як оригінальне джерело, призначення пакета, використовуваний порт чи протокол, з визначеним переліком правил.
- Друге покоління брандмауера містить ще один параметр для налаштувань фільтра — стан з'єднання. На основі цієї інформації технологія може відслідковувати дані про початок з'єднання та поточні з'єднання.

– Брандмауери третього покоління побудовані для фільтрування інформації за допомогою усіх рівнів моделі OSI, зокрема і прикладного рівня. Вони розпізнають програми та деякі широко поширені протоколи, такі як FTP та HTTP.

На основі цієї інформації брандмауер може виявляти атаки, які намагаються обійти його через дозволений порт або несанкціоноване використання протоколу. Нові фаєрволи все ще належать до третього покоління, однак їх часто називають «наступним поколінням» або NGFW. Даний вид поєднує всі раніше використані підходи з поглибленим оглядом відфільтрованого контенту та його порівнянням з базою даних для виявлення потенційно небезпечного трафіку.

Сучасні брандмауери часто мають вбудовані додаткові системи безпеки, наприклад віртуальні приватні мережі (VPN), системи запобігання та виявлення вторгнень (IPS/IDS), управління ідентифікацією, управління додатками та веб-фільтрація. Переваги використання брандмауера: він забезпечує покращення безпеки та захист пристроїв від шкідливого вхідного трафіку. Також технологія може фільтрувати вихідний трафік. Це допомагає зменшити ймовірність викрадення даних зловмисниками. Крім цього, важлива функція брандмауера полягає у зменшенні ризику пристроїв стати частиною ботнету — шкідлива мережа з великою групою пристроїв, що управляється кіберзлочинцями.

2.2. Захист інформаційних систем та мереж закладу

Безпека та цифровий світ. ІКТ можуть зробити позитивний внесок у справу створення безпеки у сучасному цифровому освітньому середовищі. Але технології також можуть зашкодити довірі до такого середовища, наприклад, через хибні новини або непродумані алгоритми. У освіті, як зазначають нідерландські педагоги, ми маємо справу з уразливою цільовою групою – дітьми. Тому безпека, конфіденційність і довіра є важливими поняттями в освіті. Захист конфіденційності, надійність алгоритмів, постійно зростаючий збір даних – це ті важливі аспекти, на яких зосереджена увага освітян.

Комп'ютерна безпека – це сукупність проблем у галузі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами і розглядуваних з точки зору конфіденційності, цілісності і доступності.

Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення: «Кібербезпека – 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 і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі».

У сучасному розумінні культура – це складний суспільний феномен життєдіяльності людини, що стосується побуту, дозвілля, способу життя як окремої особи, так й усього суспільства. У філософії культура (матеріальна і духовна категорія) розглядається у всесторонньому історичному розумінні як: процес розвитку людських сил і здібностей; показник міри людського в людині;

характеристика розвитку людини як людської істоти; процес освоєння природи, який одержує своє зовнішнє вираження у всьому багатстві і різноманітті створюваної людьми дійсності, у всій сукупності результатів людської праці і думки. При цьому, на думку більшості сучасних філософів, в структурі феномена культури можна виділити два класи елементів. Перший характеризує культуру як систему еталонів суспільної поведінки людей, другий – як систему, що здійснює соціальний контроль над цінностями та ідеями. Вочевидь, у контексті запобігання кіберзлочинності доцільно розглядати матеріальну культуру в розумінні системи еталонів суспільної поведінки людей.

Отже, виходячи із завдань запобігання кіберзлочинності варто звернути увагу на психологічний, правовий та соціологічний аспекти культури суспільства, особистості соціальної взаємодії з формування досвіду, розвитку форм та способів інформаційної діяльності у кіберпросторі.

Культура кібербезпеки – це система переконань, уявлень та етичних норм щодо ведення інформаційної діяльності у кіберпросторі, знань, вмінь та навичок із забезпечення кібербезпеки, а також вимоги до професійно-психологічних якостей осіб, що необхідні для безпечної інформаційної діяльності у кіберпросторі. Історично, термін «культура кібербезпеки» був використаний у глобальному розумінні в Резолюції Генеральної Асамблеї «Створення глобальної культури кібербезпеки» (Creation of a global culture of cybersecurity) у 2002, 2003 та 2009 роках, хоча у цих документах не запропоновано його визначення. Зазначені документи були запропоновані як рекомендації для розроблення національних стратегій кібербезпеки, що визначають сутність національних систем кібербезпеки та заходи з поширення передових практик кіберзахисту.

Ще десять років тому небезпеки для учасників освітнього процесу можна було звести до відносно невеликої кількості груп – вірусні атаки, кіберзлочинність, небезпеки інтернет-серфінгу. На часі розмаїття небезпек і загроз зростає постійно. Найбільшу загрозу для здобувачів освіти мають приховані активні небезпеки. Серед них мережні загрози. Активне використання мереж, особливо підлітками, супроводжується збільшенням різних видів загроз, що надходять з мережі.

Найбільш активні приховані загрози, що походять з комп’ютерної мережі, можуть бути представлені наступною класифікацією:

- вірусні атаки;
- кіберзлочинність (спамерство, кардінг, фішинг, ботнети тощо);
- загрози від мережевого серфінгу (кібербулінг, «дорослий» контент, незаконний вміст, насильство в режимі онлайн, розголошення приватної інформації, платні послуги тощо).

Загрози, що надходять з мереж, можна розділити на наступні типи: активні та пасивні, відкриті та приховані, поточні та відкладені.

Як свідчать останні дослідження щодо кібербезпеки, інформаційно-технічні засоби в цій сфері постійно вдосконалюються і хакерські атаки переорієнтовуються більше не на техніку, а на людину. Це особливо важливо враховувати через гостроту питання особистої безпеки та результатів діяльності

людей. «Відкриваючись» під час роботи в інформаційному середовищі, людина стає не тільки предметом, а й об'єктом діяльності інших учасників інформаційного простору.

Зміщення цілей кіберзлочинності з технічних (інформаційних) об'єктів на людину спричинило появу соціальної інженерії як методів і технологій отримання необхідного доступу до інформації, заснованих на особливостях психології людей, зокрема – маніпуляція людськими страхами, зацікавленістю або довірою [2]. Основними типами соціальної інженерії на часі можна вважати наступні:

- **Претекстін**г – це набір дій, відпрацьованих за певним, заздалегідь складеним сценарієм, у результаті якого жертва може видати будь-яку інформацію або вчинити певну дію. Для використання цієї техніки зловмисник спочатку збирає певні дані про жертву (ім'я, місце навчання та проживання; дату народження; дані про батьків), використовуючі реальні запити з іменами щодо оточення жертви, а після того, як увійде в довіру, отримує необхідну йому інформацію або дії.
- **Фішин**г – техніка інтернет-шахрайства, спрямована на отримання конфіденційної інформації користувачів авторизаційних даних різних систем. Основним видом фішингових атак є підроблений лист, відправлений жертві електронною поштою, який виглядає як офіційний. У листі міститься форма для введення персональних даних (пінкодів, логіна і пароля тощо) або посилання на web-сторінку, де розташовується така форма.
- **Троянський кінь** – це техніка ґрунтується на цікавості, страху або інших емоціях користувачів. Зловмисник відправляє лист жертві за допомогою електронної пошти, як додаток, до якого знаходиться «оновлення» антивірусу, ключ до грошового виграшу або компромат на співробітника. Насправді ж у вкладенні знаходиться шкідлива програма, яка після того, як користувач запустить її на своєму комп'ютері, буде використовуватися для збору або зміни інформації зловмисником.
- **Qui pro quo** (послуга за послугу) – ця техніка передбачає звернення зловмисника до користувача по електронній пошті або корпоративному телефону. Зловмисник може представитися, наприклад, співробітником технічної підтримки та інформувати про виникнення технічних проблем на робочому місці та необхідність їх усунення. У процесі «вирішення» такої проблеми, зловмисник підштовхує жертву на вчинення дій, що дозволяють атакуючому виконати певні команди або встановити необхідне програмне забезпечення на комп'ютері жертви.
- **Дорожнє яблуко** – цей метод є адаптацію троянського коня і полягає у використанні фізичних носіїв (CD, флеш-накопичувачів). Зловмисник зазвичай підкидає такий носій у загальнодоступних місцях. Для того, щоб виник інтерес до даного носія, зловмисник може нанести на носій логотип відомої популярної компанії.
- **Байтинг** – метод, схожий на попередній, а також фішинг і троянський кінь, проте відрізняється тим, що байтер може запропонувати користувачеві реальну безкоштовну послугу (музику, фільм тощо) в обмін на конфіденційну

(приватну) інформацію.

- **Зворотня соціальна інженерія** – даний вид атаки спрямований на створення такої ситуації, при якій жертва змушена буде сама звернутися до зловмисника за «допомогою». Наприклад, створити оборотні неполадки в ґаджеті жертви з попереднім інформуванням щодо служби «підтримки». Користувач у такому випадку зателефонує або зв'яжеться по електронній пошті зі зловмисником сам, і в процесі «виправлення» проблеми зловмисник зможе отримати необхідні йому дані.
- **Дружні листи** – надсилання електронних листів, у яких особу повідомляють про отримання спадщини, призів, бонусів чи дружнього переказу грошей.
- **Вішинг** – голосова версія фішінгу. Як правило, дії пов'язані з телефонним шахрайством, метою якого є отримання реквізитів банківських карток або будь-якої іншої конфіденційної інформації або змушення жертви перевести гроші на банківський рахунок зловмисника.
- **Контакти** – розсилання спаму від імені знайомих. Тобто, заволодівши чиїмось акаунтом, чи то в соціальній мережі, чи в електронній пошті, зловмисники можуть спробувати надсилати від його імені посилання. Психологічна дія, що побудована на схильності людини довіряти своїм знайомим і не дуже вагатися, коли отримують від них пропозицію відкрити посилання.

Перераховані засоби широко застосовуються в останні роки для впливу на осіб, що приймають рішення, в політиці та бізнесі. Розроблені та вдосконалюються рекомендації, методи та засоби протидії їм. Проте практично відсутній розгляд дії та протидії методам соціальної інженерії стосовно освітньої сфери, незважаючи на те, що діти та підлітки стають все частіше об'єктами атак через інтернет. Використання засобів протидії для дорослих може бути поширене і на підлітків, але з урахуванням вікових особливостей та сфери діяльності.

Основним способом захисту від методів соціальної інженерії є навчання учасників освітнього процесу. Усі вони (учні, педагоги, батьки) мають бути попереджені про небезпеку розкриття персональної інформації та конфіденційної інформації, а також про способи запобігання витоку даних. Крім того, у кожного учасника, в залежності від місця та функції в освітньому процесі, повинні бути інструкції про те, як і на які теми можна спілкуватися із сторонніми особами стосовно персональних особливостей, яку інформацію можна надавати для служби технічної підтримки, як і яку інформацію може повідомити учасник освітнього процесу стороннім особам і працівникам масмедіа.

Представники Міністерства освіти і науки навряд чи будуть телефонувати до школи, щоб дізнатися дані щодо конкретного учня або студента. Якщо людину просять ввести особисті дані – краще окремо зайти на сайт компанії, наприклад, банку. Ще краще – зателефонувати на офіційний номер установи для уточнення інформації. Ніколи не слід відкривати вміст додатків або переходити за посиланням, не вивчивши всіх деталей. Часто адреса відправника містить помилки в назвах, а посилання мають неправдоподібний вигляд. Варто також критично ставитися до отриманих повідомлень. Рекомендується сповіщати про

такі небезпеки інших членів сімей, насамперед, літніх людей, які не мають досвіду користування електронними засобами та не обізнані з питань соціальної інженерії. Останнім часом в Україні запроваджуються спеціальні навчальні програми і курси для учнів та вчителів, які займаються питаннями безпечного інтернету.

Проблеми кібербезпеки не зводяться лише до технічних аспектів захисту інформаційних ресурсів, у повному обсязі вони мають включати такі види захисту: правові, технічні, інформаційні, організаційні та психологічні. На часі доцільно виокремити роль психологічних засобів забезпечення кібербезпеки, оскільки населення в цілому та особливо діти і підлітки все частіше стають об'єктами кібератак. Загрози учасникам освітнього процесу з боку кіберпростору доцільно розглядати як пасивні та активні, розробляючи адекватні засоби захисту та життєстійкості системи «суб'єкт освітнього процесу – засоби навчання – середовище».

Найбільш значущими серед кіберзагроз для учасників освітнього процесу є методи соціальної інженерії, знання яких та протидія яким можуть бути найбільш ефективними для забезпечення кібербезпеки.

Доступ до мережі «Інтернет» став одним з основних прав людини. Ми користуємось мережею для дозвілля, розваги, роботи, а також забезпечення повсякденного буття – від оплати рахунків до замовлення послуг. Вже залишився позаду той час, коли зловмисники використовували мережу лише для розваги або помсти. Зараз ціль будь-якого зловмисника-хакера – гроші. Кожного з них, перш за все, цікавить фінансова вигода. Тобто дії зловмисних програм, а також спеціальних шкідливих або зламаних чи скомпрометованих сайтів, спрямовані на те, щоб заробити на користувачі. А якщо на вас заробляють, то ви особисто обов'язково щось втратите: гроші, час, репутацію. Найпоширеніші способи нелегального заробітку в мережі «Інтернет»:

– Програми-вимагачі – повністю або частково блокують ваш комп'ютер та вимагають оплату для розблокування.

– Викрадення облікових записів соціальних мереж «Фейсбук», «Твітер», «Інстаграм» тощо для розсилки спаму всім вашим друзям або шантажу з приводу повернення вашої сторінки.

– Викрадення поштових даних – як самої електронної скриньки, так і листів, що знаходяться на комп'ютері, в яких міститься інформація про ваші реєстраційні дані на інших ресурсах.

– Використання комп'ютера у складі bot-net – на тисячі комп'ютерів завантажуються шкідливе програмне забезпечення, яке застосовується для масової розсилки спам-повідомлень або для атаки інших ресурсів.

– Викрадення даних, які мають відношення до фінансових операцій: особиста документація, кредитні картки та інші платіжні системи.

