**Тетяна Шевченко**

**(Суми, Україна)**

**ІНФОРМАЦІЙНА БЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ**

**Аналіз актуальних досліджень.** Питання інформаційної безпеки в сфері освіти почали привертати увагу педагогів у другій половині ХХ століття, коли збільшився об’єм та способи постачання інформації до людини, полегшився доступ до різних інформаційних джерел, а також збільшився інтерес до застосування ІКТ в освітньому процесі.

Аналіз закордонних та вітчизняних літературних джерел з питань інформаційної безпеки дозволяє стверджувати, що вчені вважають її складовою інформаційної культури особистості (І. Теплицький, С. Семеріков та ін.). Питання формування інформаційної культури вчителя висвітлено в працях В. Бикова, О. Данильчука, М. Жалдака, А. Коломієць, Л. Гаврілової та ін. [1; 4].

Серед українських учених значну увагу питанням інформаційної безпеки приділяють такі вчені, як Р. Калюжний, Г. Почепцов, Б. Кормич, П. Жарков. Іноземні публікації представлені такими авторами як І. Панарів, А. Тер-Акопов, В. Ярчкин та ін.

**Метою даної статті**

Термін «інформаційна безпека» вперше з’явився наприкінці 80-х років у праці німецького вченого Г. Одермана, який виокремив важливість інформаційного компонента у міжнародній безпеці та зробив спробу системно розглянути проблеми безпеки, які пов’язані з інформаційними загрозами. А у вітчизняній та зарубіжній пресі, починаючи з кінця 1991 - початку 1992 року, спостерігається тенденція до активного обговорення проблем інформаційної безпеки як окремого наукового і практичного завдання[5].

Інформаційна безпека є невід’ємною частиною загальної проблеми інформаційного забезпечення людини, соціальної групи, держави і суспільства в цілому. Вона спрямована на захист суб’єктів інформаційних ресурсів.

Умежах цього методологічного напряму використовується визначення інформаційної безпеки як стану, тенденцій розвитку, умов життєдіяльності соціуму, його структури, інститутів та установ, за яких забезпечується збереження якісної інформації з об’єктивно обумовленими інноваціями в ній, вільне і відповідне власній природі її функціонування.

Кібербезпека освітнього закладу передбачає комплекс заходів різного характеру, а саме: 1) захист персональних даних та інформаційного простору від несанкціонованих втручань, розкрадання інформації і зміни конфігурації системи з боку третіх осіб; 2) захист здобувачів освіти від будь-яких видів пропаганди, реклами, забороненої законом інформації тощо.

До обов’язків осіб, відповідальних за кібербезпеку, входить забезпечення безпеки даних, що захищаються, та конфіденційності відомостей, які підлягають захисту, запобігання доступу до них із боку третіх осіб; підтримка інформації у стані постійної доступності для авторизованих осіб.

Специфікою забезпечення кібербезпеки в інформаційних установах є склад характерних загроз. До них належить не лише можливість розкрадання чи пошкодження даних хакерами, а й діяльність учнів. Підлітки можуть свідомо чи ненавмисно пошкодити обладнання, чи заразити систему шкідливими програмами.

Визначають такі види кіберзагроз:

* *загрози для особистісної безпеки*: загроза ознайомлення з матеріалами небажаного змісту (порнографія, ненормативна лексика, публікації суїцидального характеру, сектантські, расистські та ненависницькі матеріали, щодо створення вибухових речовин, хакерські сайти); загроза отримання недостовірної інформації; Інтернет-залежність; загроза спілкування з небезпечними людьми (шахраями, збоченцями, гриферами тощо); загрози вчинення протиправних дій (хакерство, порушення авторських прав тощо);
* *загрози витоку персональної інформації*: загроза розголошення персональних і корпоративних даних (прізвища, імені, адреси, номерибанківських карток, телефонів тощо).
* *загрози для персональних комп’ютерів*: загроза комп’ютерних вірусів; загроза завантаження шкідливого активного коду тощо.

Сучасні технології кібербезпеки освітнього процесу передбачають забезпечення захисту на 5-ти рівнях: нормативно-правовий;морально-етичний; адміністративно-організаційний; фізичний і технічний.

Проведено класифікацію найпоширеніших кіберзагроз у секторі освіти. З’ясовано, що людський фактор, тобто помилки співробітників або учнів внаслідок необізнаності або зневажання елементарними правилами кібергігієни лежать в основі більшості успішно реалізованих кібератак. Дослідження ознак кіберзагроз у галузі освіти надав можливість розділили їх за дев’ятьма критеріями: загрози на пристрої IoT (система взаємопов’язаних комп’ютерних пристроїв, які наділені унікальними ідентифікаторми та здатні передавати дані через мережу без вимоги взаємодії між людьми та комп’ютеами), загрози через людський фактор, крадіжка персональних даних, програми-вимагачі або зловмисне програмне забезпечення, фінансова вигода, шпигунство, фішинг, DDoS-атаки (атаки на відмову в обслуговуванні та спрямовані на веб-сайти й сервери та здійснюються для того, щоб порушити роботу мережевих служб, загрози на CMS (кібератаки на веб-сайти) [3].

