НЕОБХОДИМОСТТА ОТ СПЕЦИАЛНОСТ „ПРОТИВОДЕЙСТВИЕ НА КИБЕРПРЕСТЪПНОСТТА“ В СЪВРЕМЕННОТО ИНТЕРДИСЦИПЛИНАРНО ОБРАЗОВАНИЕ

Доц. д-р Галина Ковачева,
Доц. д-р Мария Лечева
ВСУ „Черноризец Храбър“

Противодействието на киберпрестъпността е важен елемент от съвременната политика за борба с престъпността. Актуалността на проблема, свързан с престъпността в областта на информационните технологии, се отчита от редица международни организации като: ООН, Съвета на Европа, 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.

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[1]. Тенденцията е към ежегодно нарастване на глобалните щети от киберпрестъпленията. 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. В периода на глобалната пандемия от Ковид-19 са извършени множество атаки срещу здравните системи на различни държави[2]. Нараства рискът от различни посегателства в онлайн пространството, насочени срещу военни и цивилни цели по време на въоръжени конфликти[3].

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

[2] **Mahadevan,** P. (2020) Cybercrime: Threats during the COVID-19 pandemic. Global Initiative against transnational organized crime, pp. 3 – 4 (https://globalinitiative.net/wp-content/uploads/2020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf).

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

В контекста на съвременните глобални заплахи става все по-актуално разкриването на университетски специалности, свързани с противодействието на киберпрестъпността. Изследванията, посветени на подготовката на специалистите, осъществяващи противодействие на престъпността, показват, че тяхното образование не обхваща специфичните аспекти, свързани с киберпрестъпността[4]. Това от своя страна изисква придобиване на специални знания в сферата на превенцията, разкриването и разследването на компютърните и компютърно свързаните престъпления, извършвани в киберсредата. В отговор на посочената потребност в редица страни от ЕС, САЩ, Китай, Индия, Южна Корея, Русия, Беларус, Казахстан и др. се обучават специалисти по информационна сигурност, радиоразузнаване, откриване и оперативна подкрепа за разкриване, разследване и превенция на киберпрестъпления, компютърна криминалистика.

Настоящият доклад се основава на проучване на политиката на ООН, Съвета на Европа и Европейския съюз, както и на добрите практики във водещите университети в страната и чужбина. Той представя възможностите за обучение по специалност „Противодействие на киберпрестъпността“ в България в контекста на вече създадената съвместна магистърска програма на Академията на МВР и ВСУ „Черноризец Храбър“.

1. Образованието по противодействие на киберпрестъпността в контекста на политиката на ООН, Съвета на Европа и Европейския съюз

Проблемът за необходимостта от актуално обучение на специалистите, осъществяващи противодействие на престъпленията, свързани с информационните технологии, е включен в дневния ред на международните организации още през втората половина на XX век. За първи път, в рамките на VIII конгрес на ООН по превенция на престъпността и третиране на правонарушителите (Хавана, 1990), е приета Резолюция относно законодателството, свързано с компютърни престъпления[5], 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“[6].

---

[4] **Holt,** T., A. **Bossler. (**2016) Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses. New York: Routledge, p. 130; Gercke, M.Understanding Cybercrime: Phenomena, Challenges and Legal Response (2012) ITU, p. 228. (Understanding cybercrime: Phenomena, challenge and legal response (itu.int).

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

[6] 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).

В изпълнение на Резолюцията, през 1994 г. ООН публикува „Наръчник за превенция и контрол на компютърно свързаните престъпления“. В мерките, посветени на правоприлагането и юридическото обучение, е посочено, 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[7]. По този начин политиката на ООН в сферата на противодействието на киберпрестъпността отдава важно значение на интердисциплинарните аспекти в обучението.

