масової інформації, а саме інтернет-реклами. Інтернет-реклама стала одним із основних джерел інформації, що формує внутрішній світ людини. А ще більшого впливає на розвиток дітей, а саме особистості дитини та її здоров‘я, особливо у період карантину із обмеженим колом спілкування та пізнання нового. Але зазначимо, що реклама має і досить таки сприятливий вплив, адже за допомогою реклами у дитини не тільки розвиваються пізнавальні процеси, ще відбувається й формування емпатії; спонуки до конкретних дій. Але можна наголосити, що дане питання знаходиться на початковому етапі вивчення, адже проблема карантину і розвитку дітей під час карантину лише з'явилась у нашому житті.

Список використаних джерел:

1. Діти і соціум: Особливості соціалізації дітей дошкільного та молодшого шкільного віку: Монографія /А.М. Богуш, Л.О. Варяниця, Н.В. Гавриш і ін. заг. ред. Н.В. Гавриш. – Луганськ: Альма-матер, 2006. – 368 с.
2. Гуревич Р.С., Кадемія М.Ю. Інформаційно – телекомунікаційні технології в навчальному процесі та наукових дослідженнях: навч. посібник для студентів педагогічних ВНЗ і слухачів інститутів післядипломної освіти – К.: «Освіта України». – 2006. – 390 с.
3. МаксименкоС.Д..Загальна психологія.3-є видання. Перероблене та доповнене. Навчальний посібник.– К.:«Центр учбової літератури»,2008.
4 .БолтівецьС.І.Теоретико-методичніоснови психо-гігієнічного виховання молоді [Текст] // Практична психологія та соціальна робота: науково-практичний освітньо-методичний журнал. - 2009. - N 9. -С.60-63.

КІБЕРБЕЗПЕКА В ОСВІТНІЙ ДІЯЛЬНОСТІ

Лидзар О. М.
м. Полтава

Анотація. У статті розглянуто проблеми кібербезпеки учасників освітнього процесу, акцентується увага на тому, що ці проблеми не зводяться лише до технічних аспектів захисту інформаційних ресурсів, у повному обсязі вони мають охоплювати такі види захисту, як правові, технічні, інформаційні, організаційні та психологічні, оскільки в останні роки населення в цілому та особливо діти й молодь усе частіше стають об'єктами кібератак, найбільш уразливою (слабкою) ланкою мережі.

Ключові слова: кібербезпека, кіберзагроза, кібератака, цифрове середовище, навчальна діяльність.

Питання кібербезпеки гостро стоять з того часу, як комп’ютерна техніка перестала бути лише прерогативою великих наукових центрів. З появою та поширенням локальних і глобальних мереж змінилося розуміння кібербезпеки, відповідних трендів, проблем і задач. Розвиток цифрового інформаційного суспільства все більше набуває динамічності. Швидкість розповсюдження інформації потребує постійного, пильного контролю, адже в сучасному світі з’явилось безліч нових загроз, таких як дезінформація, маніпуляція, пропаганда, фейкові новини, вірусні атаки що заполонили цифрову площину. Отже, інфосфера стає дедалі більш вразливою щодо стороннього кібернетичного впливу. Тому цілком природною є необхідність контролю створення надійної системи кібернетичної безпеки.

Поняття «кібербезпека» пов’язане із захистом цифрової інформації, операційних систем, комп’ютерних мереж, серверів, баз даних, державних і приватних установ від несанкціонованого втручання сторонніх осіб.

В Законі України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) дається 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» [2].

Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та 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 [2].

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційнокомунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

Розглянемо основні кіберзагрози у сфері освіти: порушення конфіденційності, цілісності, доступності інформації, що зберігається у закладах освіти та інших структурах системи освіти (злам баз даних працівників освіти, ІСУО, ЄДЕБО, «Конкурс» тощо; знищення вірусами баз даних); порушення безпеки, сталого, надійного та штатного режиму функціонування внутришкільного та позашкільного документообігу (відсутність або недостовірність цифрових підписів; відсутність системності у документообігу); використання недостовірної, ненаукової інформації або дезінформації з Всесвітнього Павутиння під час підготовки до навчальних занять або під час занять (відсутність критичності до інформації електронної пошти; відсутність критичності до сайтів Всесвітнього Павутиння; відсутність критичності до інформації зі Всесвітнього Павутиння).

У епоху цифрового громадянства проблема кібербезпеки, зокрема в освітній галузі стає вкрай актуальною. Важливими є пошук та використання нових підходів, технологій, інноваційних форм та способів забезпечення інформаційної безпеки в педагогічній діяльності.

