ON SOME ASPECTS OF THE APPLICATION OF THE CYBERSECURITY DIRECTIVE IN THE ACCOUNTING OF MICRO AND SMALL ENTERPRISES IN BULGARIA

Valentina Staneva
Todor Kableshkov University of Transport – Sofia, Bulgaria, valiastaneva@abv.bg
Hristo Stanev
Higher School of Telecommunications and Posts – Sofia, Bulgaria, h.stanev@utp.bg

Abstract: This study examines some aspects of implementing the Network and Information Security Directive (NIS2 Directive) in the accounting activities of micro and small enterprises in Bulgaria. The Directive was adopted at the end of 2022 and aims to build cybersecurity capabilities in the European Union, limit threats to network and information systems used to provide essential services in key sectors and ensure the continuity of these services in the event of incidents, thereby contributing to the effective functioning of the economy and society. The Directive is mandatory for application from October 18, 2024.
Achieving sustainability in enterprises' development depends on the measures taken to enhance cybersecurity in their activities, including accounting. The study analyzes the application of cybersecurity requirements in protecting sensitive financial information and the effective management of accounting processes in a digital environment. The proposed management solutions are associated with the application of various complex approaches, complementing the requirements of accounting and tax legislation with the new information protection legislation.
Key aspects of implementing appropriate risk management mechanisms related to cybersecurity are examined, including raising awareness of cyber threats and the need to apply new technologies to protect economic information created in the accounting process of micro and small enterprises. The study also considers the challenges faced by enterprises, such as limited resources, lack of specialized IT personnel, and relatively high costs for implementing modern information security solutions.
The aim of this study is to offer practical guidelines and recommendations for adapting the accounting practices in the studied enterprises to the requirements of the directive. Emphasis is placed on the specific characteristics of the studied enterprises, the need for cooperation with technology providers of secure electronic resources, including the use of cloud services.
Keywords: Cybersecurity, Accounting, Micro and small enterprises, Network and information security, Management approaches.

ЗА НЯКОИ АСПЕКТИ ПО ПРИЛОЖЕНИЕ НА ДИРЕКТИВАТА ЗА КИБЕРСИГУРНОСТ В СЧЕТОВОДСТВОТО НА МИКРО И МАЛКИТЕ ПРЕДПРИЯТИЯ В БЪЛГАРИЯ

Валентина Станева
ВТУ „Тодор Каблешков” – София, България, valiastaneva@abv.bg
Христо Станев
Висше училище по телекомуникации и пощи – София, България, h.stanev@utp.bg

Резюме: Настоящето изследване разглежда някои аспекти по прилагането на Директивата за мрежова и информационна сигурност (NIS- 2 Directive) в счетоводната дейност на микро и малките предприятия в България. Директивата е приета в края на 2022 г. и има за цел да изгради способности в областта на киберсигурността в Европейския съюз, да ограничи заплахите за мрежовите и информационните системи, използвани за предоставяне на основни услуги в ключови сектори, и да гарантира непрекъснатостта на тези услуги при инциденти, като по този начин допринася за ефективното функциониране на икономиката и обществото. Директивата е задължителна за приложение, считано от 18 октомври 2024 г.
Постигането на устойчивост в развитието на предприятията се поставя в зависимост от прилаганите мерки за повишаване на киберсигурността при осъществяване на тяхната дейност, в това число и счетоводната. В изследването се анализира прилагането на изискванията за киберсигурност при защита на чувствителната финансова информация и ефективното управление на счетоводните процеси в дигитална среда. Предлаганите управленски решения се свързват с прилагането на различни комплексни подходи, като към

отчитането на изискванията на счетоводното и данъчно законодателство се допълва с прилагането на новото законодателство в областта на защитата на информацията.
Разгледани са ключови аспекти при внедряване на подходящи механизми за управление на риска във връзка с киберсигурността, включително повишаване на осведомеността за киберзаплахите и необходимостта от прилагане на нови технологии за защита на икономическата информация, създавана в счетоводния процес на микро и малките предприятия. Изследването включва и разглеждане на предизвикателствата, пред които са изправени предприятията, като ограничени ресурси, липса на специализиран IT персонал, относително високите разходи за внедряване на съвременни решения за информационна сигурност.
Целта на настоящето изследване е да се предложат практически насоки и препоръки за адаптиране на счетоводната практика в изследваните предприятия към изискванията на директивата. Акцентира се върху особеностите на изследваните предприятия, необходимостта от сътрудничество с технологични доставчици на сигурни електронни ресурси, включително и използване на облачни услуги.
Ключови думи: киберсигурност, счетоводство, микро и малки предприятия, мрежова и информационна сигурност, управленски подходи