Для безпечної роботи в кіберпросторі педагогам можна надати наступні рекомендації:

1. Не користуйтесь забороненим и поштовими сервісами (Mail.ru, Yandex) та соціальним мережами (Vkontakte, Одноклассники).

2. Використовуйте антивірусні програми.

3. Користуйтесь надійними паролями, періодично змінюйте їх.

4. Оновлюйте програмне забезпечення.

5. Залучайте батьків до профілактичної роботи з дітьми, проводьте бесіди для батьків щодо проблем кіберзагроз та засобів їх упередження.

6. Використовуйте систему превентивних заходів для вирішення проблеми кіберзахисту в шкільному середовищі.

7. Використовувати активні та інтерактивні форми роботи, такі як: перегляд кінострічок, роликів на тему кібербезпеки, обговорення переглянутого, моделювання ситуацій, які схожі на ті, які реально відбуваються, та пошуки виходу з них.

8. Проводити діагностику стану психологічного клімату класу, виявляти дітей, які зазнавали віртуального цькування або можуть піддаватися кібербулінгу [6].

Батькам потрібно починати говорити з дітьми про кібербезпеку з того моменту, коли ви даєте дитині в руки телефон, планшет, ноутбук. Вік дитини може бути різним: одні діти починають користуватися сучасними гаджетами в 3-4 роки, інші перед початком навчання в школі. Особливу увагу слід звертати на дітей підліткового віку, саме вони є особливо уразливою категорією для кіберзлочинців.

Дуже важливо навчати дітей основним правилам безпечного користування гаджетами. У своєму віці вони ще не знають, як безпечно користуватися мережею Інтернет. Тому діти мають розуміти, як себе захистити. У цьому їм повинні постійно і систематично допомагати як батьки, так і вчителі.

Постійно з’являються нові рішення у відповідь на кібератаки, весь час зростає поінформованість учасників освітнього процесу. Саме пильність і систематичне використання рекомендацій для педагогів, батьків і учнів може бути потужним ресурсом для виявлення та пом’якшення кіберзагроз, що виникають.

**Висновки.** Лише системний розгляд вказаних підходів до визначення поняття інформаційна безпека дає можливість зрозуміти це явище комплексно. Крім того, ми вважаємо, що інформаційна безпека не може розглядатися лише як окремий стан. Вона є властивістю та атрибутом інформаційного суспільства, діяльністю та результатом діяльності людини, яка спрямована на забезпечення безпеки в інформаційній сфері.

Інформаційна безпека, на нашу думку, є водночас і станом, і процесом, оскільки вона має забезпечувати майбутнє суб’єктів і об’єктів, що потрапляють під ті чи інші інформаційні впливи. Тому інформаційну безпеку розглядають через єдність таких ознак, як стан, властивість управління загрозами і небезпеками. Через ці ознаки забезпечується обрання оптимального шляху їх усунення та мінімізації впливу негативних наслідків, зокрема у сфері інформаційної діяльності держави.

Отже, одним із шляхів розв’язання проблеми кібербезпеки освітнього середовища є проведення для педагогів та працівників закладів освіти вебінарів, тренінгів, лекцій, онлайн-конференцій, воркшопів, майстер-класів із цифрової компетентності.

**Література:**

1. Гаврілова Л., Топольник Я. Цифрова культура, цифрова грамотність, цифрова компетентність як сучасні освітні феномени. Інформаційні технології і засоби навчання2017. – №61(5). – С. 1-14.
2. Доценко С. О., Ворожбіт-Горбатюк, В. В. Собченко Т. М. Онлайн-безпека учасників освітнього процесу в умовах дистанційного і змішаного навчання : навч.-метод. посіб. /Доценко С. О., Ворожбіт-Горбатюк, В. В. Собченко Т. М.– Харків : Вид-во «Ранок». 2021. – 192 с.
3. Закон України «Про основні засади забезпечення кібербезпеки України. Відомості Верховної Ради (ВВР). 2017. – № 45. ст.403
4. Коломієць А. Інформаційна культура вчителя початкових класів: рівні, критерії, показники. Педагогічні науки /Коломієць А. – 2007. – Вип. 45. – С. 279-285.
5. Рижук ОАналіз концепцій визначення «інформаційної безпеки» в умовах глобалізації // Український науковий журналосвіта регіону політологія психологія комунікації.
6. Черних О. Кібербезпека учасників освітнього процесу в умовах воєнного стану. /О.Черних // Інформаційний, науково-методичний журнал «Освіта Сумщини». –№1 (57). –2023.– С. 22-24.