– Несанкціонований показ рекламних повідомлень. Проте що може статись, коли метою атаки є не людина, а інформаційна система міста,

органу державної влади або іншої важливої установи?
Насправді, людина стає тією ланкою, яка призводить не тільки до репутаційних та особистих майнових втрат, але й каталізатором критичних, а іноді й катастрофічних ситуацій.
Наприклад, у травні 2021 року одна з найбільших страхових компаній США CNA Financial Corp. заплатила наприкінці березня $40 млн, аби відновити контроль над своєю мережею після атаки хакерів. Компанія заплатила хакерам приблизно через два тижні після того, як було вкрадено цілу низку даних компанії, а доступ до мережі топменеджерам CNA було заблоковано. CNA спочатку ігнорувала вимоги хакерів, намагаючись відновити файли без взаємодії зі злочинцями. Але вже за тиждень компанія вирішила розпочати переговори з хакерами, які вимагали $60 млн. Хакерська атака на лікарню міста Дюссельдорф призвела до смерті пацієнтки у вересні 2020 року. Жінку, якій знадобилася термінова госпіталізація, не прийняли в госпіталь через злам комп'ютерних систем і відправили в сусіднє місто Вуппераль, що знаходиться в 32 км. Через те, що час для порятунку було упущено, пацієнтка померла. Що було причиною? В обох випадках першоджерелом атаки була помилка або недбалість посадової особи: від випадкового відкриття листа з шкідливим вкладенням до неналежного нагляду за програмним забезпеченням.
Яким чином це все відбувається? Наприклад, програма, яка була завантажена Вами з недостовірних джерел мережі «Інтернет» або запущена зі знайденого USB-носія, виходить у Всесвітню Мережу та завантажує троянську програму. Не одну. Зазвичай подібні загрози поширюються на комп'ютері як грибниця – там, де одна, там і інша. Цим самим зловмисники страхують себе від того, що існуючий антивірус зможе видалити всі небезпечні програми. Тож з великою вірогідністю один запуск програми-оманки – і 1-2-3-4 загрози залишаться на комп'ютері, як би Ви його не перевіряли, і будуть виконувати свою роботу, паралельно завантажуючи нових «братів» та активуючі необхідні функції. І це не обов'язково починається із завантаження підозрілої програми. Все може починатися інакше і «елегантно». Ви переглядаєте сторінки в інтернеті і в одну мить переходите за посиланням на небезпечний сайт або відомий сайт чомусь перенаправив вас на інший. З вигляду він може нічим не відрізнятися від інших сайтів і нести цікаву чи корисну інформацію – ніхто вас не попередить ні про загрозу, ні про її наслідки. Із сайту, використовуючи вразливості Вашого браузеру чи його додатків, на ваш комп'ютер без Вашої згоди (або взагалі інформування) таємно завантажується крихітна програма, яка у свою чергу скачує та інсталює вищезазначені загрози.
Браузер, Web browser – спеціальна програма, призначена для перегляду вебсайтів. Основна мета інтернет-браузера – перевести код, за допомогою якого комп'ютери створюють веб-сайти, у текст, графіку та інші функції веб-сторінок, які ми звикли бачити сьогодні. Тобто, браузери транслюють код інтернет-сторінок у зрозумілий людині вигляд. Для передачі використовується протокол HTTP або його безпечніша версія HTTPS.
Протокол – це набір правил передачі файлів (тексту, зображень, відео тощо)

через мережу «Інтернет». Приклади браузерів: “Google Chrome”, “Mozilla Firefox”, “Microsoft Edge”, “Apple Safari”, “Internet Explorer”. Через браузери користувачі отримують доступ у цифровий простір, де можна переглядати контент з усього світу. Зараз браузери також зберігають облікові дані, файли cookie, історії пошуку та іншу цінну інформацію про користувачів, яка може опинитися під прицілом кіберзлочинців.

Cookie — це невеликі текстові файли, які зберігаються в комп’ютері під час відвідування певних веб-сторінок. Куки спрощують роботу в Інтернеті, зберігаючи потрібну інформацію. За допомогою файлів cookie сайти можуть запам'ятовувати ваш вхід в обліковий запис чи ваші уподобання, а також надавати вам персоналізований контент. Файли cookie також можуть використовуватися для збору статистики про перегляд сторінок та показу цільових оголошень. Cookies бувають тимчасовими і постійними. Постійні cookies залишаються на комп’ютері, коли ми закриваємо вкладку з сайтом, а тимчасові видаляються. Які саме cookies використовувати на конкретному сайті – тимчасові або постійні – вирішує його розробник. Саме тому на одних сайтах ми не виходимо з акаунтів, навіть коли заходимо на них раз через кілька днів, а на інших вводимо пароль заново, хоча відійшли від комп’ютера на п’ять хвилин. Самі по собі cookies не є небезпечними – це звичайні текстові файли. Вони не можуть запускати процеси на комп’ютері та взагалі взаємодіяти з операційною системою. Але їх можуть спробувати перехопити або вкрасти, щоб відстежити ваші попередні дії в мережі або входити у ваші акаунти без авторизації. Зазвичай інформацію, яку записують в cookies, зашифровують перед відправкою, а самі cookies передають за HTTPS-протоколом. Це допомагає захистити призначені для користувача дані, але за впровадження шифрування і безпечну відправку відповідає розробник сайту. Відвідувачам залишається тільки сподіватися, що все налаштували грамотно. Зі свого боку користувач може тільки заборонити браузеру використовувати cookies або час від часу чистити їх самостійно. Зовсім відключати cookies – не завжди хороша ідея. Наприклад, всі інтернетмагазини працюють за допомогою cookies. Якщо заборонити браузеру їх використовувати, сервер не зможе запам’ятати, що саме ви додали в кошик. Чистити cookies вручну практичніше, але доведеться щоразу заново налаштовувати зовнішній вигляд сайту і входити в акаунти.

Найпоширеніші загрози та ризики для безпеки браузера:

1. *Наявність вразливостей.* Через те, що користувачі часто нехтують застосуванням регулярних оновлень, браузер та встановлені плагіни чи розширення можуть містити уразливості. Їх зловмисники використовують для викрадення конфіденційних даних або завантаження шкідливого програмного забезпечення. Атаки часто починаються з фішингового електронного листа чи повідомлення або відвідування інфікованого сайту зі шкідливою програмою, а також завантаження небезпечного файлу.
2. *Використання програм.* Зловмисники націлені на програми на комп’ютері, а браузер при цьому використовується для доставки або виконання шкідливого компоненту. Серед найвідоміших форм — трояни, програми-вимагачі, віруси, черв’яки та банківські шкідливі програми. Об’єднує всі ці види шкідливих

програм — зловмисні наміри їх авторів чи операторів.

3. *Шкідливі плагіни*. **Плагін** – це програма, які полегшує користування мережею «Інтернет». Існують тисячі плагінів, які користувачі можуть завантажити, щоб покращити роботу в інтернеті. Однак багато з них мають привілейований доступ у браузері. Це означає, що зловмисники можуть замаскувати шкідливі плагіни під легітимні та використовувати їх для викрадення даних та завантаження небезпечного програмного забезпечення.

4. *Атаки «людина посередині».* Під час цього виду атаки зловмисник може змінити трафік, наприклад, переспрямувати жертву на фішингову сторінку, завантажити програми-вимагач або викрасти облікові дані. Такий ризик зростає під час використання публічних мереж Wi-Fi.

5. Інфікування системи доменних імен (DNS). DNS — це адресна книга інтернета, яка перетворює введені доменні імена на IP-адреси для відображення у браузері сайтів. Однак атаки на систему доменних імен, які зберігаються на комп'ютері, або на самі DNS-сервери можуть дозволити зловмисникам перенаправляти браузери користувачів на шкідливі домени, зокрема фішингові сайти.

6. *Перехоплення сеансу.* Більшість веб-сайтів використовують ідентифікатори сеансу під час входу користувачів. Якщо зловмисникам вдасться зламати чи перехопити ці ідентифікатори (у разі відсутності шифрування), кіберзлочинці можуть увійти на ті самі сайти чи у програми під виглядом користувача. У такому випадку можна швидко викрасти конфіденційні дані та фінансову інформацію.

Чому через браузер можуть реалізовуватись загрози?

– Браузери застарівають та з'являються вразливості, які експлуатуються хакерами віддалено.

– Хакери зламують легітимні сайти та розміщують на них шкідливий код та програми, і Ви можете навіть не знати про те, що стали жертвою.

– Зловмисники зламують публічні точки доступу до мережі «Інтернет» і намагаються перехопити інформацію користувачів.

Як покращити безпеку браузера?

Щоб запобігти потенційним загрозам для безпеки браузера та конфіденційних даних під час перегляду веб-сторінок, варто дотримуватись наступних порад.

1. Оновлюйте браузер та встановлені плагіни, щоб мінімізувати шанси використання вразливостей, а також видаліть усі застарілі плагіни.

2. Відвідуйте лише безпечні сайти з використанням протоколу HTTPS, про що свідчить замок в адресному рядку. У такому випадку хакери не зможуть перехопити трафік з браузера до веб-сервера.

3. Остерігайтесь фішингових загроз, які поширюються через електронну пошту та онлайн-повідомлення. Ніколи не відповідайте на небажані електронні листи, не перевіривши дані відправника, та не надсилайте конфіденційну інформацію незнайомцям.

4. Не завантажуйте підозрілі програми чи файли, а у випадку потреби використовуйте для цього виключно офіційні ресурси.

5. Використовуйте багатофакторну автентифікацію, щоб зменшити ризики викрадення облікових даних.
6. Застосовуйте VPN від надійного провайдера, а не безкоштовну версію.
Це створить зашифрований тунель для інтернет-трафіку та захистить від відстеження сторонніми особами. VPN або «віртуальна приватна мережа» – це сервіс, який захищає ваше інтернет-з'єднання і конфіденційність в інтернеті.

Підключення до VPN-мережі робить вашу IP-адресу майже невидимою. Зокрема VPN переносить ваше з'єднання на сервер у країні, яку ви оберете, і показує IP-адресу з того місця.
Таким чином, VPN працює як додатковий рівень захисту, шифруючи всі дані, які проходять через неї, та забезпечуючи конфіденційність в інтернеті.

Особиста інформація, дані місцезнаходження та історія веб-перегляду будуть недоступними для прочитання тим, хто спробує вас ідентифікувати та відстежити. Навіть ваш інтернет-провайдер не зможе збирати дані про вас. Під час використання загальнодоступного Wi-Fi ви підключаєтеся до менш безпечної мережі, створюючи ідеальну можливість для хакерів отримати доступ до ваших пристроїв. Використання VPN-мережі допоможе зашифрувати з'єднання та захистити вас від зловмисників, які хочуть викрасти особисту інформацію, паролі чи банківські реквізити.
7. Завантажуйте багаторівневе рішення для захисту комп'ютерів та мобільних пристроїв від різних онлайн-загроз.
8. Увімкніть автоматичні оновлення операційної системи та програмного забезпечення на пристрої.
9. Перегляньте налаштування конфіденційності та безпеки браузера, щоб запобігти відстеженню та заблокувати сторонні файли cookie і спливаючі вікна.
10. Вимкніть автоматичне збереження пароля в браузері.
11. Використовуйте параметри приватного перегляду, щоб запобігти відстеженню файлів cookie. Приватний перегляд - використання Firefox без збереження історії.
Безпечне користування месенджерами.
У перекладі з англійської «messenger» означає «гонець», «посланник», «посланець». Словом, «той, хто приносить новини».
Месенджер – це спеціальний додаток або програма, яку завантажують і встановлюють на смартфон або комп'ютер. Його основна мета - це миттєвий обмін текстовими повідомленнями, фото, картинками, відео, документами з друзями, родичами, знайомими, колегами по роботі або по навчанню. Також можна здійснювати дзвінки за допомогою аудіо або відеозв'язку.
Які ризики несе користування месенджерами?
1. Розкриття вашої приватної інформації: від номеру телефону до фотографій.
2. Шахрайство – шахраї дуже часто користуються саме месенджерами, щоб уникнути виявлення.
3. Розповсюдження шкідливого ПЗ через функції автозавантаження.
У 2017 році була виявлена тенденція – викрадення інформації через месенджери. У 2018 році кількість витоків інформації через месенджери зросла на 14,3%, хоча раніше цей канал зовсім не виділявся в статистиці. Крім того, постійно

виявляються нові модифікації шкідливих програм, що відстежують переписку в популярних месенджерах. У мирний час наше спілкування переважно відбувалася онлайн у різних месенджерах. А відколи розпочалася повномасштабна війна, і поготів – смартфони не випускаємо з рук. Але війна нині триває і у кіберпросторі – ворог намагається заволодіти нашою інформацією.

Якими месенджерами користуватися зараз найбезпечніше?

Раніше популярний здебільшого серед молоді, після 24 лютого Telegram перетворився у найоперативніший канал для повідомлення інформації. Новинні Telegram-канали набирають сотні тисяч підписників, свої канали для швидкого транслювання офіційної інформації створили Ще від початку роботи месенджера в Україні, довкола нього виникало багато підозр. Засновник Telegram – Павло Дуров, той, що придумав популярну в Росії мережу ВКонтакте. Скептики підозрювали, що Telegram зливає конфіденційну інформацію українських користувачів російській ФСБ. Відповідні пересторогиви никли знову, коли Росія розпочала повномасштабну війну в Україні. Сам Дуров написав, що має родичів в Україні, і те, що відбувається, його особиста трагедія. Він нагадав, як закінчилася його кар'єра у Росії, мовляв, 2013 року російська ФСБ вимагала керівництво ВКонтакте надати їм особисті дані українських користувачів ВК, які протестували проти президента-втікача. Дуров відмовився це зробити, і його звільнили з його ж компанії. Він більше не живе в Росії, не має там ані бізнесу, ані співробітників. І, мовляв, приватність усіх користувачів Telegram – священна. За останні роки Telegram зарекомендував себе як досить практичний і захищений месенджер, віднедавна орієнтований на групові аудіо- та відеодзвінки. Одна з головних переваг Telegram з погляду безпеки — можливість використовувати «секретні чати», які захищені наскрізним шифруванням. У секретних чатах також можна налаштувати період автоматичного видалення всіх повідомлень. За замовчуванням у Telegram встановлено двофакторну автентифікацію та власний алгоритм шифрування MTProto, який дозволяє об'єднати відразу кілька популярних протоколів безпеки (AES; RSA та протокол обміну ключами Діффі-Геллмана).

Кілька місяців тому засновник «сек'юрного» месенджера Signal Моксі Марлінспайк розкритикував Telegram і заявив, що цей сервіс нічим не відрізняється від месенджера Facebook. «Мене дивує, що після всього часу майже всі ЗМІ, як і раніше, називають Telegram „зашифрованим месенджером". Telegram має безліч привабливих функцій, але з погляду конфіденційності та збору даних найгіршого вибору немає», — написав Марлінспайк у Twitter.

Головною проблемою Telegram засновник Signal вважає те, що месенджер зберігає всі дані користувачів на своїх серверах, і в разі атаки хакера особиста інформація може потрапити до рук зловмисників. Засновник Telegram Павло Дуров відповів на цю заяву тим, що навіть «безпечні» месенджери на кшталт Signal спочатку фінансувала влада США, не кажучи вже про WhatsApp, який постійно передає дані користувачів третім сторонам. «Я чув, що наші американські конкуренти розчаровані тим, що вони не можуть зрівнятися зі зростанням Telegram, незважаючи на значні інвестиції у маркетинг (те, у що

Telegram ніколи не доводилося інвестувати). Але щоб відповідати нашому зростанню, вони повинні спочатку переконатися, що їхні дії відповідають їхнім маркетинговим заявам. До того часу витік даних і проблеми з безпекою в їхніх застосунках, на жаль, залишаться неминучими», — написав Дуров.