1. ВЪВЕДЕНИЕ

Съвременните предизвикателства пред счетоводителите в променящите се икономически условия, обусловени от национални и международни фактори, са свързани с развитието на дигиталните технологии в счетоводството на предприятията. Дигитализацията се наложи в практиката в сравнително кратки срокове в отговор на ограниченията за придвижване на хората по време на пандемията „COVID-19“. Предприятията въведоха електронна обработка и обмен на счетоводната и икономическа информация, позволяваща работа извън офиса (т. нар. home office), с което подобриха и ефективността на труда (Иванова, Р. 2024) при новите предизвикателства. От една страна дигитализацията в счетоводството се наложи като единствено възможно решение за осъществяване на бизнес процесите в извънредни условия, но от друга страна създаде възможности за компрометиране на счетоводните процеси и документи, което изисква да се набележат съответстващи на заплахите мерки. Човешкият „труд също търпи сериозни промени и все по-често се заменя от иновативни технологии и аутсорсване на процесите“ (Банкова, Д, 2020, 2). „Предимствата на технологиите, които ни предоставя дигитализацията, като облачни технологии, база големи данни, интернет на нещата и т.н. водят до спестяване време за клиенти и счетоводители, намаляване на разходи и повишаване качеството на счетоводната работа“ (Илиев, П. 2022, 187). Подетата инициативата през 2022 г. за повишаване на киберсигурността в ЕС се очаква да укрепи колективната устойчивост на Европа срещу киберзаплахи. Приложението на мерките по Пакета от документи (Директиви 2022/2555 и 2022/2057, заедно с Регламент 2022/2557) ще повиши гаранцията за всички граждани и предприятия, да се възползват от сигурни дигитални услуги и инструмент, както и „да подкрепят точното и прозрачно отчитане във връзка с устойчивостта“ (Начкова, М. 2024).
След приемането на нормативната регулация на Европейско ниво чрез Пакета от документи, в страната ни стартира дискусия за обхвата на директивата и необходимостта от обучение за въвежда на изискванията по нея. Изразява се мнение, че новата директива (Мрежова информационна сигурност - МИС 2) изисква от счетоводните фирми, независимо от категорията на предприятието, „да предприемат повече мерки за предотвратяване на нарушения на киберсигурността“.
Принципно, Директива МИС- 2 се прилага за средни и по-големи предприятия (с повече от 50 служители или годишен оборот над 10 милиона евро) в конкретно изброени сектори. Това означава, че всяко предприятие от тези сектори, което покрива критериите, следва да създаде и прилага комплекс от технически, оперативни и организационни мерки. В Директивата няма императивен текст, с който да се определя, че се отнася за счетоводители или счетоводни фирми, но поради широкият обхват на директивата е възможно някои счетоводни фирми да попаднат в нейния обхват.
Статията ще изследва възможностите за приложение на директивата за киберсигурност в счетоводството на микро и малките предприятия в България, които по определение са изключени от приложното ѝ поле. Основната теза е, че чрез подходящи управленски решения и комплексни подходи ще се създават условия за изпълнение на изискванията на новото законодателство в областта на защитата на информацията. Така поставеното предметно поле е достатъчно конкретно, за да отчете използването на системния подход и интердисциплинарния характер на статията. Тематиката е насочена към представителите на различни научни направления – IT специалисти, счетоводители, одитори, финансисти и други.

