НАУЧНИ ТРУДОВЕ НА УНСС (5) 2024, ИК – УНСС
ISSN (online): 2534-8957; ISSN (print): 0861-9344; http://unwe-research-papers.org/
DOI: https://doi.org/10.37075/RP.2024.5.05

ОСВЕДОМЕНОСТ И ОБУЧЕНИЕ ПО КИБЕРСИГУРНОСТ В УНИВЕРСИТЕТИТЕ В БЪЛГАРИЯ. СЪОТВЕТСТВИЕ С ISO 27001

инж. Елица Павлова[1]
e-mail: epavlova@unwe.bg

Резюме

Това проучване изследва текущото състояние на информираност и обучение по киберсигурност в университетите в България, с акцент върху съответствието със стандартите ISO 27001. С нарастването на цифровизацията необходимостта от стабилни мерки за киберсигурност става критична. Констатациите разкриват различни нива на осведоменост и готовност по отношение на заплахите за киберсигурността, заедно с липсата на стандартизирани програми за обучение. Направена е оценка на съответствието на съществуващите практики с изискванията на ISO 27001 и са идентифицирани пропуски в прилагането на политиката и обучението на служителите. Предоставени са препоръки за подобряване на образованието по киберсигурност, като се подчертава значението на проактивен и всеобхватен подход към киберсигурността в образователните институции.

Ключови думи: осведоменост и онлайн обучение, информационна сигурност, киберсигурност, висше образование, ISO 27001

JEL: A10, F60

Увод

В ерата на технологиите и глобалните икономически промени, висшите учебни заведения в България имат нужда от цялостна програма за осведоменост и обучението за киберсигурност, каквато вече има работеща в много страни. Важно е да се разгледат аспектите на осведомеността и обучението по киберсигурност, както и тяхното съответствие с международните стандарти, като ISO 27001 (ISO/IEC 27001, 2024). Основните цели на програмата за осведоменост за киберсигурност са да защитава репутацията на университета, като осигурява ефективна организационна структура. Киберсигурността е компонент на информационната сигурност и с нея са свързани мерки за защита на информационните активи и степента

[1] Доктор, катедра „Национална и регионална сигурност“, факултет „Икономика на инфраструктурата“, УНСС

на защита, произтичаща от прилагането на тези мерки. Крейгън дефинира „киберсигурността като набор от технологии и процеси, предназначени да защитават компютри, мрежи, програми и данни от атаки и неоторизиран достъп, промяна или унищожаване“ (Aftergood, 2017).

Академичната свобода, откритост и прозрачност са силни норми във висшето образование, но те могат да създадат конфликт, когато се сблъскат с изискванията за киберсигурност. Инструментите за сигурност, които могат да ограничат достъпа към информация или комуникация са не желани, като основната причина за това е свързана с липсата на общи познания за кибератаките. Изследване за киберрисковете показва (Netwrix, 2021), че образователните организации се фокусират повече върху сигурността на своите крайни точки, на предварително разработени системи и виртуални инфраструктури. Областите, които често се пренебрегват включват обучение на служителите, употребата на лични устройства, неструктурирани данни, съхранявани в центрове за данни на трети страни. Университетите често възприемат реактивен подход към киберсигурността, като предприемат мерки едва при установена неизправност или настъпила атака. Проучване за киберсигурността показва, че през 2021 г. висшите образователни институции модернизират инструментите за сигурност на съществуващите ИТ системи, като маркират елементи от контролни списъци за съответствие, вместо да вграждат киберсигурността в своите нови системи и услуги (Mimecast, 2022).

Методологията на изследването включва анализ на предишни проучвания, статии и доклади, свързани с обучителни програми по киберсигурност, както и идентифициране на добри практики, успешни модели и подходи в други университети.

Анализ на литературата е направен на базата на сайта за международно научно цитиране. Ключови думи на търсенето са: осведоменост и обучение, висше образование, университет, информационна сигурност, киберсигурност, ISO 27001/2. „Осведоменост и обучение по киберсигурност“ се открива в заглавията на 453 научни изследвания за последните две години, като най-голям брой от тях са в категория „Образование“ (45,475%), следвани от „Контрол на достъп“ (38,609 %) и „Политики за информационна сигурност“ (27,947%). Това ясно подчертава ролята на обучениетопо темите свързани с информационната сигурност.

