КИБЕРПРЕСТЪПНОСТТА – АКТУАЛЕН ПРОБЛЕМ НА СЪВРЕМЕННОТО ЮРИДИЧЕСКО ОБРАЗОВАНИЕ

Доц. д-р Галина Ковачева
Доц. д-р Мария Лечева
Варненски свободен университет „Черноризец Храбър”

CYBERCRIME – AN ACTUAL PROBLEM IN THE MODERN JURISTICALLY EDUCATION

Assoc. Prof. Galina Kovacheva, PhD
Assoc. Prof. Mariya Lecheva, PhD
Varna Free University “Chernorizets Hrabar”

Резюме: *Киберпрестъпността е сериозен проблем пред съвременната държавна политика, който изисква комплексни превантивни дейности. Сред тях, укрепването на капацитета на системата за превенция и контрол над престъпността обхваща и юридическото образование. Тази задача може да бъде осъществена както посредством специализирано магистърско обучение, така и чрез включване на самостоятелна дисциплина „Противодействие на киберпрестъпността”.*

Ключови думи: *киберпрестъпност, превенция, юридическо образование*

Summary: *Cybercrime is a serious problem for modern state policy, which requires complex preventive activities. Among them, strengthening the capacity of the crime prevention and control system includes juristically education. This task can be accomplished both through specialized master's training and through the inclusion of an independent discipline "Combating Cybercrime".*

Key words: *cybercrime, prevention, juristically education*

Doi: https://doi.org/10.36997/LBCS2022.33

Въведение

Киберпрестъпността е сериозен проблем пред съвременната държавна политика. Той е включен в дневния ред на редица международни организации, като: ООН, Съветът на Европа, ШОС, ОНД, Лигата на арабските държави и др. Обръща се внимание на увеличаването на заплахите от злонамерени действия в интернет пространството и на

престъпленията, извършени чрез използването на компютърни и информационни системи. Международният опит показва, че престъпленията в киберпространството стават все по-чести и по-разрушителни и са насочени не само срещу правителствени учреждения, корпоративни и политически организации, а и срещу частни лица. Нараства рискът от различни посегателства в онлайн пространството, насочени срещу военни и цивилни цели по време на въоръжени конфликти[172]. В тази връзка киберпрестъпността може да бъде представена като динамична съвкупност от престъпления, при които компютърна система и/или компютърна мрежа са средство или предмет на престъпно посегателство.

Изложение

Киберпрестъпленията се характеризират с високо ниво на икономически щети. Жертвите им са около 559 милиона души годишно. През последните години щетите от киберпрестъпленията възлизат на 1,23% от световния БВП, като по този показател икономическата цена на киберпрестъпността надвишава тази от трафика на наркотици и пиратство[173]. Тенденцията е към ежегодно нарастване на глобалните щети от киберпрестъпленията.

Противодействието на киберпрестъпността изисква комплексни превантивни дейности, включващи мерки от разнороден характер, сред които организационните са от особено значение. Към тях се отнася укрепването на капацитета на системата за превенция и контрол над престъпността. Подготовката на специалистите в тази област изисква съвременно юридическо образование, в което особена актуалност придобива обучението по противодействие на киберпрестъпността. Тази необходимост се потвърждава от съвременните изследвания. Отчита се, че подготовката на специалистите от правоохранителните органи и органите на системата за наказателно правосъдие не обхваща специфичните аспекти, свързани с киберпрестъпността (Holt, T., Bossler, A. 2016; Gercke, M. 2012). Това от своя страна изисква придобиване на специални знания и умения в сферата на превенцията, разкриването и разследването на киберпрестъпленията. В редица страни от ЕС, САЩ, Китай, Индия, Южна Корея, Ру-

[172] https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html.

[173] https://iiv.uz/ru/news/counteracting-cybercrime-is-a-requirement-of-the-time.

сия, Беларус, Казахстан се обучават специалисти по информационна сигурност, радиоразузнаване, откриване и оперативна подкрепа за разкриване, разследване и превенция на киберпрестъпления, компютърна криминалистика. Налице е недостиг на професионалисти, притежаващи специални знания и умения в сферата на противодействието на киберпрестъпността.