Facebook Messenger, Месенджер від Facebook – другий в Україні за популярністю серед користувачів. Утім, щодо його безпечності думки різняться. У деяких експертів виникають пересторогі, яким чином велика соціальна мережа може використовувати особисті дані користувачів. Особливо з огляду на те, що Facebook фігурував у схожих скандалах. Проте фахівець з кібербезпеки Костянтин Корсун цей месенджер називає непоганим. «Непогано захищений месенджер Facebook, питання лише до того, чи використовує компанія Facebook ваші дані у своїх рекламних цілях. Але це не росіяни. Це американці, у них діють закони, діють правила», – переконаний експерт. WhatsApp Месенджер, який також наразі належить компанії Facebook. На офіційному сайті розробники запевняють, що WhatsApp має наскрізне шифрування, відтак можна без жодних побоювань ділитися зі співрозмовниками особистою інформацією. Повідомлення зберігаються на пристроях користувачів, а не на серверах компанії. Утім, неодноразово WhatsApp потрапляв у різні скандали, пов'язані зі збереженням приватності. І навіть стеженні за користувачами. На початку 2021 року месенджер оновив правила конфіденційності, попередивши, що може обмінюватися даними з мережею Facebook, якій він належить. Багато користувачів таку політику розкритикували та перейшли в інші месенджери. У WhatsApp наскрізне шифрування працює за замовчуванням, можна включити двофакторну автентифікацію і налаштувати обмежений доступ до програми. Головні мінуси цього сервісу — відсутність секретних чатів, зберігання інформації на пристроях у відкритому вигляді та використання хмарних сховищ для даних резервного копіювання. В іншому ж до безпеки платформи виникає не більше запитань, ніж до її конкурентів.

Viber - найпопулярніший месенджер в Україні. Viber пропонує своїм користувачам наскрізне шифрування, секретні чати з функціями автоматичного видалення повідомлень, заборони або відстеження скріншотів, а також захисту від копіювання та пересилань повідомлень. На відміну від Telegram, у Viber повне шифрування за замовчуванням увімкнено для всіх чатів, але, як і Telegram, всі резервні копії чатів тут зберігаються у відкритому вигляді. Крім цього, кілька років тому повідомляли, що деякі сервери компанії розміщуються на території Росії і немає гарантії, що спецслужби цієї країни не мають доступу до переписки користувачів.

«Безпечні» месенджери. Окрему категорію сервісів швидких повідомлень становлять так звані «сек'юрні» месенджери, які акцентують увагу на безпеці своїх послуг і захищеності даних користувачів.

Один із найпопулярніших таких месенджерів Signal. Багато експертів називають криптографічний протокол Signal «еталоном для індустрії». Всі чати в цьому месенджері зашифровані за замовчуванням, і, як передбачається, навіть творці програми не можуть отримати доступ до ваших даних. Головною проблемою месенджера залишається відсутність популярних у Telegram, Viber і

WhatsApp функцій, а також низька популярність Signal серед користувачів, далеких від поняття «кібербезпека». Застосунок Signal для смартфона, а також його ПК-версію можна завантажити безкоштовно. І за нинішніх умов було б не зайвим це зробити.

Серед інших «сек'юрних» месенджерів варто виділити сервіси Threema, Briar, Zello, тощо. Подібні програми досить специфічні у використанні, підходять не для всіх пристроїв і деякі функції можуть бути платними. З огляду на те, що в нашій країні далеко не всі користувачі звикли платити за будь-яке програмне забезпечення саме Signal може стати оптимальним варіантом для тих, хто раптово вирішив подбати про безпеку свого цифрового спілкування. До речі, нещодавно у Мережі писали про злам месенджера Signal, але Державна служба спеціального зв'язку та захисту інформації України спростувала цю інформацію. Назвати однозначно «безпечний» месенджер — неможливо. Будь-який онлайн-сервіс може зазнати хакерських атак, унаслідок яких ваші дані можуть потрапити до рук зловмисників. Але загроза кібератак, що зросла, після вторгнення Росії в Україну — це найкращий час для виконання всіх правил інформаційної безпеки в месенджерах.

Як користуватися месенджерами безпечно?

Центр протидії дезінформації при РНБО України розробив коротку інструкцію для користувачів месенджерів.

1. Оновлюйте месенджери.
2. Не передавайте через месенджер жодну інформацію, розкриття якої для вас небажане.
3. Відключайте автоматичне завантаження файлів, особливо для контактів, що відсутні у вашій адресній книзі.
4. Не переходьте за посиланнями, особливо скороченими, які надійшли від недовірених контактів.
5. Використовуйте "зникаючі" повідомлення, або "одноразовий перегляд".
6. Активуйте двофакторну аутентифікацію, щоб додатково захистити свій обліковий запис.
7. Налаштуйте "конфіденційність", щоб контролювати, хто може бачити вашу фотографію і додавати до груп.
8. Перегляньте історію чату та членство в групах. За можливості очищайте історію чату.
9. Надсилайте скарги на будь-які контакти, які здаються вам шахрайськими, розсилають погрози або інші небезпечні повідомлення. Пам'ятайте про основне: Ваша особиста безпека – це Ваша відповідальність. Але від Вашої безпеки може залежати добробут та майбутнє співробітників, близьких та інших громадян України.

Безпечне користування електронною поштою.

Кожного дня ми використовуємо електронну пошту для робочих та особистих цілей. Вона стала одним з основних каналів комунікації з нами і тому є неабияк привабливою для кіберзлочинців та інших зацікавлених сторін. Після того, як люди почали активно користуватись емейлом, історія бачила чимало успішних кібератак, які використовували пошту як інструмент доставки шкідливого

програмного забезпечення та виманювання у людей конфіденційної інформації. Фішинг – атака, яка в основному використовує електронну пошту як вектор і обманом змушує людей завантажувати шкідливі програми собі на пристрої. Близько 60% підприємств зіткнулися з фішингом в 2021 році. У 2020 році було багато фішингових електронних листів, пов'язаних з COVID-19. Шахраї розсилали інформацію від імені Всесвітньої організації охорони здоров'я, граючи на страху осіб.

Чому електронна пошта настільки приваблива для кіберзлочинців?

- бази даних поштових скриньок легко знайти в мережі «Інтернет»;
- функція додатків до листів дозволяє злочинцям надсилати файли з шкідливим програмним кодом;
- користувачі не очікують отримати листи зі шкідливими вмістом/ користувачі часто несвідомо відкривають всі листи, які до них надходять;
- злочинці користуються людською психологією, щоб збільшити шанси відкриття шкідливих файлів.

Одним з перших правил безпеки електронної скриньки є чітке розмежування особистої та службової пошти.

Службова пошта показує вашу належність до організації – (vasyl@me.gov.ua). Ми бачимо, що Василь належить до Міністерства розвитку економіки. Тим самим викликає довіру та авторитет до листів, які надходять з цієї адреси;

- дані зберігаються на серверах вашої установи і адмініструються відділом інформаційних технологій. Треті сторони не повинні мати доступ до цих даних.

Особиста пошта:

- зберігається на серверах компанії, яка надає послуги поштового сервісу;
- містить вашу приватну інформацію;
- використовується для реєстрації у соціальних мережах та на інших ресурсах.

Які загрози існують під час користування поштовою скринькою?

- Фішинг з метою − виманити ваші конфіденційні дані;
- зараження системи/мережі організації з метою паралізації всієї системи (шифрування вашого комп’ютера);
- отримання віддаленого доступу до комп’ютера та, як наслідок, мережі.

Як відрізняти легітимні листи від фішингових (investigation)?

Вам надійшов лист. Ви очікували на нього? Ні?

Проведімо аналіз метаданих:

1. Спершу, ми подивимось, хто відправник. Ви знаєте його? Вважайте, ім’я відправника можна поставити будь-яке.

2. Яка тематика повідомлення? Якщо вона викликає якусь квапливість або кличедо швидкої дії, це має бути індикатором, що до листа треба поставитись серйозно та обережно.

Приклад: «Вас зламали! Швидше поміняйте пароль».

2. Коли ви відкрили лист, зверніть увагу на правильність написання домену відправника. Кіберзлочинці часто підмінюють літери/символи, щоб замаскуватись під авторитетне джерело.

В період президентських виборів у США 2016 року для проведення фішинг-атаки на базі схожих доменів зловмисники використали сайт «accountsgoogle.com» як клону сайту «accounts.google.com». Коли ми переконались, що лист надійшов саме з достовірної адреси, ми можемо проаналізувати зміст повідомлення.

Аналіз змісту повідомлення.

1. Перше на що варто звернути увагу: чи звертаються до вас на ім'я? Чи використовують загальні фрази «Шановні колеги», «Шановний клієнте» і тд. Злочинець може вказати ваше ім'я, тоді атаку можна вважати підготовленною спеціально під вас.
2. Наступний індикатор фішингового листа – мова та наявність граматичних/орфографічних помилок. Наприклад, "Google" надсилає листи, які стосуються облікового запису, мовою інтерфейсу цього запису. Тобто, якщо у вас інтерфейс українською мовою, а лист прийшов російською, це серйозна причина задуматися.
3. Якщо ви отримуєте файл у додатку та пароль для відкриття його, це є великою підозрою на наявність у ньому шкідливого коду. Чому? Справа в тому, що у поштових сервісів є свої антивіруси, які сканують файли на наявність вірусів. Злочинці про це також знають, тому використовують функціонал архіваторів (WinRar, ZIP, та інші), щоб зашифрувати вміст файлу паролем. Таким чином, коли ви отримуєте файл на пошту, поштовий антивірус не може розпізнати шкідливість файлу, оскільки він зашифрований.
4. Далі, подивімось чи є якісь активні посилання у листі? Спробуйте навести мишкою на посилання (не натискаючи) та потримайте декілька секунд. У лівому нижньому куті, подивіться, куди насправді воно вас веде.

Важливо!!! Посилання такого вигляду accounts.google.com.evilwebsite.pe/EditPasswd шахрайське, бо адреса має починатися з accounts.google.com/ (тобто, після.com мусить бути /, а не крапка).

Як убезпечити свою поштову скриньку?

1. Використовувати складний пароль. Складний пароль – той, який містить в собі літери, символи та цифри і за довжиною не менше 8 символів. Пароль не повинен містити слів, які можна знайти у словнику.

Приклад поганого паролю: rockandroll123

Приклад надійного паролю: T@8l3S0bk4hA7

2. Не передавайте нікому свої паролі
3. Встановити подвійний фактор аутентифікації
4. Ніколи не відкривати файли, не переконавшись у їхньому походженні.
5. Не використовувати службову пошту в особистих цілях.
6. Маєте сумніви щодо походження файлу, використовуйте https://virustotal.com для сканування файлу 50-ма антивірусними програмами.
7. Якщо у листі є скорочені посилання (https://bit.ly/xxxxx переівряйте їх за допомогою таких сервісів: – http://checkshorturl.com/ – http://www.expandurl.net/.

Якщо так сталося, що Ви перейшли за посиланням у фішинговому листі, тоді:

1. Треба якомога швидше змінити пароль;
2. Продивитися відкриті сесії та закрити ті, які тобі не належать;
3. Повідом про це ІТ-відділ.

Якщо відкрив файл у додатку і зрозумів/ла, що це був фішинг, тоді:

1. Вимкнути комп’ютер;
2. Звернитися до відділу ІТ-технологій.

Розділ 3. Кібербезпека педагогічних працівників

3.1. Захист персональних даних педагогічних працівників

Чому розбиратися в основах інформаційної безпеки потрібно кожному, як навчати здобувачів освіти кіберграмотності та що робити, якщо учень хоче рятувати світ від комп'ютерних загроз?

У липні 2020 року хакери зламали безліч акаунтів у Twitter, включаючи верифіковані. Повідомлення про безкоштовну роздачу біткоїнів було опубліковано, зокрема, на сторінках Ілона Маска, Білла Гейтса, Барака Обами та деяких інших відомих людей. За допомогою цих публікацій зловмисники закликали користувачів переказувати свої кошти на певний гаманець та обіцяли подвоювати усі вхідні платежі. В результаті люди перевели щонайменше $120 тис. на вказаний у постах рахунок. Після інциденту представники Twitter підтвердили, що кібератака пішла за компрометацією одразу кількох співробітників компанії. Примітно, що шахраї організували атаку фішингу, застосувавши таким чином соціальну інженерію проти співробітників Twitter.

Те, що зловмисникам вдалося реалізувати таку масштабну кібератаку, ще раз доводить: методи соціальної інженерії залишаються одними з найдієвіших. Саме тому в сучасному світі володіння базовими правилами інформаційної безпеки так само потрібне, як, наприклад, знання основ здорового способу життя або пожежної безпеки. Причому формувати навички так званої кібергігієни у людей потрібно з ранніх років. Батькам слід розповідати своїм дітям про правила безпечної поведінки в інтернеті, як тільки юні користувачі отримують доступ до комп'ютера чи смартфона, подібно до того, як дитина дізнається про правила безпечного переміщення містом, коли вона починає самостійно ходити до закладу освіти.

Сучасні заклади освіти широко використовують цифрові технології у своїй діяльності для ведення журналів, контролю навчальних досягнень, адміністративної діяльності тощо.

До проблем інформаційної безпеки відносять такі фактори:

- використання застарілих і свідомо небезпечних платформ;
- встановлення піратського програмного забезпечення;
- низька кваліфікація обслуговуючого персоналу, в ряді випадків відсутність посади фахівця з підтримки інформаційних систем; відсутність практики регулярного аудиту безпеки.

Для освітнього середовища проблема інформаційної безпеки пов’язана із захистом персональних даних абітурієнтів, здобувачів освіти, співробітників, включаючи їх особисту, фінансову, навчально-професійну та іншу інформацію. Таким чином, забезпечення інформаційної безпеки пов’язане з роботою всіх структурних підрозділів освітньої організації, починаючи з роботи приймальної комісії, навчальної частини і закінчуючи кадровою службою.

Сучасна людина є своєрідним заручником високих технологій. Важко відволікти увагу дитини від смартфону чи монітора комп’ютера? Діти повсякчас щось

шукають в мережі чи завантажують з неї, спілкуються у чатах. Це може свідчити про інтернет залежність. Як цьому запобігти?

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

Будучи невичерпним джерелом інформації, інтернет приваблює дітей можливістю дізнатися і побачити все що завгодно. Цікава до всього дитина прагне отримати якомога більше: спілкування, ігор, мультфільмів, розваг – і тому багато часу проводить у віртуальному просторі, часто на противагу реальному життю. Соціалізацію і спілкування з однолітками замінює фактично однобоким онлайн спілкуванням. Активним іграм на свіжому повітрі все більше дітей протиставлять мережеві ігри, далеко не завжди нешкідливі. Іноді пошук нової інформації стає буквально нав'язливою ідеєю.

Як виявити залежність?

