

НАЦИОНАЛНА СИГУРНОСТ

КИБЕРГРАМОТНОСТ В ЕПОХАТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ: ОБРАЗОВАНИЕТО КАТО ПЪРВА ЛИНИЯ НА ДИГИТАЛНА ЗАЩИТА

ПРОФ. Д-Р ИЛИН САВОВ, Д.Н.

МЕЖДУНАРОДЕН ЕКСПЕРТ ПО КИБЕРСИГУРНОСТ И КИБЕРПРЕВЕНЦИЯ

Резюме: В статията се анализират комуникативните особености на киберобученията в съвременната образователна среда в България, с акцент върху нарастващото използване на изкуствен интелект от ученици и учители. Статията разглежда комуникационните дефицити, поведенческите модели и рисковете от некритично използване на изкуствения интелект, като формулира стратегически препоръки за изграждане на устойчива дигитална култура в условията на дигитална трансформация.



Ключови думи: киберобучения, киберсигурност, изкуствен интелект, дигитална грамотност, образование

CYBERLITERACY IN THE AGE OF ARTIFICIAL INTELLIGENCE: EDUCATION AS THE FIRST LINE OF DIGITAL DEFENSE

PROF. DR. ILIN SAVOV, PHD

INTERNATIONAL EXPERT IN CYBERSECURITY AND CYBER PREVENTION

Abstract: The article analyzes the communicative features of cyberlearning in the modern educational environment in Bulgaria, with an emphasis on the increasing use of artificial intelligence by students and teachers. The article examines communication deficits, behavioral patterns and risks of

uncritical use of artificial intelligence, formulating strategic recommendations for building a sustainable digital culture in the context of digital transformation.

Keywords: cyberlearning, cybersecurity, artificial intelligence, digital literacy, education

УВОД

Дигиталната трансформация на образованието изправя институциите пред предизвикателства, които надхвърлят технологичната рамка. Изкуственият интелект, социалните мрежи и онлайн комуникацията променят не само начина на учене, но и механизмите за влияние, манипулация и социализация.

В този контекст образованието се превръща в критичен фактор за националната и личната сигурност. Какви са рисковете? Липсата на адекватна подготовка в областта на дигиталната грамот-

ност създава условия за уязвимост на ученици и учители спрямо дезинформация, киберпрестъпления и онлайн манипулации.

Образователната система все по-често изостава от реалната дигитална среда, в която младите хора функционират ежедневно. Това разминаване между формалното обучение и реалните дигитални практики поражда дефицити в критичното мислене и в способността за самостоятелна оценка на информацията. В резултат се формират рискови поведенчески модели, които се пренасят от виртуалната в реалната среда. Именно поради

това образованието следва да поеме активна роля в изграждането на устойчиви дигитални компетентности и ценности, насочени към сигурност, отговорност и осъзнато използване на технологиите.

ТЕОРЕТИЧНА РАМКА И ОСНОВНИ ПОНЯТИЯ

Киберсигурността в образованието включва не само технически знания, но и комуникационни, етични и поведенчески компетентности. Дигиталната грамотност се разглежда като способност за критична оценка на информацията, разбиране на рисковете и осъзнато онлайн поведение.

В този смисъл тя представлява ключов компонент на съвременното гражданско образование и на подготовката за активно участие в дигиталното общество. Липсата на подобни компетентности води до повишена уязвимост спрямо манипулации, дезинформация и социално инженерство. На всичко това ставаме свидетели в Република България през последните няколко години.

Образователната среда има потенциала да формира устойчиви нагласи за сигурност чрез системно и целенасочено обучение, съобразено с възрастовите и когнитивните особености на обучаемите. Особено значение има интегрирането на етични принципи при използването на дигитални технологии и изкуствен интелект, които влияят пряко върху ценностната система на учениците. Развиването на отговорно дигитално поведение не следва да се разглежда като допълваща дейност, а като неразделна част от образователния процес. В този контекст киберсигурността се утвърждава като интердисциплинарна област, обединяваща технологии, комуникация, психология и образование.

Изследването използва качествени методи като автоетнографско и киберетнографско наблюдение, външно наблюдение и анализ на повтарящи се поведенчески модели. Данните са събрани в реална образователна среда чрез обучения на ученици и учители. Прилагането на автоетнографския подход позволява задълбочен анализ на процесите от гледна точка на пряк участник и наблюдател. Киберетнографското наблюдение дава възможност за проследяване на комуникационните практики и моделите на поведение в онлайн среда. Чрез външното наблюдение се осигурява по-обективна перспектива върху взаимодействията между участниците в обучителния процес.

Анализът на повтарящите се поведенчески модели спомага за идентифициране на устойчиви тенденции и рискови практики при използването на дигитални технологии. Комбинирането на различните методи гарантира по-висока валидност и надеждност на резултатите. Методологичният подход е съобразен със сложния и динамичен характер на дигиталната образователна среда.

КОМУНИКАЦИОННА ТРАНСФОРМАЦИЯ И ДОВЕРИЕ В КИБЕРОБРАЗОВАТЕЛНАТА СРЕДА

Качествените киберобучения могат да трансформират традиционната образователна комуникация в мрежов модел, при който учителят функционира като модератор и доверен експерт. Емпиричните наблюдения, които съм извършил при обучаването на над 16 500 деца и над 5600 учители в страната показват сериозни дефицити в разпознаването на манипулации и дезинформация.

