НАУЧНИ ТРУДОВЕ НА УНСС (3) 2022, ИК – УНСС
ISSN (online): 2534-8957; ISSN (print): 0861-9344; http://unwe-research-papers.org/
DOI: https://doi.org/10.37075/RP.2022.3.01

ПРОФЕСИИ И ДЛЪЖНОСТИ В КИБЕРСИГУРНОСТТА И СВЪРЗАНОТО С ТЯХ ОБУЧЕНИЕ

Константин Пудин[1]
e-mail: kpoudin@unwe.bg

Резюме

Новите технологии и тяхното навлизане в различни сфери на живота водят до редица промени. Част от тези промени са свързани с появата на нови професии и длъжности. Публикацията има за цел да представи промените в професиите, длъжностите и работните позиции, предизвикани от съвременните социално-икономически и технологични условия. Тези промени без съмнение пораждат и нови изисквания пред обучението по специалностите, имащи отношение към тях и неговото качество. Фокусът е поставен върху длъжностите в киберсигурността и свързаното с тях обучение.

Ключови думи: професии, длъжности, киберсигурност, обучение

JEL: J60, H56

Увод

С всяка изминала година значението на технологиите и техниката в живота ни се увеличава. Без тях вече става немислимо ефективното протичане на ежедневието ни на работното място или в дома. Те намират приложение в свободното ни време, при гарантиране на сигурността и грижата за нашето здраве. Технологиите и машините, при равни други условия, правят живота ни по-удобен, по-лесен, по-приятен, по-сигурен.

Сред най-ярките примери за тази тенденция, която се налага от няколко века насам, е автоматизацията, замяната на човека и по-конкретно на неговия труд с машината. В наши дни тя придобива ново измерение, свързано с все по-широкото приложение на изкуствен интелект (artificial intelligence – AI). Един процес, който води до повишаване на производителността и до създаването на нови и по-качествени стоки и услуги. Безспорно тенденция, имаща положителни последствия в дългосрочен план.

В доклада на Световния икономически форум The Future Jobs Report 2020 е отбелязано, че през 2020 г. делът на автоматизация в различните дейности е 33%, докато делът на човешкия труд е 67%. Очаква се този дял да се повиши на 47% до 2025 г.

[1] Доцент, доктор, катедра „Национална и регионална сигурност“, УНСС

Автоматизацията в контекста на цялостното технологично развитие променя живота на хората. Промяна, която често пъти е свързана с поемането на висока социална цена. Типичен пример за това е изчезването на съществуващите на даден етап професии, тяхното трансформиране с цел адаптация в новите условия или появата на нови професии, която същите тези условия налагат.

Тези процеси неминуемо засягат отделния човек и неговата сигурност. Те налагат демонстриране на гъвкавост и адаптивност, промяна в поведението, повишаване на квалификацията в рамките на упражняваната професия и дори много често професионална преориентация, което е свързано с придобиването на нови знания, умения и компетентности в рамките на различните форми, които системата за обучение предлага. Всичко това е свързано и с провеждането на цялостна политика, която, отчитайки процесите и възникващите потребности, трябва да бъде насочена към по-плавното и по-безболезнено приспособяване на обществото и отделната личност към новите изисквания на цялостния технологичен, икономически и социален контекст.

Целта на тази публикация е да представи промените в професиите, последвани от промени в длъжностите и работните позиции, а също свързаните с тях задачи и изисквания към знанията, уменията и компетентностите, които заемащите ги лица, трябва да притежават. Тези промени неминуемо пораждат и нови изисквания пред обучението по специалностите, имащи отношение към тях. Фокусът е поставен върху длъжностите в киберсигурността и свързаното с тях обучение.

Реализацията на тази цел предполага изпълнението на следните три основни задачи:

- анализ на общите тенденции в развитието на професиите;
- представяне на професиите и длъжностите, имащи отношение към киберсигурността на съвременния етап, в т.ч. изясняване на тяхната същност и изискванията към знанията и уменията, които лицата, които ги упражняват, следва да притежават;
- анализ на съществуващите практики в обучението по специалности, имащи отношение към гарантиране на киберсигурността и представяне на насоките за развитие с цел повишаване качеството на това обучение.

Изпълнението на третата задача е подпомогнато от част от отговорите на анкета, посветена на подобряване на качеството на преподаването и обучението по дисциплина „Основи на киберсигурността“ от учебната програма на магистърска специалност „Управление на киберсигурността“, водена от катедра „Национална и регионална сигурност“ на УНСС. Анкетата е ано-

нимна. Проведена е през юли 2021 г. чрез приложението MS Teams, като в нея участват завършили бакалавърска и магистърска степен по специалност „Икономика на отбраната и сигурността“ в УНСС.

Тезата, която се издига в настоящата статия е, че потребността от нови умения в рамките на възникващи професии или променящи се професии в съвременните условия на средата налага преосмисляне, периодична актуализация на обучението в областта на сигурността, в т.ч. киберсигурността, което ще бъде свързано и с повишаване на неговото качество.