Основни теми за осведоменост и обучение

Киберсигурността във висшите учебни заведения се осигурява чрез процеси, които ръководството следва, за да идентифицира, анализира и реагира по подходящ начин на рискове, които могат да влияят неблагоприятно на

организацията. Много университети предлагат курсове по киберсигурност, които обхващат основни концепции, заплахи, уязвимости и защита на данни. Тези програми могат да бъдат задължителни или факултативни и често включват практически занимания. Статията „Защо киберсигурността трябва да бъде приоритет за образователния сектор“, разглежда политиките за информационна сигурност, като списък на ресурсите, които трябва да бъдат защитени, възможните заплахи, оценка на риска и начини за противодействие“ (Swivel Secure, 2021). В нея се казва, че университетите са уязвими към кибератаки поради своята децентрализирана структура, разнообразна група потребители (изследователи, студенти, докторанти, преподаватели, служители и други), различни нива на компетентност и сложна мрежова свързаност на всички устройства.

Докладът „Кибер заплахи за образователната индустрия“ (Fokker, 2021) документира високо ниво на податливост към кибератаки в академичните среди. Изследователите очертават и обсъждат ключови предизвикателства за киберсигурността. Университетите са изложени на киберриск, защото съхраняват масивни архиви от данни. Много системи за контрол са „несигурни по замисъл“, тъй като мерките за киберсигурност не са заложени в процеса на проектиране. В центъра на вниманието са хората и възможностите за тяхното обучение, с което да бъде снижена уязвимостта от кибератаки, загубата на данни или репутация. Анализ на инцидентите показва, че по-голямата част от тях са причинени от социално инженерство и компрометирани потребители. Освен това, уязвимите активи и нарушения на политиките за информационна сигурност представляват над 50% от всички инциденти. Злоупотребите и неволното разкриване на информация се срещат често и почти винаги се дължат на човешки грешки. Заплахите идват в безброй форми и маскировки и именно затова, от решаващо значение е те да бъдат идентифицирани и докладвани навреме.

Сигурността на уебсайтове, приложения и онлайн услуги се превръща в основен приоритет за университетите по целия свят. Доклад за сигурността на софтуера от 2021 г. отбелязва тревожно голям брой уязвимости в сигурността на уеб приложенията (Veracode, 2021). Разбирането на тези уязвимости е от ключово значение за откриването им и защитата на данните. Анализът към доклада показва, че повече от половината от всички прегледани сайтове могат да бъдат компрометирани напълно автоматично. Най-широко разпространените уязвимости са междусайтови скриптове, различни видове изтичане на информация, SQL инжекция, отворена потребителска сесия, грешна автентификация.

Една от възможните стратегии за противодействие на рисковете за киберсигурността е обучението на служителите. В зависимост от целите и

методите, обучението може да бъде структурирано на базата на информираност, изграждане на организационна култура или управление на поведението на персонала. Обучението на базата на информираност се основава на необходимостта служителите да бъдат запознати със съдържанието и изискванията на политиката и програмата за киберсигурност на университета. Основните теми за обучение, описани в статията „Какво представлява обучението по сигурност и защо е важно“ са:

Защита на имейл и социално инженерство. Фишингът се счита за един от най-популярните начини за компрометиране на компютърна мрежа. Нападателите използват различни техники за да подмамят служителите към връзка в имейл или изтегляне на злонамерен прикачен файл. Именно затова, практиките за сигурно сърфиране трябва да бъдат включени в обучението.

Пароли и удостоверяване. Създаването на сложна парола е толкова важно, колкото и нейното запомняне и съхранение. Използването на прости пароли или наличието на разпознаваеми модели улеснява достъпа на киберпрестъпниците, се казва в статията „100-те най-често използвани пароли 2022“ (SecuredYou, 2022). Според проучване, близо 59% от служителите използват една и съща парола за множество акаунти, 60% съобщават, че не променят сложността на паролите си, 53% никога не променят паролата си, ако не се изисква да го правят, а 85% променят паролата си, защото са я забравили (Schneier on Security, 2006).

Внедряването на автоматично генерирани пароли, двуфакторна автентификация и технологии за криптиране, осигуряват допълнителни слоеве на сигурност. Приложенията за управление на пароли решават проблема, като изискват създаването на една главна парола даваща достъп до място, където се пази информация за всички други акаунти. Мениджърите на пароли биват различни типове, като някои се инсталират на компютър и съхраняват данните локално, други са уеб базирани на облачни сървъри, трети могат да запазват биометрични данни. Повечето от тях предлагат междуплатформена поддръжка, предоставяща достъп както през интернет, така и локално (например LastPass, DashLane и 1Password).

