https://doi.org/10.53656/str2026-2-1-dig

Education in the Information Society
Образованието в информационното общество

ДИГИТАЛНАТА СИГУРНОСТ В УЧИЛИЩЕ КАТО КЛЮЧОВ ФАКТОР В ОБРАЗОВАТЕЛНАТА ПОЛИТИКА

Мирослав Людмилов
Университет за национално и световно стопанство

Резюме. В условията на интензивна дигитализация училищната среда все по-често функционира чрез електронни системи, което превръща дигиталната сигурност в приоритет на образователните политики. Динамичното навлизане на учебно съдържание, генерирано от изкуствен интелект, както и дигитализацията на административните процеси, създават нови предизвикателства пред учителите и администрацията. Изследването анализира дигиталната сигурност отвъд техническите ѝ параметри – като структурен елемент, гарантиращ устойчивостта и общественото доверие в системата. Приложен е политико-аналитичен подход върху стратегически документи от национален и европейски мащаб, комбиниран с PESTEL анализ на технологичните и институционалните рискове. Акцентът е поставен върху „киберхигиената“ и човешкия фактор като фундамент на културата на сигурност. Основната теза е, че липсата на единна секторна политика в тази област генерира дългосрочни рискове, надхвърлящи образованието и засягащи националната сигурност.

Ключови думи: дигитална сигурност; училищно образование; образователна политика, киберхигиена; култура на сигурност; национална сигурност

Увод

През последното десетилетие дигиталната трансформация преобрази из основи образователния сектор, променяйки не само педагогическите подходи, но и самата функционална рамка на училищата. Масовото внедряване на облачни технологии, електронна администрация и инструменти, базирани на изкуствен интелект, предефинира средата, като създава критична необходимост от нови управленски модели за гарантиране на сигурността и институционалната устойчивост. В този контекст дигиталната сигурност все по-ясно се очертава като фактор, който надхвърля техническите измерения и придобива стратегическо значение за формирането и прилагането на образователната политика.

На европейско равнище дигиталната сигурност е дефинирана като неразделна част от обществената и институционалната устойчивост, като образованието се разглежда като ключова сфера за изграждане на култура на сигурност и доверие в цифровата среда. Стратегията на Европейския съюз за киберсигурност за цифровото десетилетие подчертава значението на човешкия фактор, институционалния капацитет и превенцията на рисковете в условията на нарастваща зависимост от цифрови технологии. В същото време, европейските политики в областта на цифровото образование поставят акцент върху необходимостта от по-ефективно и координирано управление на рисковете, свързани с използването на технологии в образователните системи.

В национален контекст българската образователна система се развива в рамките на последователни стратегически документи, които насърчават дигитализацията като инструмент за повишаване на качеството, достъпността и ефективността на обучението. Националната стратегия за киберсигурност и стратегическата рамка за развитие на образованието очертават сходни цели, свързани с устойчивостта на публичните системи, защитата на информационните ресурси и развитието на човешкия капитал. Въпреки това дигиталната сигурност в училище често остава разглеждана фрагментарно – като техническа или административна задача, а не като интегрален елемент на образователната политика.

Подобна фрагментация поражда редица предизвикателства, свързани с управлението на цифровите рискове, защитата на данни, използването на изкуствен интелект в образователния процес и подготовката на учителите и учениците за работа в сигурна цифрова среда. Когато липсва единна стратегия за киберхигиена, последствията надхвърлят чисто оперативните смущения и водят до ерозия на институционалния авторитет на училището. Тук дигиталната сигурност се третира като фундамент на управленските политики, а не като периферен технологичен казус. За да се дефинират рисковете пред дигиталната трансформация, изследването прилага PESTEL методология върху актуалната стратегическа рамка на национално и европейско ниво. Анализът цели да аргументира необходимостта от по-цялостна и последователна политика за дигитална сигурност, ориентирана както към устойчивостта на образователната система, така и към по-широкия контекст на обществената и националната сигурност.