Якщо у дитини спостерігаються деякі з перелічених нижче ознак, варто бити тривогу:

- збільшення інтервалу часу, проведеного з комп'ютером;
- зниження успішності;
- втрата інтересу до того, що відбувається навколо;
- втрата інтересу до позааудиторних занять;
- порушення сну;
- часті та різкі перепади настрою;
- неадекватна поведінка у відповідь на пропозицію вимкнути комп'ютер – аж до прояву агресії та сварки.

Інтернет може бути чудовим та корисним засобом для навчання, відпочинку чи спілкування з друзями. Але – як і реальний світ – Мережа також може бути небезпечною: у ній з'явилися своя злочинність, хуліганство та інші малоприємні речі. Віртуальність спілкування надає людям з недобрими намірами додаткові можливості заподіяти шкоду дітям. В останній час в інтернеті з'являється багато матеріалів агресивного та соціально небезпечного змісту. Дорослим слід пам'ятати про існування подібних загроз і приділяти особливу увагу питанню забезпечення безпеки здобувачів освіти в інтернеті.

З кожним днем інформаційні технології все більше проникають в життя сучасної людини. Сьогодні майже кожен має смартфон з доступом до інтернет-мережі, що дозволяє користувачам завжди бути онлайн. Зокрема у будь-яку мить ви можете перевірити пошту чи месенджер, купити квиток в кіно чи забронювати житло для відпустки та навіть здійснювати платежі, не звертаючись до відділень банку. Всі ці дії в інтернеті передбачають обмін певною особистою інформацією чи конфіденційними даними, які у разі вашої неуважності можуть опинитися в руках зловмисників. Для забезпечення захисту ваших персональних даних під час роботи в інтернет-мережі спеціалісти рекомендують дотримуватися основних правил кібергігієни. В свою чергу кібергігієна — це заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації.

Правила кібергігієни: 7 кроків для покращення захисту даних.

1. Перевірка безпеки активних акаунтів. Першим правилом кібергігієни є перевірка безпеки вже існуючих облікових записів електронної пошти та акаунтів в соцмережах. Зокрема такі веб-сайти як haveibeenpwned.com та breachalarm.com допоможуть з'ясувати, чи був пароль до електронної пошти викрадений зловмисниками.

2. Аналіз програм. Сьогодні у кожного сайту, магазину та навіть банку є спеціальний мобільний додаток. Проте це не означає, що всі вони мають бути на вашому пристрої. Завантажуйте тільки необхідні для роботи програми. Спеціалісти радять проаналізувати вже завантажені додатки, видалити непотрібні та в подальшому контролювати встановлення кожної програми. Також під час завантаження кожного додатку варто звертати увагу на дозволи, які ви надаєте. Часто шкідливі програми надсилають запит на отримання великої кількості дозволів, які не відповідають їх функціоналу. Це дозволяє збирати багато інформації про користувача з метою отримання прибутку.

3. Регулярне оновлення. Для запобігання інфікуванню шкідливими програмами варто здійснювати своєчасне оновлення операційної системи та окремих додатків, яке передбачає виправлення уразливостей та помилок в програмному забезпеченні.

4. Надійний пароль. З метою запобігання несанкціонованому доступу до пристроїв переконайтеся у надійності ваших паролів. Важливо створити складну комбінацію, яка містить не менше 12 символів, великі та малі літери, цифри та символи. Крім цього, для кожного акаунта варто використовувати унікальний пароль. Таким чином викрадення однієї з комбінацій не поставить під загрозу інші облікові записи.

5. Додатковий рівень захисту. Для покращення безпеки облікових записів використовуйте двофакторну аутентифікацію, яка передбачає підтвердження особистості під час входу в певний акаунт. Найчастіше для цього використовуються SMS-повідомлення або окрема програма. Таким чином у разі викрадення пароля зловмисники не зможуть отримати доступ до ваших даних.

6. Регулярне резервне копіювання. Необхідним кроком для уникнення втрати важливих даних є регулярне резервне копіювання інформації на зовнішній жорсткий диск або у хмару. Це допоможе відновити потрібні дані у разі їх шифрування програмою-вимагачем або видалення шкідливим програмним забезпеченням.

7. Надійний захист. Останнім, але не менш важливим, правилом кібергігієни є використання надійного рішення для захисту вашого комп'ютера чи смартфона від різних загроз, зокрема програм-вимагачів, шпигунських програм, вірусів, троянів та фішинг-атак.

Ці сім основних правил кібергігієни допоможуть вам своєчасно виявити підозрілу діяльність зловмисників та запобігти втраті персональних даних та іншої особистої інформації. Запровадження дистанційного навчання на початку пандемії спонукало педагогічних працівників швидко шукати способи, інструменти та електронні канали комунікації для його проведення і взаємодії з учнями та батьками.

Цифровізація освітнього процесу й робота з технологіями дистанційного навчання вже помітно вплинула на те, як відбувається освітній процес. З одного боку значно розширилися і продовжують розширюватися можливості педагогів проводити навчання, а учнів – навчатися. З іншого – використання цих методів, технологій та інструментів тісно пов’язане з безпекою роботи, зокрема, використанням та обробкою персональних даних учасників освітнього процесу.

Існує певна проблема, пов'язана з засвоєнням основ інформаційної безпеки. Ніщо так не вчить фінансової грамотності, як втрата грошей, і ніщо так не вчить кіберграмотності, як витік персональних даних, зламування акаунту і знову ж таки втрата грошей. Або набагато більшого. Виникає закономірне питання про те, чи може людина, у тому числі дитина, навчитися дотримуватись правил особистої кібергігієни, уникнувши такого «суворого» досвіду. Може. Для цього необхідно подолати деякі негативні установки.

Поява Інтернет-технологій зумовила стрімкий розвиток дистанційного навчання, яке ґрунтується на принципі самостійного навчання слухача. Суть роботи вчителя в цих умовах полягає не в читанні лекцій, а в створенні навчально-методичного забезпечення дисципліни в електронному вигляді, у постійній роботі над внесенням необхідних змін у навчальний матеріал, підборі кольорових ілюстрацій, графіків, створенні Flash-анімацій, тестів для самоконтролю.

Для розробки, управління та поширення навчальних онлайн-матеріалів із забезпеченням спільного доступу використовуються різноманітні системи управління навчанням (LMS – Learning Management System). Найпоширенішими з них є системи Microsoft Teams, Moodle, Blackboard Learning System.

Якщо ж упроваджувати у навчальний процес елементи дистанційного навчання, то це можливо здійснити засобами існуючих в Інтернеті інструментів та веб-ресурсів, наприклад:

- електронні лекції, які містять текст, демонстраційний матеріал, додаткові відомості можуть зберігатися у хмарних сховищах (Google Диск);
- індивідуальні або групові консультації доцільно проводити за допомогою Skype, e-mail, Google Hangouts;
- дискусії, обговорення, робота в малих групах організовуються за допомогою форумів, чатів, веб-конференцій;
- для організації дослідницької діяльності вчителів використовуються вебквести;
- технологія, що дає можливість повною мірою відтворити умови спільної форми організації навчання, а саме семінарських і лабораторних занять, лекцій тощо – вебінар на платформах SeeMedia, Meeting Butner, Pruffme;
- контроль знань у вигляді тестування можливо здійснити засобами Google Форми, або інших онлайн-конструкторів тестів.

Як уже відзначалося, крім інструментів, методів та джерел відомостей і даних, web-технології надають нові можливості для:

- забезпечення вільного доступу до навчальних матеріалів завдяки соціальним сервісам і технологіям у хмарі;

- забезпечення комунікації між учасниками процесу навчання, що дозволяє здійснювати обмін професійним досвідом, методичними ресурсами та ін. і сприяти персоналізації навчального процесу;
- сприяння створенню інноваційних засобів навчання;
- сприяння вдосконаленню особистих досягнень вчителів і учнів завдяки участі в певних навчальних проектах;
- сприяння підвищенню мотивації до навчання учнів й удосконаленню професійної діяльності вчителів;
- сприяння розвитку ключових компетентностей, зокрема когнітивних навичок, самонавчанню, реалізації особистісного потенціалу суб'єктів освітнього процесу

Огляд найпоширеніших web-сервісів для створення дидактичних матеріалів
Дидактичний матеріал – засіб навчання, матеріальний або ідеальний об’єкт, який «розміщено» між суб'єктами освітнього процесу, і використовується для засвоєння знань, формування досвіду пізнавальної та практичної діяльності, та суттєво впливає на якість знань, їх розумовий розвиток; це особливий тип наочного навчального посібника, переважно: карти, таблиці, набори карток з текстом, цифрами або малюнками, рослини, інструкції щодо виконання деяких навчальних завдань, шаблони сценаріїв презентацій, публікацій, веб-сайтів, якими можно користуватись учням з метою засвоєння навчального матеріалу. Вчителі створюють їх з метою управління навчальним процесом: організації дослідження, вивчення нового матеріалу, повторення, узагальнення, формування практичних навичок, перевірки набутих знань тощо. Вони допомагають збуджувати та підтримувати пізнавальні інтереси учнів, покращувати надійність навчального матеріалу, зробити його більш доступним, забезпечувати більш точну інформацію про явище, що вивчається, інтенсифікувати самостійну роботу слухача та її темп.

До дидактичного матеріалу можна віднести:

- дидактичні тексти (пам’ятки) для роботи з різними джерелами інформації (підручником, картами, довідниками, словниками, електронними ресурсами тощо);
- узагальнені плани деяких видів пізнавальної діяльності: вивчення наукових фактів, підготовки і проведення експерименту, проведення дослідження, вимірювання, аналізу графіка функціональної залежності, аналізу таблиць тощо;
- пам’ятки (інструкції) щодо формування логічних операцій мислення: порівняння, узагальнення, класифікації, аналізу, синтезу;
- завдання різного рівня складності: репродуктивного, перетворюючого, творчого;
- інструктивні картки, що відображають логічну схему вивчення нового матеріалу і необхідні способи навчальної діяльності;
- картки-консультації, матеріали з пояснюючими малюнками, планом виконання завдань, з вказівкою типу завдань та ін.;
- інструкції до лабораторних робіт і дослідів;
- довідкові матеріали;

- тести з можливістю контролю й самоконтролю тощо.

В умовах сучасного розвитку інформаційного суспільства та комп'ютеризації освітнього процесу виник інший вид дидактичного матеріалу – електронний. Під електронним дидактичним матеріалом розуміють цілеспрямовано розроблені документи для використання у навчальному процесі за допомогою прикладних програм загального призначення (або навчальних програмних середовищ) і побудовані відповідно до змісту навчальної теми і методики навчання предмету. Використання електронних дидактичних матеріалів дозволить педагогу:

- індивідуалізувати, диференціювати та інтенсифікувати процес навчання (оптимальність поєднання індивідуальної, групової, колективної роботи на уроці);
- посилити мотивацію навчання за рахунок використання різних видів діяльності і джерел інформації;
- формувати в учнів уміння орієнтуватися в проблемі і шукати шляхи її вирішення;
- змінити характер пізнавальної діяльності учнів (підтримка особистих намагань учнів сформувати власний стиль навчальної роботи);
- діагностувати помилки і оцінки результатів;
- здійснювати контроль із зворотним зв'язком за наслідками діяльності учня; візуалізувати навчальну інформацію;
- моделювати та імітувати об'єкти, що вивчаються або досліджуються, (комп'ютер може не тільки створити модель, а й дозволяє змінити умови демонстрування, відтворивши інформацію з оптимальним темпом її сприймання учнем);
- забезпечити доступ до інформації (доступ до Інтернету, електронних довідників і т.д.);
- формувати інформаційну компетенцію педагога та учнів.

Електронний дидактичний матеріал створюють за допомогою web-сервісів, які працюють за певним принципом:

- реєстрація користувача;
- вибір виду або шаблону завдання;
- заповнення готового шаблону;
- публікація в мережі.

Приймаючи рішення про використання засобів ІКТ, педагог має бути готовий використовувати хмарні технології в навчальному процесі, працюючи в хмарних сховищах, а також до розробки власного контенту та дидактичних продуктів, підготувати учнів до навчання з використанням ІКТ та активно залучати їх до створення цих матеріалів.

Сервіси Google та Web 2.0 відкривають перед педагогами безліч можливостей:

 використання відкритих, безкоштовних і вільних електронних ресурсів (навчальних комп'ютерних програм, електронних підручників, ігор, зображень і звукових файлів), які можуть бути використані з навчальною метою; самостійне створення власного мережного контенту (текстів, малюнків, фотографій, аудіо- та відео-фрагментів);

 можливість активно долучати учнів до колективної співпраці в режимі онлайн;

 участь у нових формах навчально-пізнавальної діяльності;
 участь у професійних наукових спільнотах.

Для навчального процесу web-технології дають можливість створення суб'єктних відносин між педагогами і учнями в мережі «Інтернет», а також обміну досвідом між педагогами, зворотний зв'язок із учнями тощо. Використання сучасних web-технологій та розроблених на їх основі web-ресурсів є важливою передумовою успішності навчальної діяльності.

Постійне оновлення інформаційних технологій є ресурсом інноваційного руху як освітнього середовища, так і особистості у ньому, адже розвиток технологій є необмеженим, вони постійно вдосконалюються й забезпечують ефективне функціонування інформаційних систем для управління закладом освіти, моніторингу якості, підготовки здобувачів освіти на основі інформаційних засобів, у тому числі й дистанційних.

Серед розмаїття нових інформаційних технологій сьогодні увага науковців та практиків зосереджена на упровадженні в освітній процес технологій дистанційного навчання, організація якого здійснюється на основі сучасних інформаційних систем, що функціонують за наявності відповідно створених організаційно-педагогічних умов в освітньому середовищі закладу.

Обґрунтовуючи модель дистанційного професійного навчання, можно виділити наступні блоки організаційно-педагогічних умов, а саме:

- організаційно-технічний (наявність нормативно-правового супроводу дистанційної освіти;
- наявність спеціалізованої системи дистанційного навчання), змістово-процесуальний (розробка та розміщення в електронному середовищі сучасних педагогічних програмних комплексів (дистанційних курсів);
- застосування змішаного навчання у професійній підготовці кваліфікованих робітників), особистісно-професійний (рівень володіння учнями (слухачами) інформаційними технологіями;
- безперервний розвиток готовності педагогів до впровадження технологій дистанційного навчання.

Означені умови дистанційного навчання співвідносяться із вимогами до створення інформаційної системи в освітньому середовищі, оскільки інтегрують організаційні, технічні, методичні, особистісні складові цього процесу, забезпечують педагогічну взаємодію в електронному середовищі для повноцінної реалізації індивідуальних освітніх траєкторій суб'єктів навчання на основі педагогічних та інформаційних технології.