Политики за информационна сигурност. Неспазването или заобикалянето на политиките за информационна сигурност е често срещан модел на поведение който не само да намалява ефективността на контрола, но и създава възможности за нови атаки, които не са присъствали преди контрола. Осъзнаване на рисковете от достъп до компютри, информационни ресурси, кражба или копиране на документи оставени без надзор, може да предотврати значителни рискове за сигурността на университетите.

Защита на мобилно устройство. Използването на собствено мобилно устройство е стандарт за висшето образование, където учащите и служите-

лите свързват техните лични устройства към университетската мрежа. През последните години необходимостта от гъвкава работна среда, съчетана с бързото навлизане на нови технологии, повиши риска от пробиви в сигурността. Проблемите възникват, когато мрежата има неподходяща архитектура за сигурност и лоши контролни механизми. Обучението по безопасно използване на преносими носители и мобилни устройства е необходимо за всички служители, независимо дали са лични или корпоративни.

Уеб защита – Wi-Fi, IoT, сигурност на търсачките, работа от разстояние, сигурност в облака. Облачните изчисления промениха начинът, по който данните се съхраняват. Повишаването на знанията на служителите за сигурното използване на базирани на облак приложения, безопасното използване на обществен Wi-Fi, откриването на потенциална измама, споделянето на криптирани файлове и удостоверяването на изтегляния, ще намали риска.

Платформи за обучение по киберсигурност

Съществуват редица платформи за обучение, които позволяват да се осигури непрекъснато обучение и да бъдат постигнати оптимални и дългосрочни резултати чрез възприемане на научен подход. Всички те имат общи теми за осведоменост, но това което ги отличава една от друга е ефикасността и начинът, по който се прилагат на работното място.

Най-популярните платформи за обучение по киберсигурност са:

NINJIO. Платформата предлага обучение чрез кратки анимирани видеоклипове, предназначени да покажат различни сценарии с които служителите могат да се сблъскат, и как да се справят с тях (NINJIO, 2023)Има геймифицирана класация, която насърчава ангажираността. Ключовите характеристики включват частен хостинг портал, интерактивни въпросници, многоезичност и др.

KnowBe4. KnowBe4 осигурява интерактивно обучение за осведоменост по киберсигурност (Knowbe4, 2024). Основни предимства на платформата са многоезична поддръжка за административната конзола и опции за локализация на крайния потребител. KnowBe4 има допълнителни функции за персонализиране, които позволяват геймификация, библиотека с актуално съдържание, статистически данни и графики за обучението.

Cofense. Каталогът на Cofense PhishMe, предлага множество програми със сценарии за симулация на фишинг, прикачени файлове, разнообразно образователно съдържание и най-добри практики въз основа на текущи активни заплахи (Cofense, 2024). Платформата осигурява персонализирано обучение, което позволява на служителите да следват курсовете със свое собствено темпо и обхваща най-добрите практики за отдалечена работа, като кражба на идентификационни данни и социално инженерство.

CybSafe. Платформата осигурява персонализирано обучение за информираност, симулиран фишинг, възможност за установяване на нива на възприемане на риска, съвети за сигурност и актуализации на заплахите (CybSafe, 2024). Ключовите характеристики включват персонализирано и управлявано от данни съдържание, както и сертифицирано обучение.

Proofpoint. Платформата работи с водещи инструменти за разузнаване за заплахи (Proofpoint US, 2024). Обучението включва интерактивно и базирано на игри учебно съдържание, фишинг симулации, инструмент за оценка на знанията на потребителите, който обхваща критичните проблеми със сигурността.

Living Security. Living Security използва геймификация и спомога за предотвратяване на пробиви в киберсигурността (Living Security, 2024). Административният панел предоставя възможност на ръководството да измерва ефективността и напредъка на служителите.

Infosec IQ. Платформата предлага над 2000 ресурса за информираност и обучение (Infosec IQ, 2024). Всеки аспект на обучението може да бъде персонализиран, за да съответства на дадена организация.

Възприемането на задълбочен подход към обучението за информираност за киберсигурността води до промяна на нагласите и вярванията на служителите. Колкото повече са информирани служителите, толкова по-вероятно е те да успеят да защитят информационните активи. Някои служители са изложени на по-голям риск от други за кибератаки. С помощта на прогнозни анализи лесно могат да се идентифицират и наблюдават високорисковите длъжности според специфични маркери. Осведомеността за киберсигурността е ефективна, само когато се прилага на практика. Обратната връзка в реално време показва на служителите възникналите грешки и как да предотвратят подобни ситуации в бъдеще. Програмите за обучение трябва да се провеждат многократно, като същевременно непрекъснато интегрират нови знания.