През 2010 г. на XII конгрес на ООН по превенция на престъпността и наказателно правосъдие (Салвадор, Бразилия) е приета Декларацията от Салвадор, която поставя въпроса за националните и международни отговори на киберпрестъпността[8]. В пункт 41 от Декларацията се препоръчва изграждане на капацитет от специалисти, осъществяващи противодействие в сферата на киберпрестъпността[9]. Към основните мерки, необходими за осигуряване на изискуемия капацитет, се отнасят обученията, свързани с повишаване на квалификацията на държавните служители.

Необходимостта от специализирано образование в борбата с киберпрестъпността намира отражение и в политиката на Европейската общност. През 2013 г. е приета 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. Съгласно пункт 28 от Директивата „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, както и за стимулиране на сътрудничеството и обмена на най-добри практики“[10].

В 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 от 24.7.2020 г. COM(2020) 605 final е отделено внимание на повишаването на уменията и на осведомеността. Посочено е, 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

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

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

[9] 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).

[10] Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. 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).

действия за увеличаване на броя на завършилите образование в областта на науката, технологиите, инженерството, изкуствата и математиката, необходими в авангардни области като киберсигурността“[11].

2. Проблемът за повишаване на компетенциите в сферата на противодействието на киберпрестъпността в България

Политиката за противодействие на киберпрестъпността в България се основава на световните тенденции, обусловени от развитието на дигиталните технологии. Те изискват гъвкав подход и интердисциплинарно образование за повишаване на капацитета на държавната система за превенция и контрол над престъпността. Основните инструменти за реализиране на тези цели са усъвършенстване на законодателството и разработване на актуални стратегии за противодействие на киберпрестъпността.

През 2018 г. в България бе приет Закон за киберсигурност. Той въведе изискванията на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза. Сред стратегиите, визирани в чл. 8, ал. 1, т. 5 от Закона, е: „повишаването на осведомеността, знанията и компетентностите; стимулиране на изследванията и иновациите в областта на киберсигурността“[12]. 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.

Важно значение в изследваната област имат и стратегическите документи за управление на превенцията и контрола над киберпрестъпността. През 2016 г. Министерски съвет прие Национална стратегия за киберсигурност „Киберустойчива България 2020“. Сред мерките, предвидени в стратегията, е включено и обучението за придобиване на компетенции в сферата на киберсигурността[13]. Тази идея е доразвита в актуализираната национална стратегия за киберсигурност „Киберустойчива България 2023“. В нея е акцентирано върху необходимостта от ефективно използване на формите на продължаващо обучение, допълнителна квалификация и преквалификация на всички нива за допълване и актуализиране на компетентностите в сферата на киберсигурността и използването на ИКТ във връзка с бързото развитие на технологии и платформи и произтичащите нови отговорности и заплахи, функционална и тематична квалификация в съответствие с установените стандарти и сертификация чрез създаване на сертификационни

---

[11] 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).

[12] Закон за киберсигурност (ДВ, бр. 94 от 13 ноември 2018 г.).

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

програми за служителите в администрацията, сектора за сигурност и академичния сектор[14].

Може да бъде направен извод, че разкриването на специалности, свързани с противодействието на киберпрестъпността, ще отговори в значима степен на потребността от внедряване на мерки от образователен характер.

3. Добрите практики за образование в магистърски програми по противодействие на киберпрестъпността

В отговор на изискванията на държавата и частния сектор за осигуряване на специалисти по киберсигурност и противодействие на киберпрестъпността, 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“[15].

За установяване на съществуващите добри практики в други държави през 2021 г. бе проведено проучване от екип специалисти от ВСУ „Черноризец Храбър“. Резултатите от него показаха, че най-често предлаганите образователни програми са по киберсигурност. Те покриват основите на компютърните науки, както и предмети като: „Информационни системи“, „Системи за сигурност“, „Информационни технологии“, „Киберзащита“, „Етика и право“, „Системни комуникации“, „Дигитална криминалистика“ и др.