Проблемът за необходимостта от актуално юридическо образование в посочената област е включен в тематично ориентираните форуми на международните организации още през втората половина на XX век. На VIII конгрес на ООН по превенция на престъпността и третиране на правонарушителите (Хавана 1990 г.) е приета Резолюция относно законодателството, свързано с компютърни престъпления[174], в която държавите членки са призовани да усъвършенстват националното си наказателно законодателство, като осигурят мерки за ефективно разкриване, разследване и наказване на компютърната престъпност. В пункт 9.1.(d) от Доклада на Секретариата до Конгреса е препоръчано да се „предвидят адекватни мерки за обучение на съдиите, служителите и агенциите, отговорни за превенцията, разследването, наказателното преследване и наказването на икономическите и компютърно свързаните престъпления"[175].

В публикувания през 1994 г. „Наръчник за превенция и контрол на компютърно свързаните престъпления" са включени мерки, свързани с юридическото обучение. Посочено е, че „за да са в състояние разследващите органи да разберат пълния потенциал на престъпното използване на компютърните технологии, те трябва да притежават знания и умения, свързани с тези технологии"[176].

Въпросът за националните и международните отговори на киберпрестъпността е поставен в приетата през 2010 г. Декларация от Салвадор[177]. В пункт 41 от Декларацията е обоснована необходи-

---

[174] https://www.cybercrimelaw.net/un.html .

[175] Eighth United Nations Congress in the Prevention of Crime and the Treatment of Offenders. Havana, 27 August – 7 September 1990: Report prepared by the Secretariat. UN: New York, 1991, p. 142 (https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf).

[176] UN Manual on the Prevention and Control of Computer-Related Crime. // International Review of Criminal Policy, 1994, Vols. 43 and 44, New York: UN, p. 34 (https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF).

[177] https://www.unodc.org/documents/congress//About/information/65-years-brochure_en.pdf .

мостта от изграждане на капацитет от специалисти, осъществяващи противодействие в сферата на киберпрестъпността[178]. Обученията, свързани с повишаване на квалификацията на държавните служители, се отнасят към основните мерки за осигуряване на изискуемия капацитет.

Отражение в политиката на Европейската общност намира и необходимостта от специализирано обучение в борбата с киберпрестъпността. В приетата през 2013 г. Директива 2013/40/ЕС на Европейския парламент и на Съвета относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета е посочено, че „следва да се насърчава активизирането на усилията за осигуряване на подходящо обучение за съответните органи, за да се подобри разбирането за киберпрестъпността и нейните последици и за стимулиране на сътрудничеството и обмена на най-добри практики“[179].

Особено внимание на повишаването на уменията и осведомеността е отделено в Съобщението на Комисията до Европейския парламент, Европейския съвет, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно Стратегията на ЕС за Съюза на сигурност, 24.7.2020 г. COM (2020) 605 final, където се посочва, че: „бъдещият план за действие в областта на цифровото образование следва да включва целенасочени мерки за изграждане на ИТ умения в областта на сигурността у цялото население. Приетата Програма за умения подпомага изграждането на умения през целия живот. Тя включва специално предвидени действия за увеличаване на броя на завършилите образование в областта на науката, технологиите, инженерството, изкуствата и математиката, необходими в авангардни области като киберсигурността“[180].

---

[178] Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World (https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf).

[179] Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 година относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета (https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32013L0040).

[180] Съобщение на Комисията до Европейския парламент, Европейския съвет, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно Стратегията на ЕС за Съюза на сигурност, 24.7.2020 г. COM (2020) 605 final, P. 33 (https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52020DC0605&from=ES).

Академичните институции в различни държави създават специализирани образователни програми, учебни планове и центрове за обучение. Изследването на Службата на ООН за наркотиците и престъпността, проведено сред 69 държави членки, показва, че „все по-голям брой университети предлагат степени, сертификати и професионално обучение в сферата на киберсигурността и проблемите, свързани с киберпрестъпленията. Университетите насърчават и приложното обучение и развитието на социални мрежи за противодействие на киберпрестъпността чрез организиране на семинари и конференции. Те предоставят възможности за обмен на информация и съвети относно разработването на превантивни мерки и технически решения"[181].