В материала се анализират процеси и тенденции, които се наблюдават през последните пет-шест години, даващи отражение в настоящия момент и които най-вероятно ще се запазят в рамките на следващите пет-десет години. Изследването, базирано на прилагане на метода на сравнителния анализ, допълнен от резултати получени от анкетно проучване, обхваща обучението във ВУЗ в страната по актуални специалности и свързаните с тях професии и длъжности по киберсигурност.

Още в самото начало следва да бъде направено уточнението, че под понятието „професия“ следва да се разбира – съвкупност от длъжности, чиито основни функции и задачи се характеризират с висока степен на сходство, а под „длъжност“ ще се има предвид – съвкупност от функции и задачи, които едно лице изпълнява на работното си място. В International Standard Classification of Occupations (ISCO) се използват понятията „occupation“, което на български се приема за професия и „job“, което на български е еквивалентно на длъжност.

Съвременни условия и тенденции в развитието на професиите, в т.ч. професии в сферата на сигурността

При новите технологични условия, които водят до икономически и социални промени, много професии изчезват или се налага да бъде преосмислено тяхното съдържание и обхват. Появяват се нови професии, които до този момент общественото развитие не е познавало.

Тези процеси дават отражение и върху броя на работните места и заетостта като цяло. В споменатия вече доклад на World Economic Forum (2020) се отбелязва, че до 2025 г. 85 млн. работни места може да изчезнат в резултат от разделението на труда между хората и машините. В тази връзка се прогнозира и друга тенденция – появата на 97 млн. нови работни позиции.

Обществото постепенно се разделя с професии и съответно с работни места, които са свързани с обслужването на клиенти в различни сфери. Така например компютрите и комуникациите улесняват подаването и обработката на най-различни документи, закупуването на билети и пазаруването, кое-

то прави излишен човешкия труд „на гише“ или каса. Роботите постепенно изместват човека в сферата на транспорта, сигурността, образованието и дори здравеопазването. Редица производствени процеси в индустриалната сфера и селското стопанство са механизирани от години, като се наблюдава непрестанен процес на технологична модернизация, водеща до отпадане на човешкия труд или до промяна в изискванията към неговото качество.

Много от професиите не отпадат, а променят своето съдържание. Пример за това са професиите, които са свързани с преподаването на знания и развитието на умения. В условията на интернет, предоставящ възможност за бърз достъп до информация, ролята на преподавателите все повече се променя. Освен даващи знания, новото изискване към тях е да бъдат хора, които трябва да насочват и най-вече да мотивират обучаваните сами да търсят информация, да работят с нея, да я анализират и да намират нейното практическо приложение в професионален и личен план.

Новите професии и работните места, които се създават с тяхната поява, са в съответствие със съществуващите технологични и социално-икономическа условия.

Редовните наблюдения по отношение на търсенето на хора за определени работни позиции показват, че се увеличава търсенето на: *анализатори на данни и специалисти в тази област*, *специалисти в областта на изкуствения интелект и алгоритмите за машинно обучение*, *специалисти в областта на големи данни, софтуерни разработчици*, *специалисти в дигиталния маркетинг, а също такива в областта на киберсигурността*.

Тенденция към намаляване на търсенето се наблюдава по отношение на: *служители, ангажирани с въвеждането на данни*, *административни секретари*, *счетоводители, касиери и други служители, занимаващи се със счетоводна дейност и одит*, *лица, ангажирани с обслужването и информирането на клиенти, монтажници и работници в индустриалната сфера, пощенски служители, административни мениджъри* и др. (таблица 1).

Таблица 1: Топ 20 работни позиции с нарастващо и намаляващо търсене в рамките на индустриите

НАРАСТВАЩО ТЪРСЕНЕ	НАМАЛЯВАЩО ТЪРСЕНЕ
1	2
Data Analyst and Scientist	Data Entry Clerks
AI and Machine Learning Specialist	Administrative and Executive Secretaries
Big Data Specialists	Accounting, Bookkeeping and Payroll Clerks

Продължение

1	2
Digital Marketing and Strategy Specialists	Accountants and Auditors
Process Automation Specialists	Assembly and factory Workers
Business Development Professionals	Business Services and Administration Managers
Digital Transformation Specialist	Client Information and Customer Service Workers
Information Security Analyst	General and Operations Managers
Software and Application Developers	Mechanics and Machinery Repairs
Internet of Things Specialists	Material-Recording and Stock-Keeping Clerks
Project Manager	Financial Analyst
Business Services and Administration Managers	Postal Services Clerks
Database and Network Professionals	Sales Rep., Wholesale and Manuf., Tech. and Sci. Products
Robotics Engineers	Relationship Managers
Strategic Advisors	Bank Tellers and Related Clerks
Management and Organization Analyst	Door-to-Door Sales, News and Street Vendors
FinTech Engineers	Electronics and Telecoms Installers and Repairs
Mechanics and Machinery Repairers	Human Resources Specialists
Organizational Development Specialists	Training and Development Specialists
Risk Management Specialists	Construction Laborers

Източник: World Economic Forum (2020).