Предизвикателства и ползи от постигането на съответствие с ISO 27001/2

Киберсигурността в университетите е свързана с прилагане на ефективни практики за управление на данните и подпомагане на членовете на университетската общност за адаптиране към новите технологии. „Най-голямото предизвикателство пред образователните институции е прилагането на сигурността в по-отворена среда. Искаме да си сътрудничим, да споделяме и да бъдем лесно достъпни, а това често е в противоречие със сигурността и защитата на данните“, казва Кийт К. Хартранфт, главен директор по сигурността на информацията в университета Лехиг във Витлеем, Пенсилвания

(Toptal Insights, 2022). От друга страна, конфигурацията на мрежи, в които има голямо сегментиране на системи и данни, увеличават уязвимостта. Това означава по-голяма сложност и висококвалифицирани мрежови специалисти и експерти по сигурност. През последните няколко години сигурността на информационните технологии придоби огромно значение във висшето образование. Някои университети въвеждат нови протоколи и контролни списъци за киберсигурност всеки месец, но тези усилия обикновено водят само до формалното съответствие, а не върху реална устойчивост. Всяка контрола на сигурността принадлежи към конкретна политика. Например достъп до удостоверяване чрез потребителско име и парола е контрола и свързаната с нея политика е дефиниция на това, което прави определени низове от знаци приемливи, като потребителски идентификатор и парола. По същия начин блокирането на сайт е контрола на сигурността, а действителният списък на блокираните сайтове е нейната политика.

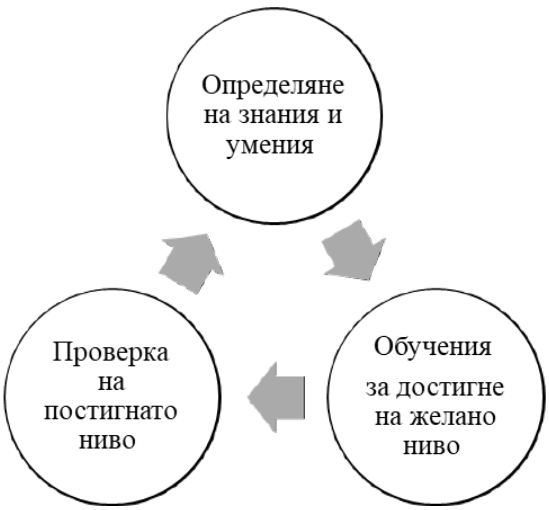
ISO 27001 е международен стандарт за управление на информацията и осигуряване на сигурността на данните. В контекста на университетите той е свързан с:

- Политики за управление на информация: университетите, които се стремят да отговарят на ISO 27001, трябва да разработят политики и процедури за управление на информационната сигурност.
- Оценка на рисковете: стандарта изисква редовни оценки на рисковете, свързани с информационната сигурност, което е важно за идентифициране на уязвимости и прилагане на мерки за защита.
- Обучение на персонала: обучението по киберсигурност трябва да бъде систематично и редовно, за да осигури, че всички служители и студенти са информирани за политиките и практиките на университетите в тази област.
- Мониторинг и подобрения: съответствието с ISO 27001 изисква постоянен мониторинг и оценка на мерките за сигурност, за да се адаптира към новите заплахи и технологии.

ISO/IEC 27001 се базира на процедура за оценка и анализ на риска, насочена към ключовите информационни активи и избор на мерки за минимизация на рисковете до приемливо ниво (ISO, б.д.). Стандартът ISO 27002 е поддържащ документ, който подпомага изпълнението на ISO 27001 и съдържа най-добри практики за това, което влиза в изграждането на цялостна програма за информационна сигурност.

Целта на приложение A.7.2 към ISO 27001/2 е да се гарантира, че служителите и изпълнителите разбират заплахите за информационната сигурност и получават обучение. Клауза 7.2.2 гласи: „Всички служители на организацията и, когато е уместно, изпълнителите, трябва да получават подходящо

информирано образование и обучение и редовни актуализации на организационните политики и процедури, в зависимост от тяхната длъжностна функция“. Клауза А.8.2, посочва обучението за информираност като контрол: Според нея, за да бъде дадена система за сигурност съвместима с ISO 27001 се изисква служителите да познават политиките за информационна сигурност и да могат да откриват и докладват атака по имейл или в мрежата. Обучението трябва да следва цикъла на ISO 27001/2, като първо се определят знанията и уменията, които се изискват за конкретен служител, след това се провеждат обучения за достигне желаното ниво на знания и умения, и накрая се прави проверка чрез тестване, интервюта и т.н.