Педагогічна практика засвідчує, що дистанційне навчання у закладах освіти сьогодні впроваджується у поєднанні із традиційним навчанням, з використанням в освітньому процесі елементів дистанційного навчання й розглядається у науці як «змішане навчання» (blended learning). Застосування змішаного навчання, наприклад, у закладах професійної освіти, передбачає вивчення предметів теоретичної підготовки засобами дистанційного навчання, професійно-практична підготовка та державна кваліфікаційна атестація проводиться традиційно, в умовах навчального закладу, безпосередньо на робочих місцях на підприємстві чи у сфері послуг. Здобувши засобами

дистанційного навчання теоретичні знання, вчителі набувають базу та підґрунтя для переходу до інтенсивного практичного навчання.
Розвиток технологій дистанційного навчання є перспективним напрямом інформатизації освіти (формальної, неформальної, інформальної), що ґрунтується принципах відкритої освіти, може відбуватися в різних організаційних формах (онлайн-курси, вебінари, онлайн-тренінги, веб-конференції) із використанням інтерактивних електронних підручників, контент-бібліотек, смарт-комплексів, віртуальних лабораторій, соціальних мереж, мультимедійних засобів навчання, платформ тощо.
Отже, системне використання інформаційних технологій у формуванні освітнього середовища закладу освіти забезпечує функціонування інформаційно-освітнього простору, максимально наближеного до сучасних тенденцій розвитку інформаційного суспільства; сприяє розвитку мобільності користувачів при здійсненні електронних комунікацій; уможливлює доступ до інструментальних середовищ проектування і моделювання; передбачає поєднання традиційних технологій із дистанційними засобами навчання, застосування хмарних сервісів (Google, Microsoft), інформаційних баз і систем, електронних бібліотек в освітньому процесі тощо, сприяючи при цьому формуванню й удосконаленню мережних якостей особистості.
організація мережевої взаємодії між інститутом післядипломної педагогічної освіти, районною методичною службою та навчальним закладом сприяє реалізації основних принципів компетентнісно спрямованої та практико орієнтованої освіти. Такий підхід забезпечує вибір учасниками освітнього процесу індивідуальної освітньої траєкторії, сприяє формуванню індивідуального комплексу знань, диференційованих відповідно до професійних функцій, освітніх потреб і запитів, високого рівня знань, умінь і навичок щодо розробки інтернет-ресурсів і використання засобів інтернет-технологій загального призначення, моделюванню інформаційних процесів, проектуванню функціонально орієнтованих компонентів освітньої діяльності з метою ухвалення оптимального професійного рішення тощо.

3.2. Методи кібергігієни для організації безпечного навчання

Впровадження та застосування цифрових технологій є важливим серед численних інноваційних напрямків розвитку навчання і освіти в цілому. Розробляється безліч інформаційних сервісів, які вчитель може впроваджувати і ефективно використовувати в навчальному процесі та для свого професійного розвитку. Багато шкіл користуються такими цифровими ресурсами, але не займаються питаннями захисту даних. Але захист інформації є дуже важливим, оскільки часто використовуються особисті дані учнів та вчителів, навчальні матеріали та результати навчання. Тому важливими для освітян є питання безпеки в інтернеті, що є особливим компонентом ширших ідей кібербезпеки та комп’ютерної безпеки, що включає в себе такі складові як: безпека браузера, поведінка в інтернеті, безпека мережі. Оскільки на сьогодні існує багато ризиків, серед яких COVID-19 та військові дії, що спричинило запровадження

дистанційної форми навчання, тобто значну частину свого часу освітяни проводить в інтернеті, і важливо розуміти, які загрози існують.

Серед загроз можна виділити такі:

- **злом**, це коли сторонні неавторизовані користувачі отримують доступ до комп'ютерних систем, облікових записів електронної пошти або веб-сайтів; віруси або зловмисне програмне забезпечення, що може нанести шкоду вашим даним або зробити системи вразливими до інших загроз;
- **крадіжка особистих даних**, коли злочинці викрадають особисті дані та фінансову інформацію.

Існують різні види **інтернет-атак**, серед яких можна виділити такі:

- **фішинг** – це кібератака, яка включає замасковані електронні листи, задача – обдурити людей, щоб вони передали свою особисту інформацію або завантажили шкідливе програмне забезпечення.
- **злом і віддалений доступ**, який хакери намагаються використати для викрадання конфіденційної інформації та даних користувачів, оскільки програмне забезпечення для віддаленого доступу дозволяє користувачам отримувати доступ до комп'ютера та керувати ним віддалено (актуально при пандемії та воєнному стані, коли багато людей працюють віддалено). Протокол, який дозволяє користувачам дистанційно керувати комп'ютером, підключеним до інтернету, називається протоколом віддаленого робочого столу або RDP. Хакери використовують різні методи для використання вразливостей RDP, поки не отримають повний доступ до мережі та її пристроїв. Вони можуть здійснювати крадіжку даних самостійно або продавати облікові дані в темній мережі;
- **шкідливе програмне забезпечення** — це набір «зловмисного» та «програмного забезпечення» (віруси, хробаки, трояни тощо), які хакери використовують для руйнування та крадіжки конфіденційної інформації. Будь-яке програмне забезпечення, призначене для пошкодження комп'ютера, сервера чи мережі, можна назвати шкідливим.
- **зловмисна реклама** — це онлайн-реклама, яка розповсюджує шкідливе програмне забезпечення, оскільки інтернет-реклама — це складна екосистема (включає веб-сайти видавців, біржі реклами, рекламні сервери, мережі ретаргетингу), яку зловмисники використовують для розміщення шкідливого коду у місцях, які видавці та рекламні мережі не завжди виявляють, а користувачі Інтернету, які взаємодіють із шкідливою рекламою, можуть завантажити шкідливе програмне забезпечення на свій пристрій або перенаправляються на шкідливі веб-сайти;
- **програми-вимагачі** – це зловмисне програмне забезпечення, яке не дозволяє вам використовувати свій комп'ютер або отримувати доступ до певних файлів на вашому комп'ютері, якщо не сплачено викуп (поширюється як троян).
- **ботнет** – це мережа комп'ютерів, які навмисно заражаються шкідливим програмним забезпеченням для виконання автоматизованих завдань в Інтернеті без дозволу чи відома власників комп'ютерів та може використовувати його для здійснення шкідливих дій (створення підробленого інтернет-трафіку на сторонніх веб-сайтах для фінансової вигоди, використання потужності вашого

комп’ютера для допомоги в атаках розподіленої відмови в обслуговуванні (DDoS) для закриття веб-сайтів, розсилка спаму мільйонам користувачів Інтернету, здійснення шахрайства та крадіжки особистих даних, атаки на комп’ютери та сервери).

- **загрози Wi-Fi** у громадських місцях та вдома, оскільки безпека в цих мережах – у кав’ярнях, торгових центрах, аеропортах, готелях, ресторанах тощо – часто слабка або відсутня, тобто кіберзлочинці та викрадачі особистих даних можуть стежити за тим, що ви робите в інтернеті, і викрадати паролі та особисту інформацію користувачів.

При дистанційному навчанні всі вище перелічені загрози можуть виникнути, тому персонал навчального закладу має вміти захистити свої дані та інформацію про всіх учасників освітнього процесу в інтернеті.

Розглянемо деякі шляхи забезпечення кібергігієни в інтернеті:

- багатофакторна автентифікація (MFA) – це метод автентифікації, який просить користувачів надати два або більше методів перевірки для доступу до облікового запису в інтернеті (наприклад: додатковий одноразовий пароль, який сервери аутентифікації веб-сайту надсилають на телефон або адресу електронної пошти користувача; відповіді на питання особистої безпеки; відбиток пальця або інша біометрична інформація, як-от розпізнавання голосу чи обличчя тощо). Багатофакторна аутентифікація знижує ймовірність успішної кібератаки. Також можна використати програми аутентифікації, наприклад Google Authenticator і Authy;
- використання брандмауеру, програми чи пристрою, що здійснює захист комп'ютерних мереж, вони блокують небажаний трафік, а також можуть допомогти заблокувати шкідливе програмне забезпечення від зараження комп’ютера (часто ваша операційна система та система безпеки мають попередньо встановлений брандмауер, але бажано переконатися, що ці функції ввімкнено, а ваші налаштування налаштовані на автоматичний запуск оновлень, щоб максимально підвищити безпеку в Інтернеті);
- уважно вибраний браузер, який буде безпечним та захистить від злому даних;
- створення надійного паролю або використання безпечного менеджера паролів (надійний пароль має бути: довгим, щонайменше з 12 символів; поєднувати символи, тобто великі і малі літери, символи і цифри; уникати простого використання порядкових номерів («1234») або особистої інформації, такої як дата вашого народження чи ім’я домашньої тварини; зберігати свої паролі конфіденційними та не повідомляйте їх іншим і не записувати їх; не використовувати один і той самий пароль для всіх своїх облікових записів і регулярно змінювати їх);
- застосовувати антивірусну програму та постійно оновлювати її, вона має вирішальне значення для забезпечення конфіденційності та безпеки в інтернеті, оскільки захищає від різних типів інтернет-атак і захищає дані в інтернеті.

Необхідно зазначити також, що безпека в інтернеті для дітей має вирішальне значення, оскільки вони мають бути захищені від шкідливого чи невідповідного

вмісту та контактів, а також від шкідливого програмного забезпечення чи атак, а навчання дітей кібергігієні може допомогти захистити їх.

Щодо забезпечення кібергігієни для навчання необхідно:

- мати чіткі вказівки, коли існує безліч інструментів електронного навчання, які можуть зацікавити вчителів необхідно переконатися, що будь-який навчальний ресурс, який використовується є безпечним;
- необхідно навчати учнів, вчителів та інших працівників школи безпечному поводженню в інтернеті;
- необхідно постійно оновлювати паролі та використовувати методи багатофакторної аутентифікації, щоб зменшити ризики викрадення паролів.
- визначити потенційні загрози, оскільки дистанційне навчання створює унікальні проблеми безпеки для навчання, а саме вчителі та учні використовують свої персональні пристрої вдома та існує ймовірність того, що користувачі працюють у незахищеній мережі або забувають оновлювати свої пристрої та програмне забезпечення.

Слід зазначити, що кібергігієна має бути включена в плани дистанційного навчання. Це є запорукою безпеки та дотримання конфіденційності, які сприятимуть навчанню.

На сьогодні існують онлайн ресурси в Україні, які навчають кібергігієні. Одним з таких ресурсів є освітній серіал «Основи кібергігієни», який розміщено на Національній онлайн-платформі для розвитку цифрової грамотності «Дія. Цифрова Освіта» [1]. Серіал було створено в рамках проекту «Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки», що реалізується Координатором проектів ОБСЄ в Україні за підтримки Міністерства закордонних справ і міжнародного розвитку Великобританії та Федерального міністерства закордонних справ Німеччини та знайомить вчителів із базовими принципами кібергігієни та типовими алгоритмами дій у разі виявлення ознак інформаційних атак на реальних прикладах.

Організація методичного супроводу професійного вдосконалення вчительа, його індивідуальних особливостей та професійних потреб, розробку індивідуальних програм професійного саморозвитку, допомогу у процесі реалізації програми самовдосконалення, що реалізується через дистанційне навчання актуалізована на позитивність взаємодопомоги в процесі професійного самовдосконалення, до якого можуть бути залучені як фасилітатори і досвідчені педагоги так і молоді фахівці.

Доцільність методичного супроводу для забезпечення професійного зростання вчителів, в процесі дистанційногої освіти полягає у зверненні до проблеми самоаналізу особистості взагалі і самоаналізу професійної діяльності вчительа зокрема. Необхідно звернутм увагу на факт активізації розвитку професійної компетентності вчителів в цілому в будь-якому педагогічному колективі внаслідок реалізації цілісної програми розвитку кадрового потенціалу в системі дистанційної освіти. В цьому контексті визначено, що форми методичного супроводу, організовані у межах діяльності навчального закладу, сприяють розвитку професійної компетентності вчителів.

Сучане суспільство вимагає поглиблення системи професійної освіти за допомогою дистанційної форми навчання, що сприйяє необхідністі перегляду підходів щодо вдосконалення, виникає потреба активізувати процес якісної зміни професійної компетентності вчителів.

Зазначена проблема може бути вирішена через застосування індивідуального підходу як у впливі на мотивацію вчителів самовдосконалюватись, так і в допомозі щодо організації процесу дистанційного навчання. Отже, актуальності набуває вирішення питання створення для вчителів умов професійного вдосконалення та методичного супроводу зазначеного процесу.

При розробці методології дистанційного навчання потрібно враховувати специфіку професійної освіти, оскільки перепідготовка педагогічних кадрів потребує засвоєння практичних навичок, що вимагає безпосередньої участі вчителів у цьому процесі під час навчання. Знання можливостей комп'ютерної техніки, мережі «Інтернет» і методик їхнього використання на сучасному етапі є необхідністю для будь-якого вчительа – як технічної, так і гуманітарної сфери знання.