От различни източници – специализирани изследвания и доклади или статии в популярни издания, става ясно, че в бъдеще ще се развиват професии, които са свързани с дигитализацията и комуникациите, изкуствения интелект и роботизацията. В наименованието си повечето от тях съдържат думи като *разработчик* (например *software developer* или *web developer*), *специалист* (например *AI specialist, AI business development specialist/manager, Data specialist, Internet of things specialist* или *E-commerce specialist*), *анализатор* (*Big Data analyst*) или *инженер* (например *3D architect and engineer*).

Прави впечатление, че се появяват нови професии или се разширява обхвата на съществуващи до момента такива, имащи отношение към комуни-

кацията, общуването на ниво организация или отделен човек, изграждането и поддържането на имидж. Такива са *community manager*, чиито функции се доближават до тези на познатия специалист по връзки с обществеността, но имат и нов прочит. Според едно от обясненията на ролята на community manager е, че той/тя е посланик на дадена марка в обществото, сред което трябва да създаде лоялна група от основни потребители и да изгражда и поддържа отношения с тях. Те също са фокусирани върху измерването на настроенията около марката, като използват инструменти за социално слушане, за да следят обратната връзка и ангажираността. Друга близка професия е тази на *social media analyst*.

В съвременните условия се появяват и утвърждават професии, които имат отношение към организирането на различни аспекти от живота на човека. Става дума за професии, в чието наименование се съдържат думи като: *наставник (mentor)*, *инфлуенсър (influencer)*, *треньор/инструктор (coach)*. Счита се, че една такава професия ще бъде тази на т. нар. *wholeness mentor*, който ще подпомага хората при разработването на жизнените им стратегии и ще допринася те да организират ежедневието си по един хармоничен начин, занимавайки се с нещата, които обичат и общувайки пълноценно помежду си. До голяма степен дейността на *wholeness mentor* съвпада с тази на вече придобилата известност професия на *life mentor*.

В дигиталната ера светът не е по-сигурно място за живеене. Появяват се нови уязвимости, нови заплахи и разбира се нови подходи, методи и средства за превенция и реакция с цел гарантиране на сигурността. Всичко това извежда интересът към професии, в чийто обхват влиза изпълнението на задачи по наблюдение и анализ на средата – вътрешна и външна, идентифициране на опасностите и заплахите за интересите на конкретни субекти на сигурността – отделни лица, организации, държави, а също и управлението на риска. В този контекст не е случаен факт, че в доклада на Световния икономически форум The Future Jobs Report 2020 професията *risk management specialist* попада в групата на двадесетте професии, към които се забелязва нарастващо търсене.

Наред с традиционните измерения на сигурността – отбрана, вътрешен ред и правосъдие, външна политика и измеренията в рамките на нейното широко разбиране – икономика, енергетика, екология, образование, здравеопазване и т.н., днес голяма актуалност придобива темата за киберсигурността и нейното гарантиране. Това прави професии като *information security analyst* и *cybersecurity manager* търсени от работодателите и желани за професионална реализация.

Съвременни професии и длъжности, свързани с киберсигурността

Във всяка сфера на човешка дейност се забелязват измеренията на сигурността и безопасността. Сигурността, както многократно е изтъквано, е много широко понятие. Най-общо може да се приеме, че то засяга съществуването, нормалното осъществяване и развитието на дадената дейност и респективно съществуването, функционирането и развитието на конкретните субекти, които имат отношение към нея. В този контекст гарантирането на сигурността може да обхване всеки един аспект, който е свързан с въпросната дейност. Така например лицето, занимаващо се с производството на дадено изделие, без директно да има нещо общо със сигурността, може да се окаже със своите знания, учения, компетентности и най-вече мотивация и морален облик фактор за тази сигурност. Несигурност би могла да бъде породена от лошото управление на дейността, намиращо израз в последица от грешни управленски решения.

В не толкова общ и широк смисъл сигурността се свързва със защита на ценности, анализ на информация за средата, предвиждане на опасности, предприемането на превантивни действия и отговор на конкретни заплахи. Напоследък все по-често под сигурност се разбира управление на риска. С това разбиране за сигурността и нейното гарантиране са свързани определени професии, представени в този материал.

През последните години понятието киберпространство придобива особена актуалност. Това е новата среда, в която хората живеят. В него те работят, общуват и прекарват свободното си време. Пандемията от COVID-19 от 2020 г. дава допълнителен тласък за по-бързото развитие на дигиталния живот. Както в недигиталния, така и в дигиталния живот ясно се открояват измеренията на сигурността – въпросите за оцеляването и съществуването, нормалното функциониране и развитието, намиращи конкретен израз в придобиването и увеличаването на материални и нематериални ценности, а също защитата им от посегателство. Кибрепространството и хората в него се оказват също толкова уязвими, колкото преди. В киберсредата се наблюдават както познатите опасности и заплахи, така и нови такива.