Източник: Isms.online (2024).

Фигура 1: Цикъл на обучение ISO 27001/2

Университетите трябва да разработят програми за информираност в съответствие с различните роли на служителите в организацията, които да обхващат възникващите заплахи за сигурността и контролите за сигурност към тях. Програмите следва да включват различни форми на обучение, като например информационни бюлетини, компютърно базирано обучение за сигурност, симулирани фишинг упражнения и съвети за киберсигурност. Всички курсове трябва да предоставят показатели за ангажираност или да позволяват персонализиране на модулите. Областта осведоменост и обучение е определяща за това дали преподавателите и служителите получават обучение за киберсигурност и дали могат да изпълняват своите задължения и отговорности в съответствие със съответните политики, процедури и споразумения.

Темата „Осведоменост и обучение“ присъства във всички разгледани стандарти. В таблица 1 са показани нейните подкатегориите и референтните документи към всяка от тях.

Таблица 1: Осведоменост и обучение, подкатегории и референтни документи

Подкатегория	Референтни документи
Обучение по сигурността	CIS CSC 17, 18
	COBITAPO07.03, BAI05.07
	ISO/IEC 27001/2A.7.2.2
	NIST CSF PR.AT-1
Привилегировани потребители и служители	CIS CSC 5, 17, 18
	COBITAPO07.02, APO07.03, DSS06.03
	ISO/IEC 27001/2A.6.1.1,A.7.2.2
	NIST CSF PR.AT-2
Заинтересовани лица от трети страни	CIS CSC 5, 17, 18
	COBITAPO07.03, APO10.04, APO10.05
	ISO/IEC 27001/2A.6.1.1,A.7.2.2
	NIST CSF PR.AT-3

Източник: Собствено проучване

Описанието на референтните документи към всеки стандарт е както следва:

CIS CSC: CIS.5 Сигурна конфигурация за хардуер и софтуер на мобилни устройства, лаптопи, работни станции и сървъри, CIS.17 Прилагане на програма за осведоменост и обучение по сигурността, CIS.18 Сигурност на приложния софтуер.

COBIT: APO07 Управлявани човешки ресурси, APO10 Управлявани доставчици, DSS06 Управлявани контроли за бизнес процеси.

ISO/IEC 27001/2: A.6.1 Вътрешна организация, A.7 Сигурност на човешките ресурси.

NIST CSF: PR.AT-2 Собственост и отговорности, PR.AT-2 Обучение по сигурността.

Основното предимство на внедряването на ISO/IEC 27001 е че, информационният риск се управлява ефективно и ефикасно от гледна точка на вложените средства и изходните данни. Това изисква от организациите да идентифицират рисковете за информационната сигурност и да изберат подходящи контроли за справяне с тях. Стандартът определя и оценява процесите по управление на сигурността на информацията, като същевременно осигурява непрекъсваемост на процесите във всички бизнес направления. Внедряването му отнема време и трябва да бъдат изпълнени всички негови препоръки и политики.

Заключения и препоръки

Висшите учебни заведения трябва да се съсредоточат върху изграждане на програми за обучение по киберсигурност, защото те ще повишат нивата на информираност на членовете на университетската общност и ще им даде практическите умения, необходими за по-добра защита на организацията.

Университетите трябва да разработят програмите за информираност в съответствие с различните роли на служителите в организацията, като са обхванати основните елементи и критични въпроси, свързани с разпространението и прилагането на политиката за информационна сигурност. Платформи като „NINJIO“ или „KnowBe4“ могат да бъдат успешно използвани в кобинация с използване на изкуствен интелект или машинно обучение за наблюдение и прогнозиране на рисковете за киберсигурността в университетите. Прилагането изисква одит на потребителите, а разпространението чрез обучение на служителите е важно, защото заобикалянето често произтича от незнание на потребителя. Обучението трябва да включва различни дигитални форми на онлайн обучение, разширена и виртуална реалност, симулирани фишинг упражнения, сигнали и съвети за киберсигурност.

