Пінчук О.П.,
кандидат педагогічних наук, старший науковий співробітник,
заступник директора з науково-дослідної роботи,
Інститут інформаційних технологій і засобів навчання НАПН України,
м. Київ, Україна
Буров О.Ю.,
доктор технічних наук, старший дослідник,
провідний науковий співробітник відділу технологій відкритого навчального середовища,
Інститут інформаційних технологій і засобів навчання НАПН України,
м. Київ, Україна

КІБЕРБЕЗПЕКА УЧАСНИКІВ НАВЧАЛЬНОГО ПРОЦЕСУ І ДИСТАНЦІЙНЕ НАВЧАННЯ

Постановка проблеми. Закономірний, проте поступовий, перехід до більш широкого використання інформаційно-комунікаційних технологій (ІКТ) в цілому і дистанційного навчання, зокрема, значно прискорився внаслідок непередбачено швидкого зростання ролі цифровізації усіх сфер життя, у тому числі освіти [1]. Як наслідок, прискорилась трансформація навчального середовища [2] та усіх аспектів освітнього процесу, також, посилилась гетерохронність розвитку інтелектуальних і особистісних якостей учнів [3] як результат системної дії освіти [4]. Усі світові експерти відмічають стрімке зростання кіберзлочинності під час пандемії [5] і необхідність звернути увагу на кібербезпеку освітнього процесу, насамперед, при дистанційній формі [6].

Аналіз актуальних досліджень. Основними рисами освіти в цифровому навчальному середовищі станом на 2020 рік є наступні:

- Збільшилась питома вага цифровізації усіх сфер життя людини, водночас тенденції глобалізації біо-соціальної та матеріальної взаємодії людей уповільнилися.
- Суспільство вимагає нових принципів і засобів, критеріїв оцінювання результативності навчання/підготовки працівника в інформаційну еру (Всесвітній економічний форум в Давосі, 2020 р.).
- Прискорилось зміщення фокусу від поняття «інтеграція мереж» до «інтегрована людино-центрична мережа», зокрема у галузі освіти.
- Зростає необхідність захисту інтелектуального капіталу країни від несприятливих факторів дії мережі [7].

Під час пандемії людей вдалось частково захистити від хвороби шляхом самоізоляції та переходу до дистанційного режиму праці та навчання. Проте за даними компанії *PurpleSec LLC,* що спеціалізується на захисті кіберпростору, кіберзлочинність зросла на 600% (2020 Cyber Security Statistics. The Ultimate List Of Stats, Data & Trends. PurpleSec LLC. https://purplesec.us/resources/cyber-security-statistics). Основними рисами нової тенденції є:

- Зловмисне програмне забезпечення (*malware*): 92% потрапляє через email.
- Програми-шантажисти (*ransomware*): кількість атак зросла на 72%.
- Соціальна інженерія (*social engineering*): 98% усіх кібератак.

87% учасників освітнього процесу зіштовхувались із результативними кібератаками!

Мета статті. Визначити основні чинники середовища дистанційного навчання, що впливають на кібербезпеку його учасників.

Виклад основного матеріалу.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає кіберпростір 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». Через періодичне посилення карантину саме в кіберпростір наразі перенесено навчання як реальної можливості учням неперервно отримувати освіту, здобувати знання. Кіберпростір можна представити тріадою, до якої входять:

1) *інформація* у своєму цифровому представленні: *статична* (файли на носії інформації) та *динамічна* (пакети, потоки, команди, запити тощо);

2) *технічна інфраструктура*: ІКТ, програмне забезпечення, бази даних і бази знань;

3) *інформаційна взаємодія* суб'єктів з використанням отриманої (переданої) інформації та обробки через технічну інфраструктуру.

Діти народжуються, зростають, навчаються та будуть працювати з цифровими пристроями, об'єднаними комп'ютерними\ІК мережами як природним для них середовищем. Їхнє життя зазнає впливу цифрового простору зі старими та новими ризиками/небезпеками, дія яких: 1) все більше впливає на когнітивну сферу та моделі поведінки (інтерфейс, зміст тощо); 2) пов'язана з безпекою, ефективністю та якістю життя.