Новите условия придават все по-голямо значение на ролята на специалистите по киберсигурност, което води до увеличаване търсенето на техния труд. В различни източници, в т.ч. Cybersecurity Job Report 2017, се посочва, че до 2021 г. ще има незаети 3,5 млн. позиции, свързани с киберсигурността (Morgan, 2017, p. 2). Според данните на Бюрото по трудова статистика (BLS) търсенето на работни места в киберсигурността в САЩ, като например анализатори на информационната сигурност, ще нарасне с цели 31% през следващите десет години. В публикацията на Канадския център за киберсигурност (CCCS) Cyber Security Career Guide се посочва, че броят на

работните места за специалисти по киберсигурност в Канада нараства със 7% всяка година (CCCS, 2020).

Едно сравнително пълно описание на професиите, които в наши дни имат отношение към киберсигурността, предоставя сайта Cybersecurity Guide и конкретно частта Guide to Cybersecurity Jobs (Bowcut, Liddle, et. al., 2021). От него се вижда, че може да се наблюдават различни длъжности, чиито задължения са свързани с гарантирането на разнообразните аспекти на киберсигурността. Наред с допълването, което съществува между отделните длъжности, се забелязва и припокриване на техните задачи. Някои от представените в сайта длъжности са:

Security Engineer – Инженерите по сигурността или инженерите по информационна сигурност изпълняват по-скоро техническа роля във компанията/организацията. Тяхната работа се състои в това да внедрят и наблюдават компютърни и мрежови протоколи за защита, за да защитят поверителната информация от хакване или кражби. Подобно на други професии по киберсигурност, инженерите по киберсигурност често може да имат и други задължения в зависимост от размера на компанията или организацията, отрасъла и др.

Chief Information Security Officer – Директорът по сигурността на информацията или Главният служител (буквално преведено – главен офицер) по сигурността на информацията е най-високата позиция, която има отношение към информационната сигурност в една компания/организация. Той докладва директно на изпълнителния директор. Позицията изисква богат опит, знания и практически умения във възможно най-много аспекти на информационната сигурност.

Security Analyst – Анализаторът на сигурността или анализаторът на информационната сигурност има широки задължения, които са свързани със защитата на компютърната инфраструктура и мрежите. Отговорностите на лицата на тази длъжност може да варират от контрол на достъпа до файлове, удостоверяване, поддържане на защитни стени и актуализации на мрежата до търсене на уязвимости и слабости в рамките на проактивни действия, свързани с избягване на атаки.

Computer Forensics или *Computer Forensics Analyst*, или *Computer Forensic Investigator* – Специалистът по компютърни разследвания събира, анализира и проучва данни и компютърни доказателства.

Security Consultant – Функциите на консултанта по информационна сигурност се доближават до тези на анализатора на информационната сигурност. Той/тя е специалист по информационна сигурност, който е обучен да защитава поверителността, целостта и наличността на данни и мрежови устройства.

Digital Forensics – Специалистът по дигитални разследвания или Специалист по разследване на киберпрестъпления разследва кражбата на информация от компютри, мрежи, уеб приложения, мобилни телефони или други цифрови устройства. Работата му е да определи точно какво е направено и как е направено, да се опита да възстанови и/или да поправи откраднати или повредени файлове с данни и да работи с други експерти по информационна сигурност, за да предотврати това да се повтори. Съществува припокриване на функции с функциите на специалиста по компютърни разследвания.

Cryptographer – Криптографът или шифровчикът допринася за гарантиране на информационната сигурност на компания или организация, като създава и прилага кодове. Чрез тях се защитава предаваната по мрежата или съхранявана информация.

Security Administrator или *System Security Administrator*, или *IT Security Administrator* – Администраторът по сигурност или Системният администратор по сигурността има конкретни задължения, свързани с различните аспекти на информационната сигурност. Задълженията му могат да варират в зависимост от големината на организацията и спецификата на дейността. Работата му има много общо с тази на анализатора по сигурността и на консултанта по сигурността.

Penetration Tester – Лицата, които трябва да тестват сигурността на системата, като се опитат да проникнат в нея или т. нар. „етични хакери“ са наети от собственици на мрежи и доставчици на уеб базирани приложения. Те трябва да търсят уязвимости, които недобронамерените хакери могат да използват за събиране на данни и друга разузнавателна информация.

Security Softwear Developer – Разработчиците на софтуер за сигурност са част от екипа на компанията и организацията, отговарящ за програмното осигуряване на нейната дейност. Те разработват съответните програми за сигурност.

Malware Analyst – Анализаторите на злонамерен софтуер следва да притежават знания, които са присъщи на инженерите по информационна сигурност, специалистите по дигитални разследвания и софтуерните разработчици. Основните им функции са да идентифицират и проучват различните форми на зловреден софтуер, а също и да неутрализират начините на тяхното проникване и въздействието им. Този злонамерен софтуер включва разнообразни форми, в т.ч. ботове, грешки, шпионски софтуер, рансъмуер, троянски коне, вируси, червеи и др.

Security Architect – Архитектът по информационна сигурност играе важна роля при изграждането и поддържането на компютърните мрежи. Наред с това част от неговата работа може да включва анализ на риска, сканиране на уязвимости и пенетрейшън тестове.