1. Дигиталната сигурност като елемент на образователната политика

В съвременните публични политики дигиталната сигурност все по-често се дефинира не просто като технически параметър, а като хоризонтален приоритет, засягащ устойчивостта на критичните системи. Тази трансформация е нормативно закрепена в чл. 2 на Закона за киберсигурност, който определя киберсигурността като „състояние на обществото и държавата“, а системата

за киберсигурност – като неразделна част от системата за защита на националната сигурност[1]. В този смисъл образователната система се очертава като критична инфраструктура, чиято защита изисква комплексен подход, надхвърлящ инсталирането на софтуерни защити.

От гледна точка на образователната политика дигиталната сигурност следва да се разглежда като управленски процес, който гарантира непрекъсваемост и качество на обучението. Стратегическите документи на национално ниво, като Националната стратегия за киберсигурност, изрично подчертават необходимост от „формиране на изцяло нова култура на киберхигиената“[2]. Това кореспондира с разбирането, че училището не е просто място за трансфер на знания, а среда за изграждане на социални навици и устойчивост.

Тази логика намира своето потвърждение и в други механизми за образователна устойчивост. Пример за това е образователната медиация, която функционира като стратегически инструмент за социална стабилност, базиран на постигането на институционален и правов консенсус (Lyudmilov, 2025). Този принцип на споделена отговорност е напълно валиден и за дигиталната сигурност – тя не може да бъде гарантирана без съгласуваните усилия на всички участници в процеса. Справянето с дигиталните рискове, подобно на управлението на социалните конфликти, изисква култура на превенция и пряко ангажиране на човешкия фактор – учители, ученици и родители. Паралелно с това, европейските регулации диктуват необходимост от трансформация на самите управленски модели.

Съгласно чл. 20 от Директива (ЕС) 2022/2555 управителните органи са пряко задължени да одобряват мерките за управление на риска и да преминават специализирано обучение[3]. Това нормативно изискване предефинира административната функция на директора, превръщайки го в пряк отговорник за киберустойчивостта на организацията. Въпреки тази рамка Националната стратегия за киберсигурност отчита необходимостта от изграждане на „нова култура на киберхигиена“, тъй като липсата на такава създава критични уязвимости за образователните институции.

Пропуските в киберхигиената създават уязвимости, които застрашават дългосрочно доверието в образователната система. Следователно интегрирането на дигиталната сигурност като структурен елемент на образователната политика е наложително условие за гарантиране на онази „базова култура на сигурност“[2], която е необходима за функционирането на модерното училище.

2. PESTEL анализ на дигиталните рискове в училищното образование

Приложението на PESTEL перспектива в анализа на дигиталната сигурност в училищното образование позволява систематично разглеждане на външните фактори, които оказват влияние върху формулирането и прилагането на образователните политики. В условията на ускорена дигитализация и

преход към „високоефективна екосистема за цифрово образование“[4] този аналитичен подход се откроява като методологично обоснован и адекватен. Този подход позволява да се излезе извън рамките на технологичните заплахи и да се анализират в дълбочина политическите, социалните и институционалните контексти, в които оперира училището.

Тази системна перспектива намира опора в утвърдените модели за сигурност в социалните системи. Аналогията с образователната медиация е показателна: както управлението на конфликти изисква разбиране на структурните и културните специфики на средата (Lyudmilov, 2025), така и дигиталната сигурност представлява многопластов процес, зависещ от синергията между публични политики и управленски решения. В този смисъл PESTEL рамката действа като инструмент за сканиране на макросредата, необходим за дефиниране на външните фактори в стратегическото образователно планиране (Karadzhov & Patarchanova, 2025). Този подход осигурява структурирана оценка на рисковете и възможностите, произтичащи от политическите, икономическите, социалните и технологичните динамики. За целите на настоящото изследване стандартната PESTEL рамка е адаптирана, като факторите са групирани в три ключови направления, отразяващи спецификата на българското училище: политически и нормативни; технологични и институционални; и социални измерения.