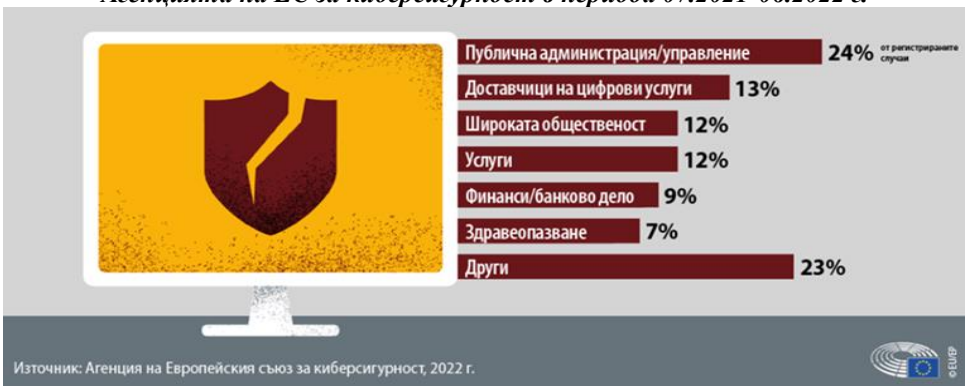
2. ИДЕНТИФИЦИРАНЕ НА ОСНОВНИТЕ ЗАПЛАХИ И КЛЮЧОВИ ДАННИ ПО ПРИЛОЖЕНИЕ НА ДИРЕКТИВАТА ЗА КИБЕРСИГУРНОСТ В СЧЕТОВОДСТВОТО НА МИКРО И МАЛКИТЕ ПРЕДПРИЯТИЯ В БЪЛГАРИЯ

Изследване за периода юни 2021 – юни 2022 г., цитирано от Агенцията на Европейския съюз за киберсигурност (ENISA), идентифицира осем основни заплахи за киберсигурността в ЕС:

- Рансъмуер (Ransomware) - овладяване контрола върху данните на дадено устройство с последващо искане за плащане на определена сума, за да бъде възстановен достъпа до данните;
- Малуер (Malware) – чрез компютърни вируси, червеи, троянски коне и софтуер за шпиониране, се прониква в дадена система за да се използва по друго предназначение (напр. криптоджакинг (тайно използване на процесорна мощ за създаването на криптовалути) или получаване на контрол върху камери или рутери);
- Използване на човешки грешки (Exploiting human errors) – около 60% от пробивите на системи в Европа, Близкия Изток и Африка (Интернет адреса от https://www.europarl.europa.eu/topics/bg/article/20220120STO21428/kibersighurnost-ghlavnite-i-novite-zaplakhi) са свързани с използването на човешки грешки чрез заблуда на потребителите и отваряне на опасен файл или посещение на несигурен уебсайт, се осигурява непозволен достъп до компютърни системи или данни. Най-често подобни атаки започват с изпращането на имейл („фишинг“) или текстови съобщения („смишинг“), които изглеждат като изпратени от официални финансови институции (банки);
- Заплахи спрямо данните (Threats to data) – използват се методи като Ransomware, Malware, Phishing, пробиви (умишлени атаки) или изтичания (неволно изпускане) на данни;
- Заплахи срещу достъпността на данни или услуги (Threats to the availability of data or services) - преустановят достъпа на потребители до информационните им ресурси чрез претоварване на мрежовата инфраструктура или повреждане на системата (т. нар. Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks, Ransomware или Hardware failures);
- Заплахи за достъпа до интернет (Threats to internet access) - поемането на контрол или унищожаването на инфраструктурата за интернет свързаност (пак чрез Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks, Network outages или Government censorship);
- Дезинформация и пропаганда (Disinformation and propaganda) – чрез създаване на фалшиви изображения, видеоклипове или аудиозаписи, които са трудно различими от истинските (напр. ботове се представят за реални публични личности и изпращат множество фалшиви коментари);
- Атаки срещу веригата на доставки (Supply chain attacks) – намесата в бизнес взаимоотношенията между доставчици и клиенти, чрез едновременно атакуване за получаване на икономическа изгода (подканване за плащане по реална фактура но на сметка на трета страна) или опит за влошаване на взаимоотношенията между тях (т. нар. Inserting malicious cod, Compromising third-party services или Exploiting vulnerabilities).

Според други данни в същото изследване, дяловото разпределение на всички случаи на сериозни заплахи, регистрирани от Агенцията на Европейския съюз за киберсигурност между юли 2021 г. и юни 2022 г. са както следва (фиг. 1)

Фигура 1. Разпределение на сериозните заплахи, регистрирани от Агенцията на ЕС за киберсигурност в периода 07.2021-06.2022 г.



Източник: https://www.europarl.europa.eu/topics/bg/article/20220120STO21428/kibersighurnost-ghlavnite-i-novite-zaplakhi.