Други споменати длъжности са: *Security Specialist*, *Security Code Auditor*, *Data Protection Officer*, *Cybercrime Investigator*, *Cryptanalyst*, *Security Incident Responder*, *Chief Privacy Officer*, *Risk Manager*.

В Националния класификатор на професиите и длъжностите (НКПД) в България са включени следните четири длъжности, които имат отношение към информационната и комуникационна сигурност:

- *Експерт, сигурност на информационни и комуникационни технологии*, като в НКПД от 2005 г. наименованието е било *експерт, системно осигуряване и информационна сигурност*. В класификатора от 2005 г. е съществувала и длъжността *специалист, системно осигуряване и информационна сигурност*. В класификатора от 2011 г. тази длъжност е обединена с длъжността на експерта, сигурност на информационни и комуникационни технологии;
- *Консултант, сигурност на данни*, която не е съществувала в НКПД от 2005 г.;
- *Специалисти, компютърни престъпления*, която е добавена в класификатора от 2011 г.;
- *Специалисти, сигурност на данни*, която също е добавена в класификатора от 2011 г.

И четирите от гореизброените длъжности са от групата на специалистите по бази данни и мрежи. В класификатора понятието киберсигурност не се среща.

Обучение по специалности, свързани с киберсигурността – състояние и насоки за подобряване

Дигиталната трансформация поражда търсене на специалисти по киберсигурност. Това поставя изискването пред обучаващите организации и най-вече университетите да осигурят подготовката на такива специалисти, чиито работни задачи могат да варират. Част от тези задачи биха могли да бъдат свързани предимно с управлението, докато друга биха могли да имат чисто технически, софтуерен характер. Във всеки случай съвместно те трябва да допринасят за гарантирането на киберсигурността както на организационно, така и на национално равнище.

Проучването за целите на настоящата публикация показва, че в отговор на тази обективна потребност от висшите учебни заведения в страната са разработени програми за обучение по киберсигурност. През учебната 2020/2021 г. такова се предлага както от държавни университети – УНСС, УниБИТ (информационна сигурност), Висше училище по телекомуникации

и пощи (ВУТП) и др., така и от частни учебни заведения – НБУ, ВСУ „Черноризец Храбър“, Висше училище по сигурност и икономика (ВУСИ) и др.

Интересен е опитът на УНСС, където от учебната 2019/2020 г. стартира двусеместриална магистърска програма „Управление на киберсигурността“. В учебната програма са включени дисциплини, които допринасят за изграждането на мениджъри по киберсигурност, в т.ч.: „Основи на киберсигурността“, „Системи за индустриален контрол (ICS) и SCADA“, „Правни аспекти на киберсигурността“, „Антикризисен мениджмънт в киберсигурност“, „Криптография в киберсигурността“, „AI и киберсигурност“ „Основи на киберразузнаването“, „Добри практики в киберсигурността“, „Интернет сигурност“ и др. Преподавателският екип е съставен от университетски преподаватели и специалисти с богат практически опит в областта на информационните технологии, киберсигурността, управлението и правото.

Обучение по киберсигурност се води и от обучаващи организации от системата на военното образование, в т.ч. ВА „Г. С. Раковски“, ВВМУ „Н. Й. Вапцаров“, факултет „Артилерия, ПВО и КИС“ към НВУ „Васил Левски“.

Обучението в сферата на киберсигурността във висшите учебни заведения се осъществява в трите образователно-квалификационни степени и е с различна продължителност. Така например обучението в ОКС „професионален бакалавър“ е с продължителност 3 години или 6 семестъра. Обучението в ОКС „бакалавър“ е четиригодишно и се осъществява в рамките на 8 семестъра. Всяко висше училище, предлагащо обучение по киберсигурност, е определило различни срокове за обучението в магистърска степен. Забелязват се както едногодишно или двусеместриално обучение, така и двугодишно обучение, провеждано в рамките на 4 семестъра.

Някои обучаващи организации, притежаващи съответната акредитация, подготвят и докторанти в областта на киберсигурността.

Забелязва се разлика в областите на висше образование и професионалните направления, в които се подготвят специалистите по киберсигурност. Те варират както следва: 3. „Социални, стопански и правни науки“ в професионално направление „Икономика“, 4. „Приложни науки, математика и информатика“ в професионално направление „Информатика и компютърни науки“, 5. „Технически науки“ със съответно професионално направление „Комуникационна и компютърна техника“ и 9. „Сигурност и отбрана“ в професионално направление „Национална сигурност“.

Някои работодатели провеждат обучение или сертифициране за служителите си в областта на киберсигурността. Все по-честа практика са и безплатните онлайн ресурси за обучение.

Подготовката на специалисти в областта на компютърните науки, в т.ч. информатика, информационни и комуникационни технологии се осъщест-

вява и в други висши училища, в т.ч. Софийския университет „Св. Климент Охридски“, ВТУ „Св. Кирил и Методий“, техническите университети в страната и т.н. През 2014 г. стартира обучението на програмисти в рамките на СофтУни (Софтуерен университет). Получилите подготовка в тези учебни заведения, както отбелязва в своя интернет публикация Христо Петров, много лесно могат да се преквалифицират в експерти по киберсигурност (Петров, 2020).