2.1. Политически и нормативни фактори (Political factors)

Политико-нормативната рамка за дигитална сигурност в България се определя от сложен комплекс от национални и европейски регулации. В основата стои Законът за киберсигурност, който регламентира организацията и управлението на националната система за киберсигурност[1]. Въпреки наличието на нормативна база основният политически риск се крие във фрагментираното прилагане на тези норми в образователния сектор.

На европейско ниво, приемането на Директива (ЕС) 2022/2555 (МИС 2) налага нови, по-строги изисквания за управление на риска и докладване на инциденти, които засягат и публичния сектор, включително образованието[3]. Насоките на Европейската агенция за киберсигурност (ENISA) изрично посочват необходимостта от идентифициране и картографиране на конкретни умения за реакция при инциденти. Тези компетентности следва да бъдат интегрирани и в образователните структури, които попадат под регулацията на директивата (ENISA, 2025).

Основното предизвикателство за българската образователна система обаче се корени в липсата на специализирана секторна политика, която да преведе тези високи стандарти на езика на реалните училищни възможности. Това разминаване генерира своеобразен „нормативен вакуум“: докато законовите отговорности са ясно разписани, конкретните механизми за тяхното практическо изпълнение на терен често отсъстват или остават неясни за училищните ръководства.

2.2. Технологични и институционални фактори (Technological and institutional factors)

Технологичните рискове в образованието не се изчерпват само с външни кибератаки, а са структурно обвързани с нивото на институционален капацитет. Според Националната програма „Цифрова България 2025“ въпреки подобрената свързаност съществуват дисбаланси в широколентовото покритие и достъпа до високоскоростен интернет, което създава риск от „информационна откъснатост“ и ограничен достъп до качествени цифрови образователни ресурси за определени региони[5].

В училищна среда това се проявява чрез зависимост от външни платформи и облачни услуги, чиято сигурност често е извън контрола на училищното ръководство. Липсата на специализирани звена по киберсигурност във всяко училище превръща технологичния дефицит в институционален риск. Както се посочва в Плана за действие в областта на цифровото образование (2021 – 2027), успешната дигитална трансформация изисква не само оборудване, но и ефективно стратегическо планиране и устойчив организационен капацитет, който в момента е неравномерно разпределен[4].

2.3. Социални измерения и човешки фактор (Social factors)

Човешкият фактор се очертава като ключов и системно уязвим елемент в системата за сигурност. Този извод кореспондира с тезите за ролята на социалната среда при управлението на кризи. Както дълбокото разбиране на социалната среда на ученика е от съществено значение за справяне с агресията и конфликтите в училище (Lyudmilov, 2025), така и разбирането на дигиталното поведение е ключово за киберсигурността. Липсата на „киберхигиена“ сред учениците и учителите не е просто технически пропуск, а социален феномен, свързан с ниската базова култура на сигурност.

Националната стратегия за киберсигурност изрично подчертава, че реализирането на политиките изисква „формиране на изцяло нова култура на киберхигиена“[2]. Социалният риск тук е ясно изразен: високата дигитална активност на учениците рядко е съпроводена с умения за критичен анализ на заплахите. Този дефицит на „дигитална зрялост“ ги превръща в системна уязвимост – своеобразна входна точка за компрометиране на сигурността в цялата училищна среда.

3. Киберхигиената и човешкият фактор в контекста на дигиталната сигурност в училище

Гарантирането на дигитална сигурност в училищна среда е невъзможно, ако се разчита единствено на технически решения и формално спазване на нормативите. Макар технологичната инфраструктура да е от значение, европейските регулации, визирайки Директива (ЕС) 2022/2555 (NIS 2), категорично поставят „основните практики за киберхигиена“ (като редовни актуали-

зации и управление на достъпа) в основата на защитата[3]. В образователен контекст обаче киберхигиената надхвърля техническите протоколи и се превръща в поведенчески и културен феномен.