Освіта через мережу «Інтернет» (дистанційна) може бути визначена як цілеспрямований процес навчання та виховання, що супроводжується формалізованою констатацією досягнень і здійснюється через мережеві канали; основою такої освіти виступає навчання через мережу «Інтернет» – процес передачі та засвоєння знань, умінь, навичок діяльності, що здійснюється з допомогою можливостей глобальної мережі. Освітній процес на базі комп'ютерних технологій та Інтернету обов'язково передбачає диференціацію та індивідуалізацію освіти і навчання Важливим аспектом доцільності включення телекомунікаційних технологій в сучасний педагогічний процес є фактом оволодіння слухачами можливостей здійснювати між собою опосередковане міжособистісне спілкування, передаючи один одному повідомлення у вигляді тексту, звуку і зображення, забезпечуючи тим самим стійку мотивацію пізнавальної діяльності. Сприяють цьому також можливості використовувати мережеві бази даних та інформаційно-пошукові системи, бібліотечні каталоги і файл-сервери, що допомагають залучитися до світових інформаційних ресурсів і організувати освітню діяльність (як під час занять, так і в інший час) на якісно іншому, вищому і більш ефективному рівні

Відзначимо, що дистанційна освіта – це форма організації пізнавальної діяльності, суть якої полягає в такій організації учбового процесу, при якій учні виявляються залученими у процес пізнання, мають можливість розуміти і рефлектувати з приводу того, що вони знають і думають. Крім того, здійснюється процес релаксації, зняття нервового навантаження, перемикання уваги, змін форм діяльності тощо, майбутня освіта носитиме, в основному, евристичний характер і в повному обсязі проявить (і вже проявляє) себе в дистанційній освіті через мережу «Інтернет». Евристична освіта включає в себе спосіб навчання учнів самостійному пошуку і засвоєнню знань, умінь, способів діяльності (замість пасивної «передачі знань»). Процес навчання, таким чином, стає евристичним, тобто перед тим, хто навчається, ставиться якісно нове завдання –

не тільки одержувати знання, але і визначати траєкторію своєї освіти, включаючи розвиток цілей, технологій і змісту освіти.
Актуалізується цінність прецедентів єднання навчально-дидактичних, професійно-діяльнісних завдань і завдань самопізнання, самоосвіти та саморозвитку.
Можна відзначити наступні особливості впливу освіти через мережу «Інтернет» на тих, хто отримує освіту відповідним чином (такі особливості виступають одночасно напрямами видозміни діяльності при використанні мережі «Інтернет» та інших комп'ютерних технологій у освітніх цілях):
1) прискорення процесу екстеріоризації задуму, його матеріалізації у вигляді схеми, таблиці, діаграми, анімації, відеокліпу тощо;
2) розвиток активної візуалізації, пов'язаної з роботою з двовимірною і особливо тривимірною графікою;
3) прискорення отримання результатів шаблонних перетворень ситуації;
4) розширення можливостей здійснення пошукових дій у всьому величезному інформаційному масиві всесвітньої мережі «Інтернет»;
5) інтенсифікація можливостей повернутися до проміжних етапів складної діяльності;
6) розвиток можливостей одночасного розгляду відразу декількох варіантів перетворення об'єкту.
Часто такі відозміни діяльності активно сприяють розвитку творчих потенціалів у тих, хто навчається.
Були визначені психолого-педагогічні умови використання мережі «Інтернет» у освітніх цілях:
1) достатній рівень комп'ютерної письменності вчителів;
2) уміння подати зміст учбового курсу відповідно до обраної форми заняття;
3) наявність відповідної матеріально-технічної бази;
4) моделювання освітнього середовища, що адекватно відображає необхідний зміст, репрезентований освітніми ресурсами мережі «Інтернет» з використанням мультимедійних засобів.
Характерними особливості дистанційної освіти у тих, хто отримує освіту відповідним чином, є наступні:
- підвищення самостійності процесу засвоєння знань, умінь, навичок, розвиток самостійності мислення;
- прискорення процесу екстеріоризації задуму, його матеріалізації у вигляді схем, таблиць, діаграм, анімації, відеокліпів тощо;
- розвиток активної візуалізації, пов'язаної з роботою з двовимірною та особливо з тривимірною графікою;
- прискорення отримання результатів шаблонних перетворень ситуації;
- розширення можливостей здійснення пошукових дій у всьому величезному інформаційному масиві всесвітньої мережі «Інтернет»;
- інтенсифікація можливостей повернутися до проміжних етапів складної діяльності;
- розвиток можливостей одночасного розгляду відразу декількох варіантів перетворення об'єкту.

Метою дистанційного навчання є надання освітніх послуг шляхом застосування інформаційно-комунікаційних технологій для підготовки кваліфікованих робітників відповідно до державних стандартів професійно-технічної освіти.

Дистанційна форма навчання – форма організації навчально-виховного процесу у закладах освіти (ВНЗ, ЗПО, ПТНЗ, ЗНЗ), яка забезпечує реалізацію дистанційного навчання та передбачає можливість отримання випускниками документів державного зразка про відповідний освітній або освітньо-кваліфікаційний рівень.

Технології дистанційного навчання – це комплекс освітніх технологій, в т.ч. психолого-педагогічні та інформаційно-комунікаційні, що надають можливість реалізувати процес дистанційного навчання у навчальних закладах та наукових установах.

Електронний освітній ресурс – навчальні, наукові, інформаційні, довідкові матеріали та засоби, розроблені в електронній формі і необхідні для ефективної організації навчального процесу в частині, що стосується його наповнення якісними навчально-методичними матеріалами.

Дистанційний курс – комплекс навчально-методичних матеріалів та освітніх послуг, створених у віртуальному навчальному середовищі для організації дистанційного навчання на основі інформаційних і комунікаційних технологій.

Система навчально-методичних матеріалів – це структуровані електронні інтерактивні навчальні матеріали, розміщені у віртуальному навчальному середовищі для організації навчання через інтернет, методичні рекомендації для вчителів.

Центральним компонентом навчальної дисципліни у дистанційному навчанні є *дистанційний курс*, який повинен мати:

- якісний контент;
- структуру навчально-методичних матеріалів;
- логіку вивчення навчального курсу;
- чіткий графік виконання учнями навчального плану;
- критерії, засоби і системи контролю та оцінювання;
- налагоджену систему взаємодії учня та педагога.

Вчитель має змогу самостійно створювати дистанційні курси, налаштовуючи відповідні ресурси, підписувати учнів на курс і керувати їх навчанням. Вчителі можуть дистанційно через інтернет ознайомлюватись з навчальними матеріалами, отримувати завдання та методичні вказівки щодо їх виконання, надавати результати, проходити контроль знань у вигляді тестування. Доступ суб'єктів освітнього процесу до дистанційних курсів доцільно зробити персоніфікованим з використанням індивідуальних логінів та паролів.

Основними видами навчальних занять за дистанційною формою є:

- лекції;
- лабораторно-практичні заняття;
- консультації та ін.

Отримання навчальних матеріалів, спілкування між слухачем та педагогом під час дистанційних навчальних занять забезпечується передачею відео-, аудіо-, графічної та текстової інформації у синхронному або асинхронному режимі.

Вимоги щодо самостійного вивчення навчального матеріалу конкретної навчальної дисципліни визначаються її навчальною програмою, методичними вказівками, інструкціями й завданнями, що містяться у дистанційному курсі.
Лекції, консультації можуть проводитися як в синхронному (в режимі реального часу), так і в асинхронному режимі відповідно до навчального плану. В асинхронному режимі учні можуть отримувати конспект лекцій у текстовому чи графічному вигляді або аудіовізуальний запис лекційного матеріалу. У синхронному режимі може використовуватися текстовий чат та вебінари.

Практичні заняття, які передбачають виконання практичних робіт, відбуваються дистанційно в асинхронному режимі.
Структура дистанційного курсу. Дистанційний курс повинен відповідати вимогам галузевих стандартів щодо змісту, обсягу та рівня освітньої та професійної підготовки, діючим в навчальному закладі регламентуючим документам щодо розробки навчально-методичних матеріалів, навчальним планам.
Якісний дистанційний курс має складатися з наступних елементів:

✓ ***Анотація*** – це невеликий матеріал, що презентує курс. Анотація повинна містити назву курсу, коротку характеристику курсу, перелік тем, кількість годин, які відводяться на вивчення курсу, інформація про статус курсу (в розробці, апробація, сертифікований в МОН України) тощо.

✓ ***Загальна інформація про курс (вступ)*** – окрема секція курсу з коротким описом та інформаційним матеріалом щодо дисципліни, який розкриває перелік елементів цього курсу та особливості його опанування. Саме в цій секції рекомендується розташувати частину структурних елементів навчально-методичного та дидактичного забезпечення дистанційного навчання.

✓ ***Методичні рекомендації щодо використання ресурсів курсу, послідовності виконання завдань, особливостей контролю*** – загальна інформація, яка допоможе учням ефективно використовувати веб-ресурси курсу в цілому. В рекомендації обов'язково повинні міститися календарний план (графік) вивчення дистанційного курсу та критерії оцінювання.

✓ ***Робоча навчальна програма (РНП)*** – обов'язковий елемент дистанційного курсу, який містить:

- мету, завдання та результати (компетенції) вивчення дисципліни;
- структуру дисципліни та розподіл годин за темами;
- тематику та зміст теоретичних та лабораторно-практичних занять, самостійної роботи учнів;
- завдання для контролю;
- критерії оцінювання знань учнів;
- список рекомендованої літератури.

✓ ***Підручник (навчальний посібник, конспект лекцій)*** – основний змістовний модуль дисципліни, який розкриває теоретичний зміст кожної теми за всіма питаннями, що входять до неї.
При відсутності підручників або посібників можуть застосовуватися електронні конспекти лекцій, що містять структурований теоретичний матеріал,

мультимедійні презентації з тем, додаткові навчальні матеріали (флеш-ролики, аудіо-, відеоматеріали, нормативні документи тощо).

- ***Консультації*** – необхідні для спілкування учнів з вчительем або один з одним для обміну досвідом. Для консультацій визначається час початку, тривалість і періодичність.
- ***Методичні рекомендації щодо організації самостійної роботи*** – повинні орієнтувати учнів на ознайомлення з програмою курсу та послідовність самостійної роботи щодо тем курсу.
- ***Практичні роботи*** – розробляються з кожної теми курсу (відповідно навчальної програми), додатково можуть міститися таблиці, схеми, а також методичні вказівки щодо їх виконання.
- ***Тестові завдання*** – розробляються з окремих тем (модулів) та з дисципліни в цілому й мають на меті перевірку (самоперевірку) ефективності навчальної роботи з дисципліни.
- ***Глосарій*** – перелік в алфавітному порядку термінів, ключових понять курсу з визначенням їх сутності.
- ***Список рекомендованої літератури*** – включає основну, допоміжну літературу, нормативні документи та інформаційні ресурси.
- ***Автори дистанційного курсу*** – це список авторів змістовної частини курсу, авторів дизайну та програмування із зазначенням посад, наукових ступенів та педагогічних звань.

При компоновці структурних елементів у дистанційному курсі рекомендується дотримуватися наступної структури

Технології дистанційного навчання:

кейс-технологія - заснована на використанні наборів (кейсів) текстових, аудіо-візуальних та мультимедійних навчально-методичних матеріалів та їх розсиланні для самостійного вивчення та організацією регулярних консультацій з вчительями (тьюторами) традиційним або дистанційним способом;

ТВ-технологія - базується на використанні систем телебачення для доставки навчально-методичних матеріалів та організації регулярних консультацій з вчительями (тьюторами);

інтернет-мережева технологія - базується на використанні мереж Інтернет та телекомунікацій для забезпечення навчально-методичними матеріалами та інтерактивної взаємодії між суб`єктами навчання;

змішана технологія

Стратегія дистанційного навчання:

Стратегія асинхронного дистанційного навчання. Учасники освітнього процесу не спілкуються у режимі реального часу і обмежені лише конкретними періодами часу, у який мають бути завершені окремі етапи роботи.

E-mail дистанційне навчання здійснюється через листування мережею Інтернет. Класичний варіант E-mail навчання передбачає отримання слухачем щоденних у один і той же час поштових повідомлень, що містять невелику кількість текстового матеріалу та перевірочні питання до нього. До листа також можуть входити активні посилання на додаткові матеріали (статті з періодичних видань,

оригінальні тексти, презентації, відео фрагменти), що їх можна переглянути у мережі «Інтернет».

Для спрощення доставки матеріалів можна їх надсилати всім учасникам навчання одним листом, вказавши їхні електронні адреси через крапку з комою у рядку адресування. По завершенні періоду дистанційного навчання надаються перевірочні завдання, що складені з питань, які надавалися під час вивчення окремих фрагментів матеріалу.

Стратегія навчання на платформах соціальних мереж. У обраній соціальній мережі (Google+, FaceBook тощо) створюється окрема група (коло, спільнота), на якій вчитель розміщує навчальні матеріали. Це можуть бути як його власні матеріали, так і матеріали інших авторів з теми, що знайдені у в Інтернеті, або у тій же самій соціальній мережі. Слухачам пропонується ознайомитися з матеріалами і написати до них коментар на задану тему (можуть бути як однакові, так і різні) і встановленого обсягу. У цьому випадку краще використовувати завдання, які потрібно обговорювати, хоча, і розрахункові завдання допускаються. Наприклад, для невеличкого есе-коментаря достатньо 1000–1200 символів без урахування відступів, а відповідь на розрахункове завдання може виглядати як звичайне число, або зображення сторінки зошита з його розв'язанням.

При такій формі асинхронного спілкування матеріали і відповіді доступні всім учасникам навчального процесу, але, за необхідністю, вчитель може звернутися до учня через панель швидких сповіщень (чат). Слід зазначити, що характер створеної спільноти має бути таким, щоб вчитель мав можливості керувати сторінкою і вилучати невдалі матеріали і коментарі, розміщені на ній учнями. Також для зручності можна обрати формат спільноти з обмеженим доступом (тільки для учасників спільноти).

Стратегія синхронного дистанційного навчання. Вимагає від учасників освітнього процесу одночасної присутності у віртуальному середовищі хмарного сервісу або програми. Здійснюється шляхом організації одночасної зустрічі учасників навчання через різноманітні сервіси для on-line спілкування (Skype, GoogleTalk, спільні документи).

Організація такої форми роботи може бути досить складною при великій кількості учасників освітнього процесу (безкоштовні сервіси для спілкування підтримують невелику кількість учасників, не всі учасники своєчасно під'єднуються до зустрічі через технічні складнощі налаштувань пристрою чи швидкості Інтернет-зв'язку тощо), тому цю форму доцільніше використовувати як додатковий елемент іншої форми асинхронного дистанційного навчання. Наприклад, вчителі поділяються на групи, кожній з яких надається завдання скласти (відредагувати, обговорити тощо) спільний навчальний матеріал, розташований на сервісі спільних документів. Тоді учасники групи самі зв'язуються між собою для виконання завдання, а результати (за необхідності й процес) його виконання вчитель може спостерігати у обраному хмарному середовищі або отримати його від учнів електронною поштою.

Організація самостійної роботи педагога під час дистанційного навчання. На основі аналізу організації самостійної роботи за традиційною формою навчання,

відповідно до навчального плану, потрібно розробити навчально-тематичний план самостійної роботи в умовах проведення дистанційного навчання для відповідного навчального предмету.

Доцільно сформувати завдання для самостійної роботи, враховуючи особливості використання технічних засобів підтримки дистанційного навчання. При цьому потрібно брати до уваги, що не всі форми та методи самостійної роботи можна автоматично перенести в електронне навчальне середовище. Вчителю необхідно спроектувати весь цикл завдань за темами, що вивчаються. Звичні для традиційної форми навчання адаптуються для роботи з гаджетами: вірші у формат відеозапису, контрольні роботи – у формат тестів.

При виконанні самостійної роботи в системі дистанційної освіти необхідно:

забезпечити відповідний рівень допомоги та підтримки самостійної роботи вчителів;

сформувати перелік завдань;

визначити, індивідуальні завдання;

рівень завдань повинен враховувати загальний рівень володіння педагогами інформаційними технологіями.

Унаслідок упровадження інформаційних технологій в усі сфери життєдіяльності людини в рамках мережевої взаємодії виникли нові види комунікації, які умовно можна поділити на чотири категорії:

- асинхронна комунікація «один на один»;
- асинхронна комунікація «багатьох з багатьма»;
- синхронна комунікація «один на один», «один і кілька», «один із кількома»;
- асинхронна комунікація «багато і один», «один на один», «один і багато».

Сучасна доросла людина живе в інформаційному суспільстві – суспільстві глобальної компетентності, в якому очевидними є виклики щодо її безперервного професійного й особистісного зростання, особистісної активності та ефективного самоздійснення у мінливих умовах життя. Як відомо, обсяг знань, який породжується у світовому співтоваристві, подвоюється кожні два-три роки, що загострює проблему невідповідності знань і вмінь економічно активного населення потребам ринку праці, робить особливо актуальними питання підвищення якості безперервної освіти, розширення меж традиційної системи освіти, надання їй більшої відкритості, доступності та гнучкості, розкриття особистості в процесі навчання з урахуванням її вікових, психологічних і соціальних особливостей.