Промените в образованието с цел повишаване на неговото качество в различните образователно-квалификационни степени, в т.ч. по специалности, свързани с киберсигурността, е изключително важен и винаги актуален въпрос. *Първо*, той има отношение към националната сигурност, разбирана в най-широк смисъл като качество на човешките ресурси в страната, което е условие за социално-икономическото й развитие. По-високото ниво на подготовка на кадрите означава по-качествена работна сила, по-добро изпълнение на трудовите задачи или изпълнение на задачи с по-висока степен на сложност, съответно постигане на по-добри резултати, което е предпоставка за благоденстващо общество. В контекста на киберсигурността, при равни други условия, това означава по-високи нива при гарантирането на същата и свързаните с това положителни последствия за обществото. От гледна точка на отделната личност и нейната човешка сигурност по-доброто образование е гаранция за успешна професионална реализация, по-висок жизнен стандарт и като цяло по-висока удовлетвореност. *Второ*, качеството на образованието трябва да съответства на ресурсите, които държавата отпуска за неговото развитие, в противен случай ще е налице неефективност и пилеене на средства. *Трето*, качеството на образованието следва да отговаря на очакванията на обучаваните, които често пъти заплащат/инвестират лични финансови ресурси. *Четвърто*, конкуренцията между обучаващите организации в национален и международен план, протичаща на фона на намаляване на броя на потенциалните обучаеми, извежда качеството на образователната услуга като основно преимущество и прави съответното висше училище по-предпочитано пред останалите.

Може да се приеме, че качеството на обучението, колкото и различни разбирания да има за него – било като краен резултат, като процес, като нещо, което се притежава, в т.ч. по специалностите, свързани с киберсигурността, зависи от две групи фактори: *външни* и *вътрешни.*

Външни фактори това са всички условия на средата, в която осъществяват своята дейност образователните организации. Сред тях може да бъдат посочени: световните тенденции в социално-икономическото развитие, достижения на научната мисъл в конкретната сфера, развитие на техниката и технологиите, а също темпа на тяхното навлизане в съответната страна,

цялостната политика на държавата в областта на образованието. Потребностите от кадри, които пазарът на труда поражда в резултат на актуални процеси и тенденции, в най-голяма степен стимулира разкриването и развитието на нови специалности, актуализацията на вече съществуващи, закриването на слаботърсени такива.

Вътрешните фактори за качество, които се проявяват на фона на външните условия, съществуват вътре в самите образователни институции. Сред тях са: *спецификата и организацията на дейността в образователната институция, преподавателите* и *обучаемите.*

А) Специфика и организация на дейността в образователната институция

Образователните институции подготвят кадри, които се реализират в различни сфери на обществения живот. Има високотехнологични области, които се развиват много по-динамично. Този факт влияе върху обучението на кадри, като му дава тласък, поставяйки изискване то също да не изостава и да отговаря на новите потребности. Обучението по киберсигурност в дигиталната епоха е един от примерите за това.

Първата стъпка за постигане на съответствие с потребностите на трудовия пазар е разработването и прилагането на учебни програми, включващи интересни дисциплини, които дават знания и допринасят за придобиването на способности и развитието на компетентности с голяма практическа приложимост. Тези дисциплини следва да бъдат осигурени с актуални литературни и други информационни източници за подготовка, а методите и формите на преподаване да осигуряват добра комуникация и да позволяват активно участие на обучаваните.

Прилагането на съвременни технологии и техника е един съществен видим аспект, допринасящ за по-доброто преподаване и по-лесно усвояване на знания и придобиване на умения от всички, които участват в процеса на обучение. Това е валидно за всички сфери на обучение. Техниката и технологиите предоставят възможност за развитието на онлайн дистанционно обучение, което, при еднаква висока мотивация на преподавателите и студентите, може да бъде също толкова успешно, колкото и традиционното обучение.

За по-високото качество допринася и връзката на обучението с практиката, където съответните знания намират приложение. За повечето специалности, в т.ч. специалностите, свързани с киберсигурността, е немислимо обучение без практическа подготовка. В споменатата в увода анкета връзката на обучението с практиката се определя като един от двата фактора с най-голямо значение за качеството. Така например 75% от анкетираните изразяват мнение, че връзката на обучението с практиката „*има изключително голямо значение*“, а 16,7% посочват, че „*има голямо значение*“.

Включването на обучаваните в изследователски проекти и други проекти с практико-приложен характер, представянето на техни самостоятелни изследвания на различни форуми, е също начини за развитие на обучението в съответната област. В сферата на киберсигурността се забелязва значителна активност по отношение на проекти с различни цели и участие в симулации на учения, кризи и др.