Най-често предлаганите образователни програми в тази област са по киберсигурност. Те включват предмети, като: „Информационни системи", „Системи за сигурност", „Информационни технологии", „Киберзащита", „Етика и право", „Системни комуникации", „Дигитална криминалистика" и др. Въпросът, който може да се постави, е доколко е удачно обучението по противодействие на киберпрестъпността да бъде не само част от специализирано магистърско обучение след завършване на висше образование, а и като самостоятелна учебна дисциплина, включена в учебните планове за специалност „Право".

В глобален аспект обучението в тази сфера е интегрирано в други специалности, като: „Информационни технологии с насоченост към киберсигурността"; „Криминалистика и противодействие на престъпността", даващи основа за превенция и разследване на киберпрестъпления.

В редица държави, като САЩ, Великобритания, Естония и др., съществуват магистърски програми по киберсигурност, в които не е включено обучение в сферата на цифровата и компютърната криминалистика. Друга категория университети предлагат специализирано обучение: University of East London, Великобритания; University of Portsmouth, Великобритания; Utica College Online, Utica, САЩ; Norwich University, Northfield, САЩ; EC-Council University, Албакърки, САЩ; Michigan State University, Източен Лансинг, САЩ[182].

---

[181] Comprehensive study on cybercrime. (2013). United Nations Office of Drugs and Crime, UN, New York, p. 253 (https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf).

[182] https://www.topmagistraturi.com/.

Може да се направи изводът, че в световен мащаб е преобладаващо обучението в магистърски програми по киберсигурност, което не осигурява в пълнота необходимите специализирани знания и умения за противодействие на киберпрестъпността. Необходимо е обучението да включва: превенция на киберпрестъпленията, оперативно-издирвателна дейност за разкриване на тези престъпления и тяхното разследване, както и знания относно инструментите и механизмите за осъществяване на международното сътрудничество. Това е от съществено значение, предвид транснационалния характер на киберпрестъпността.

В България, подобно на други държави, се предлагат основно магистърски програми по киберсигурност (напр.: Варненски свободен университет „Черноризец Храбър“, Нов български университет, Университет за национално и световно стопанство, УНИБИТ, Висше училище по сигурност и икономика, Военна академия „Георги С. Раковски“), като Висшето училище по телекомуникации и пощи единствено предлага магистърска програма „Комуникационни мрежи и разследване на киберпрестъпления“. Посочените магистърски програми не обхващат предметното съдържание на противодействието на киберпрестъпността. В отговор на тази необходимост през 2021 г. за първи път е разработена съвместна магистърска програма „Противодействие на киберпрестъпността“ от Академията на МВР и ВСУ „Черноризец Храбър“, която осигурява широкопрофилна и интердисциплинарна подготовка на специалистите, осъществяващи превенция и контрол над киберпрестъпленията.

Самостоятелна учебна дисциплина, свързана с противодействието на киберпрестъпността е разработена към университета на прокуратурата на Руската федерация. Това е дисциплината „Борба с киберпрестъпността“. Според А. Побегайло тя е междуотраслова дисциплина, включваща отделни елементи от: наказателното право, криминологията, криминалистиката, международното публично и частно право, наказателния процес, административното право и гражданското право. Многокомпонентното съдържание на дисциплината се обуславя от сложността и многоаспектността на изучавания обект (Побегайло, А. 2018). Подобен подход, според автора, може да осигури необходимото съчетаване на елементи от различните правни отрасли с оглед придобиването на комплексни знания и умения в борбата с киберпрестъпността.

Възможен е и друг подход, при който дисциплината „Противодействие на киберпрестъпността“ да интегрира в съдържанието си само елементи на наказателноправните науки, като: наказателно право, криминология, криминалистика и наказателнопроцесуално право. Такъв подход е целесъобразен, тъй като липсва интегративна учебна дисциплина в областта на наказателноправните науки, която да съответства на съвременните предизвикателства в обучението по право, произтичащи от обективния процес на дигитализация на съвременното общество.