При сравнение на изискванията по Закона за счетоводството (ЗСч), Препоръка на Комисията от 6 май 2003 г. относно определението за микро, малки и средни предприятия във връзка с въпросите по киберсигурност, както и Директивата за устойчивост се установяват разлики по някои показатели за балансова стойност на активите и нетни приходи от продажби. С приравняване към единна валута, данните са представени в таблица 1:

Таблица 1. Сравнителна таблица за критерии за МСП и микро и малки предприятия по ЗСч и по директивата

Вид предприятие	Показатели	По ЗСч	По препоръка на Комисията	По директивата за устойчивост
Микро	балансова стойност на активите	450 000 EUR	2 000 000 EUR	450 000 EUR
	нетни приходи от продажби	900 000 EUR	2 000 000 EUR	900 000 EUR
	средна численост на персонала	10 души	10 души	10 души
Малко	балансова стойност на активите	5 000 000 EUR	10 000 000 EUR	5 000 000 EUR
	нетни приходи от продажби	10 000 000 EUR	10 000 000 EUR	10 000 000 EUR
	средна численост на персонала	50 души	50 души	50 души
Средно	балансова стойност на активите	25 000 000 EUR	50 000 000 EUR	25 000 000 EUR
	нетни приходи от продажби	50 000 000 EUR	43 000 000 EUR	50 000 000 EUR
	средна численост на персонала	250 души	250 души	250 души

* Директива за устойчивост в статията е Директива 2013/34/ЕС на Европейския парламент и на Съвета от 26 юни 2013 година относно годишните финансови отчети, консолидираните финансови отчети и свързаните доклади на някои видове предприятия и за изменение на Директива 2006/43/ЕО на Европейския парламент и на Съвета и за отмяна на Директиви 78/660/ЕИО и 83/349/ЕИО на Съвета.

Източник: Собствен анализ на авторите на базата на Закон за счетоводството, Препоръка на Комисията и Директива за устойчивост.

Важна особеност е, че в Директивата за устойчивост 2013/34/ЕС на Европейския парламент и на Съвета в частта за България като обхват на предприятия са включени следните търговски дружества:
- по Приложение I - акционерно дружество, дружество с ограничена отговорност и командитно дружество с акции;
- по Приложение II - събирателно и командитно дружество.

От това следва, че в обхвата по приложение на Директива за устойчивост не попада търговско дружество с променлив капитал, Едноличен търговец и Държавно предприятие (създадено със закон по реда на чл. 62, ал. 3 от Търговския закон).

След тези уточнения се вижда, че микро и средните предприятия в България не отговарят на две от условията по Директива МИС 2, докато малкото предприятие не отговаря само на условието за балансова стойност на активите. Общото в сравняваните нормативни документи в таблица 1 е критерият численост на персонала, където не са открити разлики за различните категории предприятия.

Друга особеност е, че счетоводните къщи и предприятията с основен предмет на дейност предоставяне на счетоводни услуги най-често попадат в категорията на микропредприятията, със среден брой служители до 10. „Малките организации, поради по-ограничените си ресурси, са с относително по-слаби или липсващи контроли за киберсигурност“ (Мусов, М. 2020, стр. 160). В редки случаи има предприятия, които отговарят на изискванията за малки и средни предприятия, но определено за да са успешни, при тях се създават всички условия за съхраняване на критичната информация, съхранявана във връзка с извършваните счетоводни услуги.

3. РЕЗУЛТАТИ И ДИСКУСИЯ

Познаването на киберзаплахите е първата стъпка към ефективна защита от тях. От идентифицираните осем основни заплахи за киберсигурността в ЕС, с най-висок процент на проявление (60 %) се явяват човешките грешки. Всъщност, това е основната заплаха към микро и малките предприятия в България, които не разполагат със специалисти от IT сектора. Разбираемо е, че разходите за труд, хардуер и софтуер в тяхната комплексност за работа в среда с високи нива на киберзаплахи е трудно и скъпо за изпълнение в предприятия от категорията на микро предприятията, и постижимо със съразмерни усилия за малките предприятия. Това, че микропредприятията не са обхванати от приложното поле на Закона за киберсигурност и Директива МИС 2, не означава, че те не са застрашени от последствията на целенасочени или случайни киберинциденти.