Серед різних підходів до типологізації загроз, що надходять з інформаційно-комунікаційних мереж, слід виділити такі, що впливають на навчання: активні та пасивні, відкриті та приховані, поточні та відкладені. Серед рівнів можливого захисту від кіберзагроз доцільно визначити такі: правовий, технічний, інформаційний, організаційний, психологічний. Серед шляхів захисту слід приділяти більшу увагу організаційним підходам, що базуються на результатах дослідження профільних компаній у кіберпросторі. Наприклад, за даними доповіді Fidelis Threat Intelligence Team, лідера у США із пошуку та блокуванню кібер-небезпек, у щомісячному моніторинговому звіті за вересень 2020 р. застерігає від

використання Internet Explorer, особливо версій старших за IE11, а також Adobe Flash, що часто використовуються у навчальному процесі [8]. У цілому ж серед можливостей і шляхів забезпечення кібербезпеки навчального процесу можна виділити наступні [7]:

1. *Соціальна інженерія* (методи та технології отримання необхідного доступу до інформації, засновані на особливостях психології людей) – фішинг, троянський кінь, байтинг, *Qui pro quo* та ін.
2. *Безпечний Інтернет* (поінформованість, культура безпеки та ін).
3. *Кібергігієна* (заходи, направлені на захист приватної інформації на цифрових пристроях).
4. *"Когнітивна вакцинація"* **(**критичне мислення, безпечне та відповідальне використання Інтернету, тренування усіх учасників мережної діяльності щодо можливого впливу кібер-середовища, комп'ютерне моделювання кібер-загроз, навчання "кібер-виживанню").

Слід додати, що перехід до дистанційного навчання супроводжується також посиленням ролі мас-медіа, у яких можуть використовуватися методи соціальної інженерії. Відповідно, їх доцільно вважати складником цифрового навчального середовища з певною специфікою взаємодії з ним користувача.

Висновки та перспективи подальших досліджень

1. Проблеми кібербезпеки не зводяться лише до технічних методів захисту кіберпростору і мають включати такі види захисту: правові, технічні, інформаційні, організаційні та психологічні.
2. 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. Як складником підготовки учасників навчально-виховного процесу з питань кібербезпеки пропонується використовувати "кібер-вакцинацію",

тобто формування усвідомленого відчуттєвого досвіду перебування під дією кібер-загрози та протидії їй.

Список використаних джерел та літератури

1. Policy brief: education during COVID-19 and beyond. August 2020. United Nations. Available at https://cutt.ly/TgvIN67. Accessed 09.09.20.
2. Pinchuk O. P. et al. Digital transformation of learning environment: aspect of cognitive activity of students. *Proceedings of the 6th Workshop on Cloud Technologies in Education (CTE 2018), Kryvyi Rih, Ukraine, December 21, 2018. – CEUR Workshop Proceedings*, 2019. №. 2433. С. 90-101.
3. Буров О. Ю. та ін. Динаміка розвитку інтелектуальних здібностей обдарованої особистості у підлітковому віці / За ред. О. Ю. Бурова. К. : ТОВ «Інформаційні системи», 2012. 258 с.
4. Pinchuk O., Burov O., Lytvynova S. Learning as a Systemic Activity // Karwowski W., Ahram T., Nazir S. (eds) Advances in Human Factors in Training, Education, and Learning Sciences. AHFE 2019. Advances in Intelligent Systems and Computing. 2019. Vol 963. Pp. 335--342. Springer, Cham.
5. Pipikaite A., and Davis N. Why cybersecurity matters more than ever during the coronavirus pandemic. World Economic Forum. Access: https://cutt.ly/GgvI62D.
6. Pierce D. Here's why cyber security experts are concerned about remote learning. *eSchool News*. Available at https://cutt.ly/GgvI62D Accessed 13.10.20.
7. V. Yu. Bykov, O. Yu Burov, and N. P. Dementievska. "Cybersecurity in digital educational environment", Inf. Technol. Learn. Tools, 2 (70), 313-331. https://doi.org/10.33407/itlt.v70i2.2876, 2019
8. Fidelis Threat Intelligence Report – September 2020. Research Report. https://fidelissecurity.com/resource/report/fidelis-threat-intelligence-report-september-2020/ Accessed 13.10.2020