ЦИФРОВА ОСВІТА: ТЕНДЕНЦІЇ ТА КІБЕРЗАГРОЗИ

Буров О.Ю.,
доктор технічних наук, старший дослідник
провідний науковий співробітник НДІ інтелектуальної власності,
провідний науковий співробітник ІІТЗН НАПН України

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, зріс рівень вимог до безпеки навчального середовища та усіх аспектів освітнього процесу [2], також, посилилась гетерохронність розвитку інтелектуальних і особистісних якостей учнів [3] під впливом впровадження в практику нових технологій та інновацій [4]. Усі світові експерти відмічають стрімке зростання кіберзлочинності під час пандемії [5] і необхідність звернути увагу на кібербезпеку освітнього процесу, особливо у дистанційній формі [6].

Основними рисами освіти в цифровому навчальному середовищі є такі:

• 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 (за даними Всесвітнього економічного форуму в Давосі, 2020 р.).

• Прискорилось зміщення фокусу \зміна акценту 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 [8].

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...». 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 та динамічна;*

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

3) *інформаційна взаємодія суб'єктів.*

Діти народжуються, зростають, навчаються та будуть працювати з цифровими пристроями, об'єднаними комп'ютерними мережами як природним для них середовищем. Їхнє життя зазнає впливу цифрового простору зі старими та новими ризиками/небезпеками, дія яких:

- все більше впливає на когнітивну сферу та моделі поведінки (інтерфейс, зміст, …)
- 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 Pulse 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, які часто використовуються у навчальному процесі [9].

У цілому ж серед можливостей і шляхів забезпечення кібербезпеки навчального процесу можна виділити такі [7]:

1. *Соціальна інженерія* (методи та технології отримання необхідного доступу до інформації, засновані на особливостях психології людей) – фішинг, троянський кінь, байтинг, Qui pro quo …

2. *Безпечний Інтернет* (поінформованість, культура безпеки, …).

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 зростанням можливостей створення адаптивних систем навчання з урахуванням індивідуальних особливостей учнів [10].

Висновки

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:

1. Buroy, O., Bykoy, V., & Lytvynova, S. ICT Evolution: from Single Computational Tasks to Modeling of Life. In O. Sokoloy, O. Zholtkevych, V. Yakovyna, Yu. Tarasich, ... H. Kraytsoy (Eds.), Proceedings of the 16th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Volume II: Workshops. CEUR Workshop Proceedings, 2732. - 2020. - 538-590. http://ceur-ws.org/Vol-2732/20200583.pdf.

2. Кузнецов В. О. та ін. Концепція освіти з напряму "Безпека життя і діяльності людини". Інформаційний вісник «Вища освіта». – К.: Видавництво науково-методичного центру вищої освіти МОНУ. – 2001. – №. 6. – С. 6-18.

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. Буров О.Ю. Технології й інновації в діяльності людини ери інформації: інформація і технології. Інформаційні технології і засоби навчання.- 2015,- 49 (5). - 16-25.

5. Pipikaite A., and Dayis N. Why cybersecurity matters more than eyer during the coronayirus pandemic. World Economic Forum. https://www.weforum.org/agenda/2020/03/coronayirus-pandemic-cybersecurity. 2020.

6. Pierce D. Here's why cyber security experts are concerned about remote learning. eSchool News. https://www.eschoolnews.com/2020/07/16/heres-why-cyber-security-experts-are-concerned-about-remote-learning/ Accessed 5.10.2021.

7. Bykoy V. Yu., Buroy O. Yu., Derenlievska N. P. Cybersecurity in digital educational enyironment. Inf. Technol. Learn. Tools, 2019. - 2 (70).- 313-331.

8. Buroy O. et al. Cybersecurity in educational networks. International Conference on Intelligent Human Systems Integration. – Springer, Cham, 2020. – Pp. 359-364.

9. Fidelis Threat Intelligence Report – September 2021. Research Report. https://fidelissecurity.com/resource/report/fidelis-threat-intelligence-report-september-2020/ Accessed 5.10.2021.

10. Buroy O.Y., Pinchuk O.P., Pertsey M.A., Vasylchenko Y.V. Using the Students' State Indices For Design of Adaptiye Learning Systems. - Інформаційні технології і засоби навчання. 2018. - 68 (6). - 220-32.