В епохата на цифровите технологии е от съществено значение във всяко микро и малко предприятие да е създадена и изпълнявана организация за киберсигурност. Работата в дигитална среда е свързана с потенциални рискове от изтичане или загубване на контрола върху създадената счетоводна информация. В тази връзка следва да се предприемат стъпки за създаване на адекватна киберзащита, съобразена с финансовите възможности на отделното предприятие. Тези стъпки стават най-видими и полезни преди настъпването на „сериозен инцидент“ с обработваните за счетоводни цели данни. В Директива МИС 2 не се споменават изрично счетоводните къщи и/или предприятия, като самостоятелни субекти, които обслужват голям брой микро, малки и средни предприятия. В тяхната съвкупност, в теоретичен аспект, като се има предвид широкият обхват на документа, е възможно някои от тях да достигнат критериите по Директива МИС 2, особено когато обслужват средни и големи предприятия от изброените в директивата критични сектори, като по този начин да попаднат в нейния обхват. Това положение е практически възможно като изключение за счетоводните къщи само при едновременно покриване на критериите за малко предприятие – нетни приходи от продажби в размер на 10 млн. Евро и средносписъчен състав от 50 души.

Важна особеност, продиктувана от нормата в чл. 12 на Закона за счетоводството е задължението на предприятията да съхраняват определени счетоводни документи на хартиен и/или на технически носител в следните срокове, считано от 1 януари на отчетния период, следващ отчетния период:

- ведомости за заплати - 50 години;
- счетоводни регистри и финансови отчети, включително документи за данъчен контрол, одит и последващи финансови инспекции - 10 години;
- всички останали носители на счетоводна информация - три години.

Кибератаките потенциално могат да навредят на техническите носители, съхраняващи тези документи, ако имат свободен достъп до интернет или не се прилагат мерки за киберзащита съгласно приетите в предприятието политики за киберсигурност. Съгласно изискванията на Кодекса на труда, считано от 01.01.2024 г, по писмено искане на работника или служителя, трудовото му възнаграждение се превежда по негова платежна сметка. Тази промяна поставя началото на дискусия за необходимостта от съхраняване на счетоводни документи, които вече не се съставят и подписват на хартиен носител, като например ведомост за заплати. Предложението ни е да се преразгледа въпроса за съхраняване и архивиране само на ведомости за заплати за срок от 50 години, доколкото ведомостта при превеждане на трудово възнаграждение по платежна сметка не изисква нейното подписване от работниците и служителите.

По отношение на необходимостта от повишаване на киберзащитата в счетоводството на микро и малките предприятия в България е удачно да се отбележи, че това може да се постигне с набелязването на организационни и технически мерки, които са лесни за изпълнение и съответстват като минимално ниво на защита, осигурявано за нуждите на отделния потребител на информационни ресурси. При организационните мерки следва да се идентифицират критичните процеси и ресурси в предприятието, възможните заплахи и пропуски в киберсигурността, техническите характеристики на хардуера и възможностите на използвания софтуер. Не е без значение и въвеждането на Политики за киберсигурност, чрез които да се осигури защита чрез управление на достъпа до информационните масиви, обучение на персонала за възможните киберзаплахи и начина за предпазване от тях. Защитата на чувствителните данни следва да се организира чрез тяхното криптиране, както и чрез създаване на резервни копия на данните (т.нар. backup). Добър подход е обучението и натоварването на служител със задачи по установяване на инциденти, предприемане на контрамерки и възстановяване на сигурното състояние на информационните системи. По отношение на техническите мерки може да се създаде защита на достъпа чрез сложни пароли, четци на биометрични данни, инсталиране на антивирусни програми и защитна стена, както и предприемане на мерки за защита на безжичния интернет.

4. ЗАКЛЮЧЕНИЕ

В заключение следва да се открояят някои важни аспекти от приложението на Директивата за киберсигурност в счетоводството на микро и малките предприятия в България. Констатира се различие в критериите за определяне на категорията предприятия микро, малки и средни, използвани в различни документи на ЕС, което създава предпоставки за неедноznачно определяне на предприятията, задължени да прилагат различните директиви и регламенти.