Сучасні заклади навчання в системі післядипломної освіти повинні забезпечувати різнобічний розвиток слухача курсів підвищення кваліфікації як особистості, сприяти виявленню та розвитку здібностей, враховувати індивідуальні відмінності, розвивати самостійність, творчість, наполегливість та відповідальність, не забуваючи при цьому, що відбувається навчання сформованого педагога.

Система перепідготовки педагогів – сучасна проблема, викликана швидким старінням раніше набутих навичок і необхідністю засвоїти нові. В умовах безперервної освіти пряме педагогічне керівництво замінюється

опосередкованим, навчання все більше приймає форму самоосвіти. Тому вчительеві в системі удосконалення педагогічної освіти надзвичайно необхідно володіти специфікою навчання та самонавчання, враховувати певні особливості, а саме:

- усвідомлює себе самостійною, самокерованою особистістю;
- накопичує значний запас життєвого (побутового, професійного, соціального) досвіду, який перетворюється на важливе джерело навчання його самого і його колег;
- виявляє готовність до навчання (мотивація), прагне за допомогою навчальної діяльності вирішити свої життєво важливі проблеми і досягти конкретної мети;
- прагне до невідкладної реалізації отриманих знань, умінь, навичок і якостей;
- його навчальна діяльність значною мірою обумовлена тимчасовими, просторовими, професійними, побутовими, соціальними факторами (умовами).

У ситуації дистанційного навчання існує певна специфіка, пов’язана із тим, що процес навчання є технічно опосередкованим.

Необхідно звернуть увагу на проблеми організації комп’ютерного навчання та характеристики людино-машинної комунікації в навчальних системах. Віртуальне навчальне середовище вимагає специфічного погляду на процеси навчання та учіння не лише у фізичному, а й у психологічному аспекті. Психологічна комфортність навчального середовища для користувача є однією з передумов успішного, тобто ефективного, навчання й учіння. У концепції психологічної комфортності вирізняються два важливі аспекти: діалогово-інтерфейсний і соціально-організаційний. Перший із них відображає відповідність способу і форми подання інформації в навчальному середовищі психологічним і фізіологічним закономірностям сприйняття й обробки інформації людиною, задає вимоги до організації подання інформації, до модальності подання інформації, до візуального, текстового, лінгвістичного та інших аспектів комунікації учня з системою.

Інформацію, процес обробки якої особистістю є утрудненим, можна трансформувати у сферу візуального руху, де перебіг цього процесу відбувається краще і легше. Наприклад, якщо людині важко сприймати і запам’ятовувати такі кількісні величини, як температура, обертальний момент, вага, можна трансформувати завдання сприйняття цих величин у такі завдання, коли наш мозок має справу з візуальними формами, величинами, візуальною оцінкою відносного місцезнаходження: стрілка знаходиться справа чи зліва відносно певної позначки на шкалі, а може, просто на ній? Людський мозок успішно сприймає форми та відносне місцезнаходження. Якщо звернутися до проблеми забезпечення психологічної комфортності навчання, то виникає цілком очевидна асоціація. В діалогово-інтерфейсному аспекті, вимога комфортного навчання ставить перед проектувальниками завдання організувати взаємодію людини із системою таким чином, щоб максимально полегшити сприйняття і розуміння інформації, заощадити йому час і сили, які мають бути витрачені на змістовну інтелектуальну роботу, а не на подолання перешкод при спілкуванні із

системою, при отриманні, засвоєнні та розумінні нового знання. Вищезгадана трансформація перцепції може не лише полегшити сприйняття «невидимої» або складної інформації, а й підвисити інтенсивність потоку інформації через інтерфейс, тобто за менший час може бути прийнято більшу кількість інформації.

Одним із векторів дистанційної взаємодії суб'єктів освітнього процесу є умова комфортності навчального середовища. В це поняття вкладається як умова фізичної зручності, так і умова задоволення його базовими потребами. Тобто, відповідну комфортність можна розглядати як внутрішній (відносно структури особистості індивіда) чинник ефективності діяльності в цілому і навчальної діяльності зокрема, який у ситуації навчання стосується насамперед організації діалогової взаємодії.

При цьому варто пам’ятати, що метою комп’ютерно-опосередкованого навчання, так само, як і традиційного, є досягнення цілей навчання, як найближчих, так і віддалених. До найближчих цілей навчання належить засвоєння учнем конкретного способу дій у процесі розв’язання задачі певного типу, що передбачає також засвоєння певних декларативних і процедурних знань. Віддаленими цілями навчання вважається досягнення змін у структурі особистості учня, зокрема в когнітивній і особистісній сферах. При цьому загальна мета навчання – навчити людину аналізувати, робити висновки, усвідомлювати сутності та зв’язки між ними, встановлювати відношення між поняттями, генерувати нові знання, проводити пошук інформації, а також сформувати в ній самостійність дії і мислення, готовність до прийняття рішень, відкритість до сприйняття нового. Навчання можна назвати ефективним, якщо воно дозволяє досягти поставленої мети.

Дистанційне навчання розширює і оновлює функції вчителя, який має координувати пізнавальний процес, постійно вдосконалювати навчальний процес, що здійснюється дистанційно, підвищувати творчу активність і кваліфікацію згідно з нововведеннями та інноваціями.

Особливий інтерес становить та обставина, що під час дистанційного навчання інколи знижується мотивація до навчання, трапляється, що вчителі припиняють навчатися у прямому і переносному розумінні. Незважаючи на те, що мотивами відмови вчителів від подальшого проходження будь-якого самостійного завдання дистанційно називають в основному побутові причини (брак часу, сімейні проблеми, обставини на роботі, проблеми зі здоров’ям, технічні проблеми неможливості працювати в інтернет-середовищі тощо), це непрямі чинники. Причиною цього швидше є мотиваційний і емоційний компоненти навчання.

Проблема переривання традиційного дистанційного навчання тим, хто навчається, розглядається досить активно. Так, було досліджено, що чинником, який найбільше впливає на рішення студентів продовжити або перервати дистанційне навчання, є задоволеність або незадоволеність спілкуванням із вчительем. Під час дослідження Каськеллі, Денехера і Прунелла, проведеного у 1997 р. у Відкритому університеті Великої Британії, було виявлено, що контакт

із вчительем необхідний не лише для з'ясування незрозумілих тем, а й для підтримки мотивації до навчання і співпраці з однокурсниками.
Таким чином, не тільки недостатнє спілкування з вчительем-консультантом впливає на бажання слухача припинити дистанційне навчання, а й відчуття ізольованості та браку взаємовідносин із колегами по навчанню. Важливим фактором у перериванні дистанційного навчання стає досвід «взаємодії» слухача із комп'ютером. Слухач, який є користувачем-початківцем, за наявності більш ніж скромної текстової комунікації через відсутність звичайних елементів невербальної комунікації (візуальна інформація, вираз обличчя, зоровий контакт, жести та інші засоби невербальної комунікації), елементарних знань персонального комп'ютера відчуває невдоволеність, дискомфорт від власної неспроможності, а як наслідок – знижується його самооцінка.
Тому першочерговим завданням тьютора є оптимізація навчального процесу, перетворення його на комунікативно сприятливий, тобто такий, щоб вчителі безпосередньо контактували між собою, відчували себе причетними до групи, навчального закладу в цілому.
Дидактична ефективність як навчальної системи, так і традиційного класного навчання посилюється в разі забезпечення комфортного спілкування. Комфортний стан спричиняє позитивне світосприйняття, що підвищує мотивацію індивіда стосовно його діяльності, а це є справедливим для будь-якої форми навчання, як найсучаснішої, з використанням інформаційно-комунікаційних технологій, так і традиційної класної. Діяльність, яка не має достатньої мотивації, не дає і належних результатів.
Із точки зору концепції розвивального навчання, засвоєння нового знання означає не запам'ятовування певної інформації, а узгодження між собою нового знання і того, що вже існує в когнітивній структурі індивіда, корекція ментальних моделей індивіда шляхом «вбудовування» нового знання в наявну систему поглядів на світ.
Певна недосконаліть процесу дистанційного навчання заключається у тому, що відсутній повноцінний емоційний контакт під час навчання; недостатні комунікативні зв'язки, тому необхідно всебічно підтримувати зворотний зв'язок; організувати педагогико-акмеологічний супровід навчального процесу.
Найбільш ефективною в дистанційному навчанні є синхронна комунікація, коли той, хто навчається, веде безпосередній діалог з вчительем, може задати йому запитання відразу, у момент його виникнення, а також висловити свою думку щодо виконання завдання. У концепції дистанційного навчання таку можливість може забезпечити використання в навчанні соціальних мереж.
Соціальні мережі насамперед спрямовані на забезпечення віртуальної взаємодії та налагодження комунікації між людьми. Завдяки рівним правам користувачів у рамках соціальної мережі взаємодія набуває характеру невимушеності й відкритості. Так, використання соціальних мереж в освіті, крім досягнення основної мети – навчання, додатково надає вчителю такі можливості, як обмін досвідом із колегами, знайомство з новими методиками, демонстрація та обговорення власних напрацювань, що сприяє професійному зростанню.

З усього різноманіття сфери використання соціальних мереж для освітнього процесу можна виокремити такі функції:

- соціальна мережа як месенджер (використовується для онлайн-консультацій і організації поточної взаємодії учнів та вчителя);
- соціальна мережа як дошка оголошень (використовується для важливих повідомлень та анонсів майбутніх подій);
- соціальна мережа як каталог бібліотечних ресурсів (інтернет-бібліотеки, що дозволяють посилатися на джерела інформації з дотриманням всіх правил наукового цитування);
- соціальна мережа як замінник паперових періодичних видань.

Таким чином, використання соціальних мереж у навчанні сприяє формуванню єдиного інформаційного простору системи освіти, створенню відкритих порталів освітніх ресурсів, об'єднанню кадрового потенціалу педагогів, організації системи постійної консультативної та інформаційної підтримки всіх учасників навчального процесу, а також підвищенню комп'ютерної грамотності та формуванню нової культури мислення всіх учасників освітнього процесу.

Із розвитком інформаційного суспільства в Україні з'являються нові інструменти для організації пізнавальної діяльності, а соціальні мережі є одним із найбільш ефективних з них. Зважаючи на психологічні особливості молодих людей комп'ютерного покоління, сучасний педагог може використовувати соціальні мережі як педагогічний засіб навчання. Так, учні, перебуваючи у звичному для них віртуальному середовищі, можуть бути залучені до пізнавальної діяльності. Однак при цьому варто пам’ятати, що віртуальне навчання жодним чином не повинно замінити традиційних шкільних занять. Воно може бути їх доповненням для вирішення таких завдань, як проектна діяльність, онлайн-консультування і дистанційне навчання.

Використання соціальних мереж у навчанні сприяє розвитку інтелектуального і творчого потенціалу, підвищенню комп'ютерної грамотності всіх учасників навчального процесу, вирішенню ряду дидактичних завдань, які обмежені в традиційному процесі навчання.

- дистанційні курси;
- вебсторінки й сайти;
- хмарні сервіси;
- електронна пошта;
- форуми й блоги педагогів, чати;
- теле – і відеоконференції;
- віртуальні класні кімнати тощо.
- online спілкування (Skype, Viber, WhatsApp, Google Hangouts).

Розвиток технологій дистанційної освіти, інформаційно-комунікаційних технологій та можливостей програмного і апаратного забезпечення, і як наслідок, проблема блискавичного застарівання знань, зменшення періоду напіврозпаду компетентності зумовлюють потребу у вдосконаленні системи освіти, зокрема у пошуку нових шляхів здобуття знань.

Останнім часом запроваджуються відкриті онлайн-курси, які сприяють рівному доступу до освіти будь-кого, без аналізу попереднього рівня освіти, незалежно

від регіону проживання. Серед ознак МВОК відповідно до назви виділяють такі основні: масовий – велика кількість учасників; відкритий – безкоштовний, доступний будь-кому в будь-який момент, незалежно від дати початку і завершення; такий, що використовує відкриті ресурси, тобто відкрите програмне забезпечення. У зв'язку із стрімким розвитком нової технології з'явилася потреба в агрегаторах масових відкритих онлайн-курсів, які дають змогу переглядати каталог доступних курсів із різних платформ, різних розробників, користуватися засобами навігації та пошуку (обирати курси за тематикою, розробниками, спеціалізаціями тощо); порівнювати курси завдяки рейтингам та відгукам вчителів курсів; формувати індивідуальну траєкторію навчання (завдяки створенню власного аккаунта, інструментам нагадування про початок курсу тощо).

При цьому кожен із вчителів курсу проявляє активність стосовно інших, бере участь в обговореннях, дискусіях, але має персональне навчальне середовище, яке формується із зручних для нього інструментів. Водночас слід звернути увагу, що цей напрям дистанційної освіти більше задовольнить самостійних та цілеспрямованих вчителів, які здатні працювати з великими масивами інформації і раціонально організовувати власну діяльність. Отже, найкраще їх використовувати для неперервного навчання чи підвищення кваліфікації.

Недоліками такого дистанційного навчання є: обмеженість типів завдань – в основному використовуються такі, які можуть бути автоматично оцінені (розрахункові питання, вибір правильної відповіді тощо); водночас це зумовлює проблему у таких дисциплінах, які потребують розгорнутих відповідей; обмеженість зворотнього зв'язку – через велику кількість учасників курсу вчитель не може фізично поспілкуватися із кожним, тому велику роль відіграють обговорення, консультації з іншими учасниками курсу; ідентифікація особистості – оскільки весь процес проходження курсу відбувається дистанційно, вчитель не може бути впевненим, що відповіді дає саме зареєстрований студент, що перевірка знань відбувається без звернення до додаткових джерел чи сторонньої допомоги.

У використанні таких курсів є безумовні переваги, як для самого навчального закладу, який їх впроваджує, так і для їх учасників рівний доступ до якісної освіти – можливість вивчати курси провідних ВНЗ світу, навчатися у досвідчених і висококваліфікованих вчителів; обирати ті курси, які дійсно викликають зацікавленість; самостійно формувати свою освітню траєкторію відповідно до власних потреб; відкритість курсу світовій спільноті покращує якість підготовки такого курсу; підвищує рейтинги як вчителя, так і ВНЗ; свідчить про новий рівень викладання, інтеграцію до світового освітнього простору; дає можливість залучення більш ширшого кола.