Киберхигиената следва да се дефинира като съвкупност от знания, умения и устойчиви навици, които минимизират рисковете. Националната стратегия за киберсигурност изрично посочва, че реализирането на политиките изисква „формиране на изцяло нова култура на киберхигиена“[2]. В училищния контекст това означава трансформация на индивидуалното поведение на учениците и учителите в колективна организационна култура.

Тук ролята на човешкия фактор е решаваща и изисква прилагането на психо-педагогически подходи. Това предполага включване на киберхигиената в по-широкия спектър на превантивните и възпитателни политики в образованието.

Тук е налице пряка аналогия с инструментите на образователната медиация. Успешното справяне с агресията изисква задълбочен анализ на социалния контекст на ученика – семейна среда и травматичен опит (Lyudmilov, 2025). Този принцип е валиден и за превенцията на киберрисковете, която е невъзможна без разбиране на поведенческите модели на подрастващите в мрежата. Парадоксът е, че макар учениците да демонстрират завидни технически умения, те често страдат от дефицит на „дигитална зрялост“, необходима за идентифициране на заплахи като дезинформация и социално инженерство.

Както отбелязва Европейската комисия в Плана за действие в областта на цифровото образование[4], цифровата грамотност вече е съществена за ежедневието и изисква критично мислене, а не просто способност за работа с устройства.

Педагогическите специалисти са поставени в сложната роля на медиатори между технологиите и учениците. Емпиричните данни потвърждават наличието на дефицит: проучвания сред бъдещи педагози разкриват, че докато те се чувстват уверени в общите си дигитални умения, възприемат себе си като недостатъчно компетентни конкретно в сферата на дигиталната сигурност (Latorre-Medina & Tnibar-Harrus, 2023). Това налага трансформация в стратегиите за квалификация, която да надхвърли базовото ползване на инструменти[6]. Акцентът следва да се премести към ролята на учителя като „овластяващ ментор“, който активно изгражда защитни навици у учениците, съгласно Европейската рамка за дигитална компетентност DigCompEdu (Redecker, 2017).

Развитието на дигитална компетентност у учителите не се изчерпва само с използването на технологиите за преподаване. Съгласно Европейската рамка DigCompEdu ключов елемент е умението на педагозите да „овластяват обучаемите“ (Empowering Learners) и да насърчават отговорната и безопасна употреба на дигиталните технологии от тяхна страна (Redecker, 2017). Това превръща киберсигурността в неразделна част от професионалния

профил на съвременния учител. Емпиричните проучвания разкриват значима диспропорция: макар бъдещите педагози да демонстрират увереност в своите технопедагогически компетенции, те декларират отчетлива необходимост от допълнителна теоретична и практическа подготовка конкретно в сферата на дигиталната сигурност. Тази констатация налага ревизия на квалификационните програми, където акцентът следва да се премести от инструменталните умения към изграждането на капацитет за защита на данните и управление на киберриска.

Ефектът от изграждането на култура на киберхигиена в училище мултиплицира своето въздействие далеч отвъд класната стая. Тъй като училището функционира като обществен „микрокосмос“, формиращ социалните модели на поведение (Lyudmilov, 2025), инвестицията в дигиталната компетентност на ученици и учители придобива стратегическо измерение. Тя следва да се третира не като оперативен разход, а като дългосрочен влог в националната сигурност, изпълнявайки дефиницията за киберсигурност като „състояние на обществото“ съгласно чл. 2 от Закона за киберсигурност[1].

4. Изкуственият интелект и новите измерения на дигиталната сигурност в училище

Интеграцията на изкуствен интелект (ИИ) в образователните структури налага ревизия на архитектурата за сигурност. Прилагането на генеративни модели за учебно съдържание и автоматизирано оценяване въвежда специфични уязвимости, които надхвърлят техническия спектър и засягат етичните норми. Съгласно приоритетите на „Плана за действие в областта на цифровото образование 2021 – 2027“, успешното внедряване на тези технологии изисква спазването на специализирани „етични насоки за надежден изкуствен интелект“, за да се гарантира защита на данните и да се избегнат рискове като стереотипи и дискриминация[4].