Налага се извода, че има необходимост от актуализиране на текстове в Закона за счетоводството, в частта за сроковете за съхранение на документи, по-точно с ведомостите за заплати, които след въвеждане на преводи на възнагражденията по платежни сметки, реално не се подписват от работниците и служителите в предприятието. Дигитализацията създаде нови условия за прилагане на електронни документи в рамките на

„безхартиеното счетоводство“, съхранявани на технически носители на информация, които не са упоменати в Закона за счетоводството.

По отношение на приложението на Директивата за киберсигурност в счетоводството на микро и малките предприятия в България, се установява, че тя не е задължителна за микро предприятията, както и за счетоводните предприятия (къщи), които поради естеството на работа и размерите на нетните приходи от дейността им най-често не покриват критериите по директивата. Приложението на организационни и технически мерки за предотвратяване на кибератаки, заедно с приоритетното финансиране на дейностите в областта на киберсигурността са предпоставките за изпълнение на изискванията на нормативните документи на европейско и национално ниво.

СПИСЪК С ИЗТОЧНИЦИ

Банкова, Д. (2020). Относно киберсигурността в предприятията. Електронно списание на ИДЕС, София, бр. 1, ISSN 1314-8990 (online), 1-14.

Вейсел, А. (2023). Влиянието на изкуствения интелект върху счетоводството. Електронно списание на ИДЕС, София, бр. 3, ISSN 1314-8990 (online), 1-13.

Ursillo, St. Jr., Arnold. C. (2023). Киберсигурността е от решаващо значение за всички организации – големи и малки. Електронно списание на ИДЕС, София, бр. 3, ISSN 1314-8990 (online), 1-9.

Мусов, М. (2020). Управлението на киберриска и счетоводната професия. Научни трудове на УНСС, кн. 4, 159-191.

Начкова, М. (2024). Specific disclosures in the pension fund sustainability report (Специфични оповестявания в доклада за устойчивост на пенсионните фондове), 17 conference „Vanguard scientific instruments in management“, Равда, 10-15.09.2024 г., електронно списание, http://vsim-conf.info.

Ivanova, R. (2024). The productivity of labor and the cost of live labor in the industry of Bulgaria as objects and direct factors in economic analysis. 17 conference „Vanguard scientific instruments in management“, Равда, 10-15.09.2024 г., електронно списание, http://vsim-conf.info.

Илиев, П. (2022). Съвременният контрол в ерата на дигитализацията. София, Болид-инс, ISBN 978-954-394-27-7-0. 1-294.

Танев, Я. Митев, М. (2024). Новата Европейска политика за киберсигурност в българската държавна администрация. София, Институт по публична администрация, ISBN 978-619-7262-52-0.

Актуализирана Национална стратегия за киберсигурност „КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2023 ”. (2021). Министерски съвет на Република България. https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg- BG&Id=1587

Европейски парламент. (2022). Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерките за високо общо ниво на киберсигурност в целия Съюз, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (NIS 2 директива), обн. ОВ L 333, 27.12.2022 г. https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32022L2555&qid=1732563250519

Европейски парламент. (2022). Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 година за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета, обн. ОВ L 333, 27.12.2022 г. https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32022L2557&qid=1732563310628

Европейски парламент. (2022). Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 година относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011. https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32022R2554&qid=1732563559795

Европейска комисия. (2003). Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. ОВ L 124/20 May 2003.

Европейски парламент. (2013). Директива 2013/34/ЕС на Европейския парламент и на Съвета от 26 юни 2013 година относно годишните финансови отчети, консолидираните финансови отчети и свързаните доклади на някои видове предприятия и за изменение на Директива 2006/43/ЕО на Европейския парламент и на Съвета и за отмяна на Директиви 78/660/ЕИО и 83/349/ЕИО на Съвета. https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32013L0034&qid=1732563802916.

ENISA (European Union Agency for Cybersecurity). (2021). Cybersecurity for SMES - Challenges and Recommendations, ENISA. ISBN: 978-92-9204-409-1. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes.

Народно събрание на Република България. (2018). Закон за киберсигурност. Обн. ДВ бр. 94/13.11.2018 г., посл. изм. ДВ бр. 25/29.03.2022 г. https://lex.bg/en/laws/ldoc/2137188253

Народно събрание на Република България. (2015). Закон за счетоводството. Обн. ДВ бр. 95/08.12.2015 г., посл. изм. ДВ бр. 79/17.09.2024 г. https://lex.bg/bg/laws/ldoc/2136697598