В глобален аспект много от програмите интегрират обучението в тази сфера към други специалности. Най-общо киберсигурността е застъпена в:

- Специалности по информационни технологии с насоченост към киберсигурността. В тяхната основа е заложено изучаването на системи за сигурност и управление на данни;
- Специалности, свързани с криминалистика и противодействие на престъпността с насоченост към киберсигурността – тези програми дават основа за превенция и разследване на киберпрестъпления.

Водещите университети, предлагащи програми по компютърни науки, са в САЩ и Великобритания. Освен лидерите (имена като Massachusetts Institute of Technology, Stanford, Carnegie, Oxford, Cambridge) има няколко университета в Европа със сходни програми. Тук се отнасят:

---

[14] Актуализирана национална стратегия за киберсигурност „Киберустойчива България 2023“ (https://e-gov.bg › wps › connect › e-gov.bg-18083).

[15] 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).

- Abertay University, Шотландия – Бакалавър: „Етично хакерство“, Магистър: „Етично хакерство и компютърна сигурност“;
- Eindhoven University of Technology, Холандия – Магистър: „Информационна сигурност“; „Киберсигурност“;
- Imperial College London – Магистър: „Компютърна сигурност“;
- Lancaster University, Великобритания – Магистър: „Киберсигурност“;
- Royal Holloway, Великобритания – Бакалавър: „Компютърни науки“ със специализация „Сигурност на информацията“, Магистър: „Сигурност на информацията“[16].

Към категорията *научни организации* в Европа, които осигуряват добра професионална подготовка по киберсигурност, се отнасят и някои технологични институти в Германия, Швейцария, Италия и Швеция, сред които:

- SRH Hochschule Berlin, Германия – предлага магистърска програма по компютърни науки с фокус „Киберсигурност“;
- ETH Zurich, Швейцария – магистърска програма „Киберсигурност“;
- EIT Digital Master School, Тренто, Италия – магистърска програма „Киберсигурност“;
- Bologna Business School, Болоня – магистърска програма „Киберсигурност“, насочена специално към Европейския регламент за защита на личните данни (GDPR) в SIDA (Рим, Милано).

От 14 учебни заведения, предлагащи магистърски програми по киберсигурност *(вж. Таблица № 1),* две са във Великобритания, едно е в Естония, а останалите единадесет – в САЩ. Съществен недостатък на изброените магистърски програми е липсата на обучение в сферата на цифровата и компютърната криминалистика.

Таблица № 1

№ по ред	**Име на университета**	**Професионална квалификация на обучаващите се в магистърски програми**
1	Калифорнийски държавен университет, Сан Бернардино – САЩ	Магистър по Национални изследвания за киберсигурност
2	Университетът Карнеги Мелън, Питсбърг – САЩ	Магистър по информационна сигурност и осигуряване; Магистър по информационна сигурност; Кобе магистър по научни изследвания в областта на информационните технологии – информационна сигурност (MSIT-IS) Двойна степен; Магистър по информационни технологии – Инженеринг за поверителност; Магистър по политика и управление на информационната сигурност
3	Университет Де Монфор, Лестър – Великобритания	Магистър по киберсигурност; Докторат по киберсигурност и софтуерни технологии; Магистър по кибертехнология

[16] https://studyabroad.bg/.