В условията на дигитална среда авторитетът на учителя вече не се основава единствено на институционалната му роля, а на способността му да изгражда доверие чрез компетентна и последователна комуникация в реална и дигитална среда. Учениците все по-често черпят информация от паралелни източници с неясна достоверност, което създава конкуренция за внимание и влияние. Липсата на целенасочена комуникационна стратегия в киберобученията води до фрагментиране на знанията и затруднена ориентация в информационния поток. Това увеличава риска от некритично възприемане на съдържание и податливост към онлайн манипулации. Ефективната комуникация в киберобученията изисква развитие на умения за интерпретация, аргументация и управление на вниманието.

В този контекст комуникацията се утвърждава като ключов инструмент за превенция на киберрисковете и за формиране на устойчива дигитална култура.

ИЗКУСТВЕНИЯТ ИНТЕЛЕКТ МЕЖДУ ОБРАЗОВАТЕЛЕН ИНСТРУМЕНТ И СИСТЕМЕН РИСК НАСОЧЕН КЪМ ВСИЧКИ ВЪЗРАСТОВИ ГРУПИ

Използването на изкуствен интелект в образованието създава предпоставки за автоматизиране на мисловни процеси и зависимост от алгоритми. Липсата на ясни стандарти увеличава риска

от злоупотреби и когнитивна деградация. Все по-често се наблюдава подмяна на аналитичното мислене с автоматично възпроизвеждане на генерирано съдържание. Това води до повърхностно усвояване на знания и затруднена способност за критична оценка на информацията.

Изкуственият интелект не само подпомага обучението, но и активно моделира нагласите и поведението на обучаемите. При отсъствие на етична рамка и дигитална осведоменост за рисковете от неправомерното му използване, той може да се превърне в инструмент за манипулация и дезинформация. Особено уязвими са учениците, които все още изграждат своята ценностна и когнитивна система. Образователните институции следва да поемат активна роля в регулирането и педагогическото осмисляне на използването на изкуствен интелект. Само чрез ясни правила, критично обучение и експертен контрол ИИ може да бъде превърнат от риск в устойчив образователен ресурс.

ЕФЕКТИВНОСТ, ПРИЛОЖИМОСТ И ИЗМЕРИМИ РЕЗУЛТАТИ ОТ КИБЕРОБУЧЕНИЯТА

Практически ориентираните обучения доказват своята ефективност чрез изграждане на устойчиви дигитални рефлексии, подобряване на критичното мислене и повишаване на личната и институционалната киберустойчивост. Участниците развиват способност за разпознаване на реални киберзаплахи и адекватна реакция в динамична дигитална среда. Обученията допринасят за намаляване на рисковото онлайн поведение и за по-осъзнато използване на дигитални технологии. Особена стойност има прилагането на реални казуси и симулации, които доближават обучаемите до автентични сценарии от практиката. Натрупаните знания се трансформират в дългосрочни умения, приложими както в образователна, така и в професионална среда. Повишаването на индивидуалната дигитална устойчивост води и до укрепване на сигурността на образователните институции като цяло. Резултатите от обученията показват по-високо ниво на увереност и самостоятелност при вземане на решения, свързани с киберсигурността. В този смисъл киберобученията се утвърждават като ефективен и резултатен инструмент за киберпревенция, а не като формално образователно изискване.

ЗАКЛЮЧЕНИЕ

Дигиталната трансформация на образованието и навлизането на изкуствения интелект променят начина, по който се осъществява обучението и професионалната подготовка. Киберобученията вече не могат да бъдат разглеждани единствено като технологично решение, а като комплексен педагогически процес, изискващ ясна визия, методическа последователност и отговорна комуникация. Изграждането на сигурна и ефективна образователна среда предполага интегриране на знания, практически умения и критично мислене, насочени към превенция и управление на рискове в дигиталното пространство.

Особено значение има подготовката на специалисти, които не само да прилагат принципите на киберсигурността в своята професионална дейност, но и да поемат ролята на обучители и ментори. Това открива възможности за развитие на устойчиви обучителни общности, в които сертифицирането и непрекъснатото усъвършенстване са ключови фактори за качество. Практико-приложните обучения, водени от доказани експерти с педагогическа компетентност и стаж в службите за сигурност и МВР, доказват по-висока ефективност при изграждането на реални умения. В този контекст използването на съвременни технологични решения, интерактивни подходи и игрови елементи допринасят за по-висока ангажираност и по-добро усвояване на знанията в киберобученията.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. UNESCO. (2023). Guidance for Generative AI in Education and Research. Paris: UNESCO.
2. European Commission. (2022). Digital Education Action Plan 2021–2027: Resetting education and training for the digital age. Brussels.
3. OECD. (2021). Global Security Risks and Digital Education. Paris: OECD Publishing.
4. ENISA. (2020). Cybersecurity Skills Development in the EU. European Union Agency for Cybersecurity.
5. Buckingham, D. (2015). Defining digital literacy – What do young people need to know about digital media? *Nordic Journal of Digital Literacy*, 10(4), 21–35.
6. Floridi, L. (2019). *The Ethics of Artificial Intelligence*. Oxford: Oxford University Press.
7. Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age. *New Media & Society*, 19(5), 657–670