Към всичко това трябва да бъдат добавени и възможности за образователен обмен и специализации в рамките на страната или извън нея, а също включването в преподавателските екипи на хора с различен професионален опит. Разработването на съвместни програми с участието на университети, компании и изследователски звена повишава атрактивността на програмите и придава допълнителна стойност на обучението в тях.

Съществен принос за по-високото качество на обучението, в т.ч. и в рамките на темата за киберсигурността, има ръководството на образователната институция. То задава културата по отношение на качеството на обучението в организацията, предполагаща нагласи, поведение, а също конкретните цели, задачи и ресурси, свързани с него. Организации, в които ръководството акцентира върху качеството, развиват и прилагат активна политика в тази област, гарантираща им рано или късно успех и стабилна позиция на пазара на образователни услуги.

Б) Преподавателите

Въпреки наличието на доста субективизъм при възприемането на преподавателите от страна на обучаемите, влияещ подсъзнателно върху нагласите за работа по определена дисциплина, лекторите са един от факторите, които в най-голяма степен допринасят за качеството на учебния процес. Това се потвърждава и от получените отговори на въпросите от анкетата. Така например 50% от анкетираните са на мнение, че подготовката на преподавателите „*има изключително голямо значение*“ за качеството на обучението по киберсигурност“, а 33,3% считат, че то „*има голямо значение*“. С това този вътрешен фактор се нарежда на трето място сред факторите, влияещи върху качеството.

Без да се претендира за изчерпателност, може да се приеме, че са налице няколко основни неща, които правят преподавателя значим за обучението. Те трудно могат да бъдат степенувани по важност и следва да се разглеждат комплексно.

Първото условие преподавателите да имат принос за развитието на обучението и повишаване на неговото качество, в т.ч. в сферата на киберсигурността, е мотивацията за работа, намираща израз в желание и стремеж за изпълнение на работните задачи и то по възможно най-добър начин. За добро или лошо тази мотивация не е постоянно зададена. Има много обективни и субективни фактори, които ѝ влияят.

Възприемането и демонстрирането на определен тип поведение, което отговаря на упражняваната преподавателска професия, е друг аспект на преподаването, който е свързан с неговото качество. То се усвоява на база наблюдение на поведение на по-опитни колеги, запознаване с писмено разработени кодекси и стандарти, а също на база личности специфики – вродени или придобити в процеса на възпитание и опит.

Често пъти най-голямо значение при преподаването се дава на знанията, които преподавателят притежава. Истината е, че и те са нещо, което, подобно на мотивацията, подлежат на промяна във времето. Има добре подготвени и по-добре подготвени преподаватели, но успешният преподавател е постоянно обучаващия се или самообучаващия се.

Начина на преподаване е друг фактор, който може да допринесе за усвояване на учебния материал и повишаване на качеството на обучението. Участниците в анкетата обръщат голямо внимание на този фактор, поставяйки го на второ място след връзката на обучението с практиката. Според 75% от участниците в анкетата подходите и формите на преподаване имат „*изключително голямо значение*“ за повишаване на качеството на обучението, а за 20,8% от тях те „*имат голямо значение*“.

От една страна, методите и формите на преподаване в рамките на определени направления и дисциплини, в т.ч. свързани с киберсигурността, може да бъдат традиционно зададени. Често пъти, обаче, тяхното прилагане е повлияно от личностните характеристики на преподавателя, неговия опит и не на последно място, от особеностите на обучаемите като група или индивидуалности. Практиката показва, че по-успешни са начините на преподаване, при които се наблюдава добра комуникация и активно участие на обучаемите.

В) Обучаваните

Студентите също са фактор за повишаване качеството на обучението. Тяхната заинтересованост и нагласа към учебния процес, демонстрирани индивидуално или като група, могат да стимулират неговото развитие или забавяне. Най-често заинтересоваността проличава от активността на обучаемите в часовете, от задаваните въпроси, участието им в дискусии, старанието, показано при разработването на самостоятелни задачи, интереса към участие в научноизследователски проекти и др.

Според 29,2% от участниците в анкетата нагласите на студентите „*имат изключително голямо значение*“ за качеството на обучението по киберсигурност, а според 50% този фактор „*има голямо значение*“. Интересно е, че 4,2% от анкетираните споделят мнението, че нагласите на студентите „*имат, но несъществено значение*“ за качеството на обучението.

Заключение

Технологичното развитие изменя ежедневието на хората, правейки го по-динамично, по-усложнено, по-удобно и по-предизвикателно. Технологиите и тяхното приложение в дигиталната епоха, за добро или за лошо, постепенно водят и до промяна в цялостната представа на човека за света и за собственото му място в него.

Едно от нещата, върху които технологичното развитие оказва най-силно влияние, е трудовата дейност на хората. Израз на това влияние става появата на нови професии, трансформацията или отпадането на вече съществуващи.

Търсенето на специалисти, които да притежават знания, умения и компетентности за изпълнение на задачите в рамките на новите професии, поставя големи изисквания към образователната система. Очакванията са тя да ги осигури в съответствие с качествените и количествените потребности. За да ги създаде, образователната система трябва да демонстрира гъвкавост, бързина и същевременно да отговаря на възприетите стандарти за качество и на очакванията на обучаемите.