Рисковете в тази сфера са многопластови. От една страна, Националната стратегия за киберсигурност идентифицира заплахите от манипулирано съдържание (deep fakes) и дезинформация като елементи на хибридни въздействия, които могат да дестабилизират социалната среда[2]. В училище това създава риск от подкопаване на авторитета на преподавателите или тормоз между учениците чрез генерирано съдържание.

От друга страна, автоматизацията на процесите крие риск от дехуманизация на управлението на сигурността. Този риск не произтича от самата технология, а от нейното некритично институционално прилагане. Тук е приложим концептуалният модел за „институционален консенсус“, разработен в контекста на образователната медиация. Както ефективното справяне с конфликти изисква „психопедагогически подход“ и дълбоко разбиране на социалната среда на ученика (Lyudmilov, 2025), така и решенията, взети от алгоритми, се

нуждаят от човешки надзор. ИИ може да идентифицира аномалии в мрежовия трафик, но не може да разбере социалния контекст на поведението на ученика, който често е коренът на проблема със сигурността.

Следователно дигиталната сигурност в ерата на ИИ изисква нови компетентности от учителите и директорите. Те трябва да бъдат не просто потребители на технологии, а етични гаранти, които могат да разпознават алгоритмичните отклонения и да предпазват учениците от тях. Липсата на регламентирани правила за използването на ИИ в училище увеличава риска от „технологична зависимост“ и компрометиране на лични данни, което превръща въпроса от педагогически в системен проблем на образователната и националната сигурност.

Заключение

Дигиталната трансформация на училищното образование в България поставя пред образователната политика качествено нови предизвикателства, които изискват преосмисляне на традиционните подходи към управлението, сигурността и устойчивостта на системата. Направеният анализ показва, че дигиталната сигурност в училище вече не може да бъде разглеждана като изолиран технически въпрос, а трябва да се третира като системен фактор, който засяга институционалния капацитет, човешкия ресурс и общественото доверие в образователните институции.

Аналитичният разрез през призмата на PESTEL модела доказва, че киберуязвимостта на образователната система не е технологичен дефект, а следствие от разминаването между нормативните изисквания и реалния социален капацитет. Дефицитът на специализирана секторна политика, синхронизирана с „Плана за действие в областта на цифровото образование“, води до институционална фрагментация и реактивно, вместо превантивно прилагане на защитни мерки. Тази липса на координация възпрепятства изграждането на устойчива екосистема за сигурност и оставя критични процеси, открити за злонамерени въздействия.

Особено значение в този контекст има ролята на човешкия фактор и киберхигиената като основа на базовата култура на сигурност. Както се посочва в стратегическите документи, реализирането на ефективна защита изисква „формиране на изцяло нова култура на киберхигиена“[2]. Образователната политика разполага с потенциала да превърне училището в ключова среда за формиране на устойчиви нагласи и умения за сигурно и отговорно използване на цифрови технологии. Това предполага интегриране на темите за дигитална сигурност както в учебното съдържание, така и в системите за квалификация и подкрепа на педагогическите специалисти.

Интеграцията на алгоритми с изкуствен интелект (ИИ) в учебния процес предефинира параметрите на дигиталната сигурност, трансформирайки я от

техническа задача в етично-правен казус. Съгласно приоритетите на „Плана за действие в областта на цифровото образование 2021 – 2027“, обработката на масиви от данни чрез ИИ налага стриктно спазване на „етични насоки за надежден изкуствен интелект“, за да се гарантира неприкосновеността на личния живот на учениците. Този технологичен натиск изисква постигането на нов „институционален консенсус“ (Lyudmilov, 2025), при който автоматизираните решения подлежат на задължителен човешки одит и ясна отчетност.