Гнучкість та широкий інструментарій дистанційної освіти дає змогу використовувати її технології при очній формі навчання (перевірка домашнього завдання, контроль рівня засвоєння навичок та вмінь), в поєднанні із заочною формою (консультації в режимі «онлайн», телеконференції), а також як окремий тип організації навчання (веб-курс, тренінг). З використанням новітніх засобів усі необхідні навчальні ресурси (підручники, посібники, дидактичний матеріал,

педагогічні програмні засоби тощо) зберігаються в єдиному сховищі з постійним доступом до них.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. д-ра техн. наук, професора В.Б. Толубка. К.: ДУТ, 2015. 288 с.
2. Воротникова І.П. Умови формування цифрової компетентності вчителя у післядипломній освіті. *Відкрите освітнє е-середовище сучасного університету*, 2019. №6. С. 101–118. URL: https://doi.org/10.28925/2414-0325.2019.6.101118 (дата звернення: 09.05.2024)
3. Гончаренко С.У. Дидактичні аспекти освіти дорослих *Освіта дорослих: теорія, досвід, перспективи.* 2009. Вип. 1. С. 67–73.
4. Грабовський П.П. Критерії, показники і рівні розвитку інформаційної компетентності вчителя природничо-математичних предметів. *Інформаційні технології в освіті.* 2015. № 24. С. 135–147.
5. Гравіт В.О. Особливості впровадження дистанційного навчання в післядипломну педагогічну освіту. *Педагогіка і психологія.* 2003. № 1 С. 67–75.
6. Гуревич Р.С. Формування інформаційної компетентності майбутніх учителів засобами мультимедійних технологій. *Наукові записки*. Серія: Педагогіка. 2007. С. 38–41.
7. Державний стандарт освіти. Державний стандарт початкової освіти. Веб-сайт. URL: https://www.kmu.gov.ua/ua/npas/pro-zatverdzhennya-derzhavnogo-standartu-pochatkovoyi-osviti (дата звернення 20.05.2024)
8. Дистанційне навчання: психологічні засади : монографія / М.Л. Смульсон, Ю.І. Машбиць, М.І. Жалдак та ін.; за ред. М.Л. Смульсон. Кіровоград : Імекс-ЛТД, 2012. 240 с. URL: http://umo.edu.ua/biblioteka-kafedri. (дата звернення: 16.05.2024)
9. Дистанційні курси. Методичні рекомендації щодо підготовки веб-ресурсу дисциплін при організації навчального процесу за дистанційною формою / Укл. Новомлинець О.О., Дрозд О.П.. Чернігів: ЧНТУ. 2013. 32 с.
10. Європейська рамка цифрової компетентності для освітян. URL: https://joint-research-centre.ec.europa.eu/digcompedu_en (дата звернення: 14.05.2024).
11. Захист дітей у цифровому середовищі: рекомендації для батьків та освітян, 2020. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za-initsiativi-mintsifri- pidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP-Guidelines- for-Parents-Educators-UAfin.pdf (дата звернення: 16.05.2024)
12. Ігнатушко Ю.І. Правові засади регулювання забезпечення кібербезпеки в Україні VIII URL: http://dspace.oduvs.edu.ua/bitstream/123456789/471/1/ilovepdf_com-18-19%5B1%5D.pdf (дата звернення: 16.05.2024)
13. Калініна Л.М. Інформаційне управління загальноосвітнім навчальним закладом: системи, процеси, технології: моногр. Київ – Херсон : Айлант, 2005. 270 с.

14. Калініна Л.М. Система інформаційного забезпечення управління загальноосвітнім навчальним закладом: моногр. Київ. Херсон : Айлант, 2005. 275 с.
15. Колеснікова І. В. Цифровізація освітнього процесу в закладі післядипломної педагогічної освіти. *Науковий часопис* Нац. пед. ун-т імені М.П. Драгоманова. Серія 5. Педагогічні науки: реалії та перспективи, 2020. Випуск 78. С.117–120.
16. Концепція розвитку цифрових компетентностей до 2025 року, 2021. URL: https://thedigital.gov.ua/storage/uploads/files/news_post /2021/3/ kabmin-skhvaliv-kontseptsiyu-rozvitku-tsifrovikh-kompetentnostey-do-2025-roku/Dodatok-2.pdf (дата звернення: 14.05.2024).
17. Корченко, О.Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. Курс мережевої академії Cisco: Cybersecurity Essentials, 2020. URL: https://www.netacad.com/courses/cybersecurity/ cybersecurity-essentials (дата звернення: 14.05.2024).
18. Литвинова С.Г. Методика проектування хмаро орієнтованого навчального середовища загальноосвітнього навчального закладу на рівні керівника. *Комп'ютер у школі та сім'ї.* 2015. № 2 (122) С. 5–11.
19. Ляхоцька Л.Л. Акмеологічні особливості дистанційного навчання у підвищенні кваліфікації керівних кадрів освіти. Педагогічні аспекти IV Відкритого дистанційного навчання : монографія / О.О.Андрєєв, К.Л. Бугайчук, Н.О. Каліненко та ін.; за ред. О.О Андрєєва, В.М. Кухаренка. Харків, 2013. С. 136–148.
20. Ляхоцька Л.Л. Концептуальні засади проектування технологій навчання в системі відкритої післядипломної педагогічної освіти. URL: http://umo.edu.ua/e-biblioteka-laboratoriji (дата звернення: 16.05.2024)
21. Ляхоцька Л.Л. Психолого-педагогічні особливості навчання керівних кадрів освіти за очно-дистанційною формою підвищення кваліфікації (акмеологічний підхід). *Вісник післядипломної освіти* : зб. наук. пр.: у 2-х ч. / Ун-т менедж. освіти НАПН України. К. : АТОПОЛ, 2013. Вип. 9 (22). Ч. 1. С. 129–140.
22. Ляхоцька Л.Л. Концептуальні засади модернізації дистанційного навчання в системі післядипломної педагогічної освіти (університетський досвід). *Нова педагогічна думка*: наук.-метод. журнал, 2013. №2 (74). С. 52–57.
23. Маркова Є.С. Інформаційні технології навчання. Навчально методичний посібник. Запоріжжя, «Просвіта», 2012. 121 с.
24. Медіа-культура особистості: соціально-психологічний підхід / За ред. Л.А. Найдьонової, О.Т. Баришпольця. К. : Міленіум, 2009. 440 с.
25. Методичні рекомендації щодо організації навчання з використанням технологій дистанційного навчання. URL: http://dlc.onaft.edu.ua/index.php/novini/28-metodichni-vkazivki-2.html (дата звернення: 16.05.2024).
26. Мироненко Г.В. Динаміка уявлень реципієнтів відеопродукції про тривалість одиниці часу. *Проблеми загальної та педагогічної психології*: Зб. наук. праць Ін-ту психології ім. Г. С. Костюка АПН України. Т. 8. Ч. 8. К.: ГНОЗІС, 2006. С. 162–170.

27. Методика оцінювання ефективності наукової, науково-технічної та інноваційної діяльності наукової установи: наказ Міністерства освіти і науки України від 17.09.2018 № 1008. URL: https://zakon.rada. gov.ua/laws/show/z1504-18 (дата звернення: 14.05.2024).
28. Проєкт Концепції цифрової трансформації освіти і науки на період до 2026 року. URL: https://mon.gov.ua/ua/news/koncepciya-cifrovoyi-trans formaciyi-osviti-i-nauki-monzaproshuye-do-gromadskogo-obgovorennya (дата звернення: 29.05.2024).
29. Морзе Н.В. Підвищення кваліфікації вчителів з використанням дистанційних технологій навчання. Зб. наук. праць. К. : НПУ ім. М.П. Драгоманова. 2001. Вип. 4. 324 с.
30. Морзе Н.В. Як навчати вчителів, щоб комп‘ютерні технології перестали бути дивом у навчанні. *Комп‘ютер у школі та сім‘ї.* №6 (86). 2010. С.10–14.
31. Морзе Н.В., Воротникова І.П. Модель ІКТ компетентності вчителів / Scientific Journal «ScienceRise: Pedagogical Education». № 10(6) 2016. URL: http://journals.uran.ua/sr_edu/article/view/80644 (дата звернення 26.05.24)
32. Навчально-методичний посібник для вчителів щодо організації дистанційної форми навчання з перепідготовки та підвищення кваліфікації / За ред. Ісаєнка В.М., Кашина Г.С., Ніколаєв К.Д., Павлюченко Л.С. К. : Видавництво НПУ ім. М.П. Драгоманова, 2014. 100 с.
33. Національна онлайн-платформа для розвитку цифрової грамотності «Дія. Цифрова Освіта». URL: https://osvita.diia.gov.ua/courses/cyber-hygiene (дата звернення: 14.05.2024).
34. Нова Концепція української школи / Упорядники: Л. Гриневич, О. Елькін, С. Калашнікова, І.Коберник, В. Ковтунець та ін; за заг. ред. М. Грищенко. 2016. 34 с.
35. Нова українська школа: порадник для вчителя / за ред. Н. М. Бібік. Київ: ЛітераЛТД, 2018. 160 с.
36. Носенко Ю. Здоров’я збережувальний складник ІК-компетентності учнів як важливий елемент здоров’я збережувального використання засобів у навчальному процесі основної школи. *Нова педагогічна думка.* 2016. №2. С. 30–35.
37. О.Г. Корченко, В.Л. Бурячок, С.О. Гнатюк Безпека інформації. 2013. Т. 19, № 1. С. 40–45
38. Онлайн-курс. «Основи кібергігієни». URL: https://cybereducation.org/ (дата звернення: 14.05.2024).
39. Організація комп’ютерних мереж : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп’ютерні науки» / КПІ ім. Ігоря Сікорського; Ю.А. Тарнавський, І.М. Кузьменко. Київ : КПІ ім. Ігоря Сікорського, 2018. 259 с
40. Основи стандартизації інформаційно-комунаційних компетентностей в системі освіти України: метод. рекомендації, за заг. ред. В.Ю. Бикова, О.М. Спіріна, О.В. Овчарука. К. : Атіка, 2010. 88 с.

41. Павленко І.М. Інтернет в управлінській діяльності. *Освітні інновації: філософія, психологія, педагогіка:* збірник наукових статей у 2 частинах / За заг. ред. О.В. Зосименко. Суми : ФОП Цьома С.П., 2017. Ч. 2. С. 327–332.
42. Павленко І.М. «Хмарні» сервіси в навчально-виховній діяльності. *Науково-прикладні основи створення та використання електронних засобів у навчально-виховному процесі загальноосвітнього навчального закладу* : матеріали VI Всеукраїнської інтерактивної науково-практичної конференції, 25.10 – 26.10.17, РОІППО. Рівне, 2017. С. 325–329. URL: http://roippo.org.ua/activities/research/conferenc.php/926/ (дата звернення 26.05.24)
43. Павленко І.М. Підготовка керівника в системі післядипломної освіти до використання Інтернет-технологій в управлінській діяльності. *Електронні інформаційні ресурси: створення, використання, доступ:* Збірник матеріалів Міжнародної науково-практичної Інтернет-конференції. Вінниця : ВНТУ, 2017. С. 170–174.
44. Професійно-комунікативна компетентність (в туризмі) : підручник І.М. Писаревський, С.А. Александрова; Харк. нац.акад. міськ. госп-ва. Х : ХНАМГ, 2010. 230 с.
45. Підвищення кваліфікації керівників освіти за дистанційною формою навчання. Навч. посібник. / Олійник В.В., Биков В.Ю., Гравіт В.О., Кухаренко В.М., Жук Ю.О., Антощук С.В., Кліменко А.Л., Сябрук Т.І. / За заг. ред. В.В. Олійника. К.: Логос, 2006. 408 с.
46. Положення про дистанційну форму здобуття повної загальної середньої освіти: наказ МОН України від 08.09.2020 №1115. URL: https://mon.gov.ua/ua/npa/deyaki-pitannya-organizaciyi-distancijnogo-navchannya -zareyestrovano-v-ministerstvi-yusticiyi-ukrayini-94735224-vid-28-veresnya-2020-rokuclass/2190095-intel-blended (дата звернення: 16.05.2024).
47. Приходько В.М., Комунікативна компетентність керівника навчального закладу як основа професійної культури спілкування. Запоріжжя. *Управління школою* №25 (181)
48. Про захист персональних даних: за станом на 19.08.2022: Закон України від 01.06.2010 № 2297-VI URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 16.05.2024).
49. Про національну безпеку України: Закон України від 21.06.2018, № 2469-VIII URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 16.05.2024).
50. Про Національну програму інформатизації: Закон України від 04.02.1998 № 74/98-ВР URL: http://zakon0.rada.gov.ua/laws/show/74/98-вр (дата звернення: 05.05.2024).
51. Про освіту : Закон України від 05.09.2017 № 2145-VIII. URL: https://zakon.rada.gov.ua/ laws/show/2145-19 (дата звернення: 05.05.2024).
52. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII URL: http://zakon0.rada.gov.ua/laws/show/2163-19 (дата звернення: 05.05.2024).

53. Рекомендації ЮНЕСКО щодо політики в сфері мобільної освіти.URL: http://iite.unesco. org/pics/publications/ru/files/3214738.pdf (дата звернення: 09.05.2024).
54. Про затвердження плану заходів на 2017-2029 роки із запровадження Концепції реалізації державної політики у сфері реформування загальної середньої освіти “Нова українська школа”: Розпорядження Кабінету Міністрів України від 13.12.2017 №903-р. URL: https://zakon.rada.gov.ua/laws/show/903-2017-%D1 %80#Text (дата звернення: 09.05.2024).
55. Свінченко І.А., Використання хмарних сервісів в управлінні ЗНЗ. *Управління школою.* 2016. № 4 6 (484-486) С.74–79.
56. Семеніхіна О.В., Юрченко А.О., Сбруєва А. А. та ін. Відкриті цифрові освітні ресурси в галузі ІТ: Кількісний аналіз. *Інформаційні технології і засоби навчання.* 2020. Том 75, №1. С. 331–348.
57. Сорочан Т.М. Підготовка керівників шкіл до управлінської діяльності: теорія і практика: Монографія. Луганськ: Знання, 2005. 384 с.
58. Технології захисту інформації : навчальний посібник С.Е. Остапов, С.П. Євсеєв, О.Г. Король. Х. : Вид. ХНЕУ. 2013. 476 с.
59. Цифрова адженда України – 2020: веб-сайт. URL: http://uk.compu.wikia.com/wiki/ (дата звернення: 14.05.2024).
60. Шиман О.І. Використання сучасних інформаційних технологій. Навчальний посібник. 2-ге вид., допов. і переробл. Запоріжжя. «Просфіта». 2012. 238 с.
61. Шишкіна М.П., Татауров В.П. Формування інформаційно-комунікаційної компетентності майбутніх вчителів початкових класів у вищому навчальному закладі. Збірник наукових праць. 2011. №8. С.304–310.
62. Юрків В. Як навчитися «фільтрувати» інформацію ЗМІ. *Урядовий кур’єр.* 2012. № 170 (4814). С. 10–12.

КІБЕРБЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ
Методичні рекомендації

Здано в набір 07.06.2024 р.
Підписано до друку __ _____ 2024 р.
Формат 60х84/16
Гарнітура Times New Roman

НВВ КЗ Сумський обласний інститут післядипломної педагогічної освіти
м. Суми, вул. Римського-Корсакова, 5.
Тел.: (0542) 33-40-67