В условията на ускорена дигитализация киберсигурността придобива изключително голяма значимост. Прилагайки превантивни и реактивни мерки за гарантирането ѝ, организациите се опитват да се противопоставят на съществуващите опасности и заплахи. Конкретен изпълнител на задачите, свързани с това противопоставяне, е персоналът в сферата на киберсигурността. Така въпросът за неговата подготовка остава ключов.

Направеното изследване показа, че в много университети и други образователни звена в страната е разкрито обучение по киберсигурност. То се провежда както в граждански, в т.ч. частни и държавни, така и във военни висши училища.

На този фон много ярко се откроява непрекъсната потребност от повишаване на качеството на обучението. Конкретните мерки предполагат въздействие с оглед промяна на представените и анализирани в изложението на тази публикация фактори.

Сред препоръките за повишаване качеството на обучението, които участниците в анкетата споделят, ясно се открояват две основни: актуалност на преподавания материал, включително и на методите, подходите и проблемите, които се разглеждат и връзка с практиката, като се отчитат спецификата на дейността на организациите.

Използвана литература

НСИ. (2011). Национална класификация на професиите и длъжностите (НКПД). В сила от 1 януари 2011 г., (NSI, 2011, Natsionalna klasifikatsia na profesiite i dlazhnostite (NKPD). V sila ot 1 yanuari 2011 g.), available at: https://www.nsi.bg/sites/default/files/files/pages/Classifics/NKPD-2011_1-928.pdf (accessed 02.04.2021)

Петров, Хр. (2020). Най-добрите БГ университети за киберсигурност обучение през 2020 [Online], (Petrov, Hr., 2020, Nay-dobrite BG universiteti za kibersigurnost obuchenie prez 2020), available at: https://questona.com/kibersigurnost-obuchenie/ (accessed 01.04.2021)

Bowcut, S., Liddle, A. and Contributors. (2021). Guide to Cybersecurity Jobs. Cybersecurity Guide, available at: https://cybersecurityguide.org/resources/cybersecurity-jobs/ (accessed 03.04.2021)

CCCS. (2020). Cyber Security Career Guide, available at: https://cyber.gc.ca/sites/default/files/2020-09/2021-0089-student-guide-e-sept25-2.pdf (accessed 03.04.2021)

ILO. (2016). International Standard Classification of Occupations (ISCO), available at: https://www.ilo.org/public/english/bureau/stat/isco/isco08/index.htm (accessed 05.07.2021)

Morgan, St. (2017). Cybersecurity Jobs Report 2017. Herjavec Group, available at: https://www.herjavecgroup.com/wp-content/uploads/2018/07/HG-and-CV-The-Cybersecurity-Jobs-Report-2017.pdf (accessed 27.03.2021)

World Economic Forum. (2020). The Future Jobs Report 2020, available at: https://www.weforum.org/reports/the-future-of-jobs-report-2020 (accessed 26.01.2021)

Други източници

Сайт на ВА „Г. С. Раковски“, (Sayt na VA „G.S. Rakovski„), available at: https://rndc.bg/

Сайт на ВВМУ „Н.Й.Вапцаров“, (Sayt na VVMU „N.Y.Vaptsarov„), available at: http://www.naval-acad.bg/

Сайт на ВСУ „Черноризец Храбър“, (Sayt na VSU „Chernorizets Hrabar„), available at: https://www.vfu.bg/

Сайт на ВУТП, (Sayt na VUTP), available at: https://www.utp.bg/

Сайт на ВУСИ, (Sayt na VUSI), available at: https://www.vusi.bg/

Сайт на НБУ, (Sayt na NBU), available at: https://www.nbu.bg/

Сайт на НВУ „Васил Левски“, (Sayt na NVU „Vasil Levski„), available at: https://www.nvu.bg/

Сайт на СофтУни, (Sayt na SoftUni), available at: https://about.softuni.bg/

Сайт на ТУ-София, (Sayt na TU-Sofia), available at: https://www.tu-sofia.bg/university/163
Сайт на УниБит, (Sayt na UniBit), available at: https://www.unibit.bg/
Сайт на УНСС, (Sayt na UNSS), available at: https://www.unwe.bg/

***

OCCUPATIONS AND JOBS IN CYBERSECURITY AND RELATED EDUCATION

Assoc. Prof. Konstantin Poudin, PhD
Department of National and Regional Security
Faculty of Economics of Infrastructure
University of National and World Economy
e-mail: kpoudin@unwe.bg

Abstract

New technologies and their implementation into various spheres of human life are followed by a number of changes. Some of these changes are related to the emergence of new occupations and jobs. The paper aims to present the changes in occupations and jobs, as well as in work positions caused by modern socio-economic and technological conditions. These changes inevitably create new requirements for the education and the training in the specialties related to these new occupations and jobs. The focus is on the cybersecurity occupations, the related education and its quality.

Key words: occupations, jobs, cybersecurity, education

JEL: J60, H56