Тук е приложим принципът за необходимостта от „институционален консенсус“ и задълбочен анализ на социалната среда, подобно на механизмите при образователната медиация (Lyudmilov, 2025). Регламентирането на алгоритмични системи в училищна среда изисква стриктното прилагане на „етични насоки за надежден изкуствен интелект“, които поставят технологичните иновации под задължителен „човешки надзор“.

Интегрирането на дигиталната защита в образователните политики не е просто оперативна необходимост, а стратегически императив, изпълняващ легалната дефиниция за киберсигурност като „състояние на обществото“ съгласно чл. 2 от Закона за киберсигурност. Капиталовложенията в институционален капацитет и „култура на киберхигиена“ генерират дългосрочна възвръщаемост, която надхвърля секторните рамки и укрепва общата „киберустойчивост“ на държавата в условията на ускорена дигитализация.

БЕЛЕЖКИ

1. Закон за киберсигурност. (2018). (Обн., ДВ, бр. 94 от 13.11.2018 г., изм. и доп.).
2. Министерски съвет. (2021). Актуализирана национална стратегия за киберсигурност „Киберустойчива България 2023“. София.
3. Европейски парламент и Съвет на Европейския съюз. (2022). Директива (ЕС) 2022/2555 от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза (NIS 2).
4. Европейска комисия. (2020). План за действие в областта на цифровото образование 2021 – 2027 г.: Приспособяване на образованието и обучението към цифровата ера (COM(2020) 624 final).
5. Министерство на транспорта, информационните технологии и съобщенията. (2019). Национална програма „Цифрова България 2025“. София.
6. Министерство на образованието и науката. (2021). Стратегическа рамка за развитие на образованието, обучението и ученето в Република България (2021 – 2030). София.

REFERENCES

ENISA. (2025). *Cybersecurity roles and skills for NIS2 essential and important entities: Mapping NIS2 obligations to ECSF*. European Union Agency for Cybersecurity. https://doi.org/10.2824/8870995.

Karadzhov, V., & Patarchanova, E. (2025). How to create the best PESTEL analysis. *International Journal of Digital Research, 1*(3), 8 – 20. https://doi.org/10.63711/ijdr.net20250301.

Latorre-Medina, M. J., & Tnibar-Harrus, C. (2023). Digital security in educational training programs: A study based on future teachers' perceptions. *Information Technologies and Learning Tools,* 95(3), 102 – 111. https://doi.org/10.33407/itlt.v95i3.5204.

Lyudmilov, M. (2025). Educational mediation in Bulgaria: Role and significance in the context of national security and social stability. *International Independent Scientific Journal,* 71, 13 – 17. https://doi.org/10.5281/zenodo.15014153.

Redecker, C. (2017). *European Framework for the Digital Competence of Educators: DigCompEdu* (Y. Punie, Ed.). Publications Office of the European Union.

DIGITAL SECURITY IN SCHOOLS AS A KEY FACTOR IN EDUCATIONAL POLICY

Abstract. In the context of intensive digitalization, the school environment increasingly operates through electronic systems, making digital security a priority for educational policies. The dynamic entry of AI-generated learning content, along with the digitalization of administrative processes, creates new challenges for teachers and administration. This study analyzes digital security beyond its technical parameters – as a structural element guaranteeing system sustainability and public trust. A policy-analytical approach is applied to national and European strategic documents, combined with a PESTEL analysis of technological and institutional risks. Emphasis is placed on "cyber hygiene" and the human factor as the foundation of security culture. The main thesis is that the lack of a unified sectoral policy in this area generates long-term risks extending beyond education and affecting national security.

Keywords: digital security; school education; educational policy; cyber hygiene; security culture; national security

✉ **Miroslav Lyudmilov, PhD student**
University of National and World Economy, Bulgaria
Sofia, Bulgaria
E-mail: mr.lyudmilov@yahoo.com