Друг аргумент в подкрепа на посочения подход се открива в законодателната регламентация на борбата с киберпрестъпността в България. Така например в чл. 8, ал. 1, т. 5 от Закона за киберсигурност (2018) са визирани стратегии за борба с киберпрестъпността, сред които: повишаване на осведомеността, знанията и компетентностите; стимулиране на изследванията и иновациите в областта на киберсигурността[183]. Посочено е, че националната стратегия за киберсигурност обхваща и противодействието на киберпрестъпността (чл. 8, ал. 1, т. 2 „в”), с което изискването за въвеждане на мерки от образователен характер се включва в държавната политика за противодействие на киберпрестъпността.

Следва да се отбележи, че съществува практика в България за обучение в отделна дисциплина „Противодействие на киберпрестъпността”, включена в учебния план на специалност „Противодействие на престъпността и опазване на обществения ред” на Катедра „Сигурност и безопасност” при Варненския свободен университет „Черноризец Храбър”. Посочената практика потвърждава потребността от включването на такава дисциплина и в юридическото образование в страната.

Заключение

В заключение може да се обобщи, че киберпрестъпността е актуален проблем на съвременното юридическо образование. Той изисква както осигуряване на специализирано магистърско обучение, така и предвиждане на възможност за включване на самостоятелна дисциплина „Противодействие на киберпрестъпността“ в учебните планове на специалност „Право“.

[183] Закон за киберсигурност. // ДВ, №94, 2018.

Използвана литература:

1. Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 година относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета (https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32013L0040).

2. Закон за киберсигурност. // ДВ, №94, 2018.

3. Национална стратегия за киберсигурност „Киберустойчива България 2020" (https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1120).

4. Побегайло, А. (2018). Борьба с киберпреступностью. Учебное пособие. Москва: Университет прокуратуры Российской федерации.

(Pobegailo, A. (2018). Borba s kiberprestupnostio. Uchebnoe posobie. Moskva: Universitet prokuraturai Rossiiskoi federacii)

5. Съобщение на Комисията до Съвета и до Европейския парламент: Борбата с престъпността в дигиталната ера: създаване на Европейски център по киберпрестъпност **/* COM/2012/0140 final */ (**https://eur-lex.europa.eu/legal-content/BG/ALL/?uri=CELEX%3A52012DC0140**).**

6. Съобщение на Комисията до Европейския парламент, Европейския съвет, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно Стратегията на ЕС за Съюза на сигурност, 24.7.2020 г. COM(2020) 605 final P.33 (https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52020DC0605&from=ES).

7. Comprehensive study on cybercrime. (2013). United Nations Office of Drugs and Crime, UN: New York (https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf).

8. Gercke, M. (2012). Understanding Cybercrime: Phenomena, Challenges and Legal Response ITU, (Understanding cybercrime: Phenomena, challenge and legal response (itu.int).

9. Holt. T., Bossler, A. (2016). Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses. New York: Routledge.

10. Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their

Development in a Changing World (https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf).

11. UN Manual on the Prevention and Control of Computer-Related Crime. // International Review of Criminal Policy, 1994, Vols. 43 and 44, New York: UN, (https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF).

12. United Nations Congress in the Prevention of Crime and the Treatment of Offenders. Havana, 27 August – 7 September 1990: Report prepared by the Secretariat. UN: New York, 1991 (https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf).

13. https://www.unodc.org/documents/congress//About/information/65-years-brochure_en.pdf.

14. https://www.cybercrimelaw.net/un.html.

15. https://studyabroad.bg/.

За контакти:
Доц. д-р Галина Ковачева
ВСУ „Черноризец Храбър“,
Юридически факултет
E-mail: galya.kovacheva@vfu.bg

Доц. д-р Мария Лечева
ВСУ „Черноризец Храбър“,
Юридически факултет
E-mail: mariya.lecheva@vfu.bg