Подобряването на осведомеността и обучението по киберсигурност в университетите е от съществено значение за защитата на данните и системите. Това може да включва провеждане на редовни оценки на риска или внедряване на система за управление на информация за сигурността и събития. Съответствието с ISO 27001 може да помогне на университетите да структурират своите усилия в тази област, като същевременно осигурят сигурност и защита на информацията на студентите и служителите. Програмите за обучение на служители (например фишинг симулации или семинари за управление на пароли) пряко влияят върху устойчивостта на киберсигурността. Това изисква персонализиране на модулите, чрез показатели за ангажираност. Обучението следва да е непрекъснато и съдържанието да се актуализира редовно, като обхваща възникващите заплахи за сигурността,

пред които е изправена организация, както и контролите за сигурност, които са приложени за защита на информацията.

Използвана литература

Aftergood, S. (2017). Cybersecurity: The cold war online, Nature 547, pp. 30-31, https://doi.org/10.1038/547030a

NINJIO. (2023). All-In-One Cybersecurity Awareness Training Solution, available at: https://ninjio.com/ (accessed 10.16.24).

Cofense. (2024). Phishing Protection Solutions. Cofense, available at: https://cofense.com/ (accessed 10.16.24)

CybSafe. (2024). The Human Risk Management Platform, CybSafe, available at: https://www.cybsafe.com/ (accessed 10.16.24)

Proofpoint US. (2024). Enterprise Cybersecurity Solutions, Services & Training, Proofpoint, available at: https://www.proofpoint.com/us (accessed 10.16.24).

Fokker, J. (2021). Cyber Threat Intelligence Reports, Trellix, available at: https://www.trellix.com/en-us/advanced-research-center/threat-reports/jul-2022.html

Infosec IQ. (2024). Security Awareness Training & Phishing Simulator, Infosec IQ, available at: https://securityiq.infosecinstitute.com/ (accessed 10.16.24)

Isms.online. (2024). The Ultimate Guide to ISO 27001, available at: www.isms.online/iso-27001

ISO. (2024). ISO/IEC 27001. Information technology - Security techniques - Information security management systems - Requirements.

ISO. (n.d.). ISO/IEC 27001:2013, available at: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54534.html

Knowbe4. (2024). Security Awareness Training, Knowbe4, available at: https://www.knowbe4.com (accessed 10.16.24)

Living Security. (2024). Human Risk Management Solution. Living Secure, available at: https://www.livingsecurity.com (accessed 10.16.24)

Mimecast. (2022). What is Security Awareness Training and Why is it Important?, available at: https://www.mimecast.com/content/what-is-security-awareness-training/

Netwrix. (2021). Top Cybersecurity Risks in Education, Netwrix, available at: https://blog.netwrix.com/2017/09/05/infographics-top-cybersecurity-risks-in-education/

Schneier on Security. (2006). The Psychology of Password Generation, available at: https://www.schneier.com/blog/archives/2006/03/the_psychology.html (accessed 5.23.22)

SecuredYou. (2022). The 100 Most Common Used Passwords 2022 - Worst Passwords Ever, available at: https://www.securedyou.com/the-top-100-most-commonly-used-passwords/ (accessed 5.23.22)
Swivel Secure. (2021). Why Cybersecurity Needs To Be a Priority for The Education Sector, Swivel Secure, available at: https://swivelsecure.com/solutions/education/why-cybersecurity-needs-to-be-a-priority-for-the-education-sector/
Toptal Insights. (2022). Cybersecurity in Higher Education: Problems and Solutions, Toptal Insights Blog, available at: https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education
Veracode. (2021). State of Software Security, available at: https://www.veracode.com/state-of-software-security-report

***

AWARENESS AND TRAINING IN CYBERSECURITY AT UNIVERSITIES IN BULGARIA. COMPLIANCE WITH ISO 27001

eng. Elitsa Pavlova, PhD
Department of National and Regional Security
Faculty of Infrastructure Economics
University of National and World Economy
e-mail: epavlova@unwe.bg

Abstract

This study examines the current state of cyber security awareness and training in universities in Bulgaria, with an emphasis on compliance with ISO 27001 standards. As digitization increases, the need for robust cyber security measures becomes critical. The findings reveal varying levels of awareness and preparedness regarding cybersecurity threats, along with a lack of standardized training programs. Compliance of existing practices with ISO 27001 requirements was assessed and gaps in policy implementation and employee training identified. Recommendations for improving cybersecurity education are provided, emphasizing the importance of a proactive and comprehensive approach to cybersecurity in educational institutions.

Keywords: awareness and online learning, information security, cyber security, higher education, ISO 27001

JEL: A10, F60