

## ПРОУЧВАНЕ НА ЕКСПЕРТНИЯ ОПИТ НА ВОДЕЩИ СТРАНИ В ОБЛАСТТА НА ОБУЧЕНИЕТО ПО КИБЕРСИГУРНОСТ ЗА УЧЕНИЦИ

Галина Димитрова Момчева, Теодора Иванова Бакърджиева,  
Веселина Георгиева Спасова, Антонина Иванова Иванова  
Варненски свободен университет „Черноризец Храбър“

## STUDY OF THE EXPERTISE OF LEADING COUNTRIES IN THE FIELD OF CYBERSECURITY EDUCATION FOR K-12 STUDENTS

Galina Dimitrova Momcheva, Teodora Ivanova Bakardjieva,  
Veselina Georgieva Spasova, Antonina Ivanova Ivanova  
Varna Free University „Chernorizets Hrabar“

**Abstract:** *Cybersecurity education in schools is related to both career opportunities for students and the safe use of Internet technologies. Therefore, the topic of cybersecurity training is covered in school curricula in a number of countries. The article analyzes the good experience of leading countries in training in this field. The different forms of such training, the readiness of the teachers, the availability of resources have been studied. Recommendations have been made to be used by educational institutions in the field of school education in Bulgaria*

**Keywords:** *cybersecurity, cyber security training.*

Киберсигурността е бързо развиваща се област, в която търсенето на работни места все повече изпреварва предлагането. Обучението в тази сфера има ключова роля за справяне с този недостиг както чрез повишаване на осведомеността и интереса към киберсигурността, така и чрез предоставяне на учениците на основните знания, от които се нуждаят за да продължат към кариерно усъвършенстване.

Настоящото изследване разглежда опита на водещите страни в обучението по киберсигурност – САЩ, Германия, Франция, Израел и Великобритания. В представително проучване от CYBER.ORG на Изследователския център EdWeek в САЩ от 2020 г. се представят формите на обучението по киберсигурност на базата на изследване, в което участват повече от 900 учители и директори [1]. Резултатите показват, че учениците и преподавателите имат ограничени познания по киберсигурност и по-малко от половината от анкетираните съобщават, че техните училища предлагат обучение по киберсигурност. Достъпът е неравномерен в отделните страни, като е съсредоточен в силно развитите региони на държавите, където присъстват високотехнологични компании и университети.

Обикновено обучението по киберсигурност в училищата от 1ви до 12ти клас е част от съществуващата, по-широка учебна програма, вместо да се преподава като самостоятелен курс. Освен това, предоставянето на обучение по киберсигурност става и чрез извънкласни програми като клубове, състезания или лагери, които също могат да предизвикат по-дълбок интерес към киберсигурността като професионална ориентация. Редица ключови теми, включително криптография, изкуствен интелект и електроника рядко се преподават в училищата и преподавателите отчитат, че повечето ученици не са добре информирани по основни теми в киберсигурността [2, 3].

Изследването показва, че по-голямата част от преподавателите (91%) в училищата нямат достатъчни познания по киберсигурност. Основно те предоставят на учениците информация за свързаните електронни устройства и тяхното взаимодействие в дигиталната епоха, защита на цифровите активи от уязвимости и моралните и етични проблеми, свързани с използването на технологиите в нашето общество.

Нивата на знанията на педагозите варират значително в зависимост от работната среда и професионалната роля. По-високи нива на знания се отчитат от учители в частни училища за разлика от държавните училища, както и в образователни общности, които работят в пряка връзка с университети и специализирани организации за професионално обучение. Проведеното проучване показва, че 80% от преподавателите, които работят в слабо развитите селски региони съобщават за липса на ресурси за обучение по киберсигурност в сравнение с 33% процента в индустриалните градски региони.

От направения анализ се вижда, че повечето ученици имат оскъдни или никакви знания за киберсигурността: докато 62 % от преподавателите отчитат, че знаят нещо по темата, само 40 % казват същото за своите ученици. Познанията на учениците и преподавателите по киберсигурност са свързани: преподавателите, които имат познания по киберсигурността, считат, че 66% от техните ученици имат някои познания по темата, а преподаватели без опит в обучението по киберсигурност определят, че техните ученици нямат никаква осведоменост по киберсигурност. По-високи нива на знания на учениците се отчитат от преподаватели в частни училища, както и в индустриално развити региони отколкото в бедни и слабо развити региони. Ясно се отчита, обаче от преподавателите, че интересът на учениците по теми, свързани с киберсигурността се засилва непрекъснато. Въпреки интереса на учениците, обучението по киберсигурност рядко е фокус на извънкласните програми.

Обучението по киберсигурност се влива най-често в съществуващите основни учебни програми на училищата. По-рядко се предлага като самостоятелен курс или се предоставя чрез извънкласни кръжочни форми. Отчита се, че въвеждащите теми в обучението по киберсигурност (като компютърна грамотност, напр.) са подходящи за най-малките ученици, а за учениците от гимназиалния курс са по-подходящи специализирани извънкласни форми, например 13 % от преподавателите виждат в състезанията по киберсигурност интерес за техните ученици в гимназията, но само 4% съобщават, че децата в начална възраст имат тази възможност.

В заключение, въпреки, че най-често срещаният подход към образованието по киберсигурност е да се включи в учебната програма, повечето преподаватели казват, че техните ученици биха имали поне средно ниво на интерес към изучаването на темата чрез извънкласни дейности като клубове, състезания и лагери [1, 2, 10, 11, 12, 13].