4	Университет Джордж Вашингтон, Вашингтон – САЩ	Магистър по киберсигурност в компютърните науки; Магистър по стратегия за киберсигурност и управление на информацията; Магистър по инженерна политика в областта на политиката и спазването на киберсигурността; Магистър по професионални изследвания по стратегия за киберсигурност и управление на информацията; Световният изпълнителен магистър по бизнес администрация с концентрация в киберсигурността
5	Университет Индиана, Блумингтън – САЩ	Магистър по киберсигурност в компютърните науки; Магистър по стратегия за киберсигурност и управление на информацията; Магистър по инженерна политика в областта на политиката и спазването на киберсигурността; Магистър по професионални изследвания по стратегия за киберсигурност и управление на информацията; Световен изпълнителен магистър по бизнес администрация с концентрация в киберсигурността
6	Държавен университет в Канзас, Манхатън – САЩ	Магистър по софтуерно инженерство; Бакалаври по компютърни науки; Компютърни науки – Киберсигурност BS
7	Военноморско следдипломно училище, Монтерей – САЩ	MS, киберсистеми и операции; MS, Приложни кибероперации; MA, Управление на идентичността и киберсигурност; MS, киберсистеми и операции; Сертификати за киберсигурност
8	Държавен университет в Пенсилвания – САЩ	Магистър по професионални изследвания в областта на информационните науки – киберсигурност и осигуряване на информация; Магистър по професионални изследвания по национална сигурност – опция за информационна сигурност и криминалистика
9	Queen‘s University Белфаст, Белфаст, Северна Ирландия, Великобритания	Магистър по киберсигурност; доктор в киберсигурността – CSIT Център за докторантско обучение
10	Рочестърски технологичен институт, Рочестър – САЩ	Магистър по компютърна сигурност; Усъвършенстван сертификат за осигуряване на информация
11	Талински технологичен университет, Талин – Естония	Киберсигурност (MSc) (съвместна програма с Университета в Тарту)
12	Университетски колеж в Мериленд, Аделфи – САЩ	Магистър по киберсигурност; Управление и политика за киберсигурност (магистри); Цифрова криминалистика и киберразследване (магистри); Информационни технологии: специалност за осигуряване на информация (магистри)
13	Тексаски университет в Сан Антонио, Тексас, САЩ	Магистър по информационни технологии – Концентрация на киберсигурността
14	Политехнически институт в Уорчестър, Уорчестър – САЩ	Магистър по компютърни науки със специализация по киберсигурност

**Данните са изведени чрез проучване в Keystone (https://www.topmagistraturi.com/)*

Друга категория университети предлагат специализирано обучение в сферата на информационната сигурност и цифровата криминалистика *(вж. Таблица № 2)*.

Таблица № 2

№ по ред	**Име на университета**	**Професионална квалификация на обучаващите се в магистърски програми**
1	University of East London, Великобритания	Магистър по информационна сигурност и цифрова криминалистика
2	University of Portsmouth, Великобритания	Магистър: Киберсигурност и компютърнарна криминалистика
3	Utica College Online, Utica, САЩ	Магистър: Киберсигурност и цифрова криминалистика
4	Norwich University, Northfield, САЩ	Магистър по киберсигурност – компютърно съдебно разследване и управление на екипи за реакция при инциденти
5	EC-Council University,Албакърки, САЩ	Специализация Digital Forensic
6	Michigan State University, Източен Лансинг, САЩ	Магистър по киберпрестъпност и цифрови разследвания

**Данните са изведени чрез проучване в Keystone (https://www.topmagistraturi.com/)*

Данните от проведеното проучване показаха, че в световен мащаб е налице насищане на пазара с магистърски програми по киберсигурност, в резултат на което бе направен изводът, че обучението не може да осигури потребността от специализирани знания и умения в сферата на противодействието на киберпрестъпността. Магистърските програми по киберсигурност имат по-тесен предметен обхват. Те осигуряват знания относно сигурността на информацията в електронна среда: електронни устройства и мрежи. От друга страна – противодействието на киберпрестъпността включва: превенция на киберпрестъпленията, оперативно-издирвателна дейност за разкриване на тези престъпления и тяхното разследване. Осигуряват се знания относно инструментите и механизмите за осъществяване на международното сътрудничество. Този обхват на образователния продукт е от съществено значение предвид транснационалния характер на киберпрестъпността.