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 її особистої безпеки та результатів її діяльності. «Відкриваючись» під час праці в інформаційному середовищі, людина стає не тільки предметом, а об'єктом діяльності інших учасників інформаційного простору. Людська відкритість є результатом цілей діяльності: використовуючи інформацію як інструмент, людина має «доторкнутися» до неї, зв'язатися з нею. У цей момент людина стає відкритою для інформації та вразливою від неї [1].

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.

Наразі доцільно виокремити роль психологічних засобів забезпечення кібербезпеки, оскільки населення в цілому та особливо діти і молодь все частіше стають об'єктами кібератак, найбільш уразливою (слабкою) ланкою мережі.

У людиноцентричних мережах, що становлять постійно зростаючу частку серед загальних мереж, сама мережа набуває нових властивостей, діючи як самостійний фактор (на додаток до таких факторів, як вузол мережі, інтерфейс і зв'язкиміж вузлами).

Загрози учасникам навчально-виховного процесу з боку кіберпростору доцільно розглядати як пасивні та активні, розробляючи адекватні засоби захисту та життєстійкості системи «суб'єкт освітнього процесу-засоби навчання-середовище» [3].

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

Отже, складником підготовки учасників навчально-виховного процесу з питань кібербезпеки пропонується використовувати «кібер-вакцинацію», тобто формування усвідомленого відчуттєвого досвіду перебування під дією кіберзагрози та протидії їй як систему тренувальних заходів, які включають, крім традиційних методів, тренувальні «кібератаки», а також формування знань і вмінь стійкості (відновлення) стосовно кіберзагроз.

Зараз доцільно зосередитись на детальному вивченні структури кіберзагроз учасниками освітнього процесу, а також методам протидії. Особливе місце має зайняти проблематика стійкості до кібер-небезпек, яка може використовувати досвід підготовки операторів емерджентних галузей, насамперед, діагностування поточного стану людини та необхідне коригування з метою оптимізації її діяльності.

Список використаних джерел:

1. O. Ju. Burov, «Educational Networking: Human View to Cyber Defense», *Information Technologies and Learning Tools*, 52, 144—156, 2016.
2. Закон № 2163-VIII «Про основні засади забезпечення кібербезпеки України» (Відомості ВерховноїРади), № 45, с. 403, 2017.
3. В. Ю. Биков. «Теоретико-методологічні засади створення і розвитку сучасних засобів та е-технологій навчання». *Розвиток педагогічної і психологічної наук в Україні 1992 – 2002*. Збірник наукових праць до 10–річчя АПН України . Академія педагогічних наук України. Частина 2. Харків: «ОВС», 2002. С. 182-199.

ВИКОРИСТАННЯ БЕЗПЕЧНИХ ТЕХНОЛОГІЙ У ПРОЦЕСІ ВИГОТОВЛЕННЯ УЧНЯМИ ДИНАМІЧНИХ ІГРАШОК

Мамчур А. М.
м. Полтава

Анотація. У статті аналізуються особливості використання безпечних технологій у процесі виготовлення учнями динамічних іграшок. Розглянуто специфіку дотримання вимог безпеки праці санітарно-гігієнічних вимог при виготовлення динамічних іграшок.

Ключові слова: трудове навчання, технічна творчість, санітарно-гігієнічні вимоги, динамічна іграшка, правила техніки безпеки.

Майбутні учителі трудового навчання опановують ряд навчальних дисциплін, необхідний для якісного викладання трудового навчання у школі. Вивчення навчальної дисципліни «Прикладна і технічна творчість» спрямоване на ознайомлення, зокрема, і з технологіями виготовлення динамічних іграшок.

Зупинимось детальніше на технології виготовлення рухомої іграшки на нитковій тязі Деталі іграшок рухаються завдяки простому механізму – важелю. Важіль – це предмет (або деталь пристрою), що може обертатися навколо нерухомої точки опори й служить для піднімання й підважування вантажу або для переміщення частин пристрою.

Іграшки-танцюристи виготовляються з тонкої фанери або цупкого картону. Всі деталі цих іграшок плоскі, а з'єднання рухливі (болт з гайкою, заклепка з мідного дроту, міцна нитка).

Технологія виготовлення будь-якого персонажа-танцюриста однакова. Спочатку всі малюнки окремих деталей переносять на матеріал і вирізають або випилюють по контуру. Якщо іграшку виконують з фанери, то після випилювання краю кожної деталі ретельно зачищають. У зазначених на малюнку місцях проколюють шилом отвори і збирають кожну