Онлайн тормозът и тероризмът е най-честата тема за обучение по киберсигурност в училищата в разглеждания сегмент, като 70 % от учителите и директорите дават информация, че техните ученици са се обучавали по този предмет през последната година. По-малко от 10 % от преподавателите посочват, че през последната година техните ученици са учили теми от криптографията, изкуствения интелект, електрониката, електротехниката или кибер законодателството. Засилен интерес се отбелязва към роботиката и изкуствения интелект (ИИ) и 43 % от учителите и директорите казват, че техните ученици биха искали да научат повече за това. 70 % от гимназиалните учители и директори и 55 % от техните колеги в средния курс представят ИИ като предмет, по който учениците им биха били много заинтересовани да се обучават.

Основните теми, които се включват в обучението по киберсигурност са: базова компютърна грамотност, кибертормоз/кибер тероризъм, роботика, програмиране, изкуствен интелект, защита/сигурност на данните, мрежи и интернет, електроника, компютърен хардуер и софтуер, поверителност на данните, кибер етика, кибер законодателство, криптография [1, 2, 4, 5, 6, 14].

Направеното изследване показва редица перспективи за развитие на обучението по киберсигурност в училищата. Счита се, че със създаването на екосистеми за киберсигурност в отделните образователни общности процесите на обучение ще се подобрят и оптимизират, както и ще се увеличи броят на привлечените в отделните образователни програми обучаеми [7, 8, 9].

Обобщението на проучването на експертния опит на водещи страни в областта на обучението по киберсигурност за ученици показва, че образователните активности в това направление започват от ранна училищна възраст с подходящи теми за онлайн заплахите, уязвимостите и защита и стигат до професионални теми, свързани с криптографски алгоритми и кибер законодателство. Важен фактор, който оказва влияние върху качеството на обучителния процес е средата, в която той се осъществява, като в училища, работещи в партньорски альянси с университети и бизнес компании от сектора се постига високо ниво на заинтересованост от страна на обучаемите и висока успеваемост, като учащите получават компетенции и умения за защита на поверителността и сигурността на работата в Интернет [10, 11, 12, 13, 14].

В резултат на проучването могат да се изведат няколко препоръки, които да се използват от образователните институции в областта на средното образование в България:

- повишаване на основните нива на знания по киберсигурност на преподавателите в училищата за да се подобри качеството на обучение;
- увеличаване на броя на училищата, които предлагат различни нива на обучение по киберсигурност – от базисна компютърна грамотност до криптография и системен анализ;
- обогатяване на формите на обучение и разширяване на образователните програми – от включване на самостоятелни курсове в основната учебна програма до специализирани извънкласни форми, състезания, семинари и др.

- осигуряване на достъп до обучение по киберсигурност не само в големите градове, но и в малките населени места;
- информиране на учениците за кариерни пътеки в областта на киберсигурността и възможност за сертифициране;
- създаване на партньорски алианси между училищата, специализираните катедри за обучение по киберсигурност в университетите и бизнес компании в сектора.

**References:**

1. The State of Cybersecurity Education in K-12 Schools, Results of a National Survey, EdWeek Research Center, 2020
2. Douglas A. Levin K-12 Cybersecurity Resource Center and the K12 Security Information Exchange March 10, 2021 by EdTech Strategies, LLC, and the K12 Security Information Exchange
3. Jake Kasowski, The State of K-12 CyberSecurity Education, March 2021
4. Council of the Great City Schools, Cyber-Security in Today's K-12 Environment, 2017
5. Cyber Security for Schools, 2021, <https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools>
6. Tom Symonds, Cyber security lessons offered to schools in England, <https://www.bbc.com/news/education-38938519>
7. CYBER SECURITY A Guide to Programmes and Resources for Schools & Further Education, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/410221/bis-15-77-Guide-to-cyber-security-schools-programmes-and-resources.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/410221/bis-15-77-Guide-to-cyber-security-schools-programmes-and-resources.pdf)
8. Bringing Cyber To School: Integrating Cyber Security Into Secondary School Education, [https://www.cybok.org/media/downloads/IEEE\\_SP\\_Bringing\\_Cyber\\_to\\_School\\_-\\_Oct\\_19.pdf](https://www.cybok.org/media/downloads/IEEE_SP_Bringing_Cyber_to_School_-_Oct_19.pdf)
9. E-Learning: Bildungseinrichtungen vor Bedrohungen schützen, <https://www.datensicherheit.de/e-learning-bildungseinrichtungen-bedrohungen-schutz>
10. Kostenlos Cyber-Sicherheitsmitarbeiter schulen <https://www.fortinet.com/de/training/cybersecurity-professionals>
11. Formations en cybersécurité: découvrez notre guide complet, <https://diplomeo.com/formations-cybersecurite>
12. L'école devrait-elle enseigner les bases de la cybersécurité ?, <https://www.ladn.eu/nouveaux-usages/usages-par-generation/apprendre-cybersecurite-ecole/>
13. In Israel, teaching kids cyber skills is a national mission, <https://www.timesofisrael.com/in-israel-teaching-kids-cyber-skills-is-a-national-mission/>
14. Israel teaches cybersecurity skills to its high schoolers, <https://www.pri.org/stories/2017-03-30/israel-teaches-cybersecurity-skills-its-high-schoolers>