Образователният пазар в България в изследваната област на знанието притежава сходни характеристики. Подобно на чуждестранните университети, в страната се предлагат основно магистърски програми по киберсигурност (напр.: ВСУ „Черноризец Храбър“, Нов български университет, Университет за национално и световно стопанство, УНИБИТ, Висше училище по сигурност и икономика, Военна академия „Георги С. Раковски“). Единственият университет в България, който предлага магистърска програма „Комуникационни мрежи и разследване на киберпрестъпления“, е Висшето училище по телекомуникации и пощи, София. Но дори посочената магистърска програма не обхваща предмета на специалността „Противодействие на киберпрестъпността“.

В отговор на посочените тенденции Академията на МВР и ВСУ „Черноризец Храбър“ разработиха съвместна магистърска програма „Противодействие на ки-

берпрестъпността“, която ще осигури широкопрофилна и интердисциплинарна подготовка на специалистите, осъществяващи превенция и контрол над киберпрестъпленията. Очакваните резултати от внедряването на новия образователен продукт са свързани със задоволяване на необходимостта от висококвалифицирани кадри, притежаващи знания за вътрешноправната, сравнителноправната европейска и международна уредба на борбата с компютърните и компютърно свързаните престъпления.

ЛИТЕРАТУРА:

1. Актуализирана национална стратегия за киберсигурност „Киберустойчива България 2023“ (https://e-gov.bg › wps › connect › e-gov.bg-18083).
2. Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. 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);
3. Закон за киберсигурност (ДВ, бр. 94 от 13 ноември 2018 г.).
4. Национална стратегия за киберсигурност „Киберустойчива България 2020“ (https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1120).
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. 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. (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).
9. Gercke, M.Understanding Cybercrime: Phenomena, Challenges and Legal Response (2012) ITU, (Understanding cybercrime: Phenomena, challenge and legal response (itu.int).
10. Holt, T., A. Bossler. (2016) Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses. New York: Routledge.
11. Mahadevan, P. (2020) Cybercrime: Threats during the COVID-19 pandemic. Global Initiative against transnational organized crime (https://globalinitiative.net/wp-content/uploads/2020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf).

12. 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).
13. UN Manual on the Prevention and Control of Computer-Related Crime. International Review of Criminal Policy, Nos. 43 and 44, UN, New York, 1994, (https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF).
14. https://www.unodc.org/documents/congress//About/information/65-years-brochure_en.pdf
15. https://www.cybercrimelaw.net/un.html
16. https://studyabroad.bg/
17. https://iiv.uz/ru/news/counteracting-cybercrime-is-a-requirement-of-the-time
18. https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html.

НЕОБХОДИМОСТТА ОТ СПЕЦИАЛНОСТ „ПРОТИВОДЕЙСТВИЕ НА КИБЕРПРЕСТЪПНОСТТА“ В СЪВРЕМЕННОТО ИНТЕРДИСЦИПЛИНАРНО ОБРАЗОВАНИЕ

Доц. д-р Галина Ковачева,
Доц. д-р Мария Лечева
ВСУ „Черноризец Храбър“

Резюме: Противодействието на киберпрестъпността е актуален аспект от съвременната политика за борба с престъпността. То изисква подходяща интердисциплинарна подготовка на специалистите в тази област. Създаването на магистърска програма „Противодействие на киберпрестъпността“ отговаря на посочената потребност, международните стандарти и добрите образователни практики в други държави.

Ключови думи: противодействие, киберпрестъпност, интердисциплинарно образование, повишаване на квалификацията.

THE NEED FOR A SPECIALTY „COUNTERING THE CYBERCRIME“ IN THE MODERN INTERDISCIPLINARY EDUCATION

Assoc. Prof. Galina Kovacheva, PhD; Assoc. Prof. Mariya Lecheva, PhD
VFU „Chernorizets Hrabar“

Summary: Countering the cybercrime is an actual aspect of the modern anti-crime policy. It requires an appropriate interdisciplinary training of specialists in this field. The establishment of a master`s program „Countering the cybercrime“ meets the indicated need, the international standards and the good educational practices in other countries.

Keywords: counteraction, cybercrime, interdisciplinary education, raising the qualification.