УЯЗВИМОСТИ В КИБЕРПРОСТРАНСТВОТО И ВЪЗДЕЙСТВИЕТО ИМ ВЪРХУ МСП

Бетина Диянова Минкова
Е-поща: betina.minkova@ue-varna.bg
Докторант в докторска програма „Световно стопанство и МИО“
Икономически университет - Варна

Резюме: Настоящата разработка цели излагането на кратък теоретичен преглед на кибер уязвимостите, които оказват влияние на малките и средни предприятия (МСП), както и последващите икономически ефекти. Заложената цел е да бъдат анализирани най-честите уязвимости в системите за киберсигурност, като в резултат на това да бъдат изведени препоръки за подобряване на дигиталната защита. Подходът включва анализ на вторични източници, тематичен преглед на наличната литература и оценка на риска чрез опростен икономически модел. По презумпция МСП, които не имплементират базови методи за киберсигурност, са уязвими на всички видове произтичащи заплахи. Малките и средни предприятия често не възприемат киберсигурността като приоритет, което ги различава от големите организации, разполагащи с големи бюджети и специализирани екипи.

Ключови думи: киберсигурност, уязвимости, МСП
JEL: F23, F59, M15
DOI: 10.58861/tae.grdier.2025.07

Тази статия се цитира по APA стил, както следва: Минкова, Б. (2025). Уязвимости в киберпространството и въздействието им върху МСП. *Глобални и регионални измерения на международните икономически отношения,* (2), 92-104. DOI: 10.58861/tae.grdier.2025.07.

VULNERABILITIES IN THE CYBERSPACE AND THEIR IMPACT ON SMES

Betina Diyanova Minkova
E-mail: betina.minkova@ue-varna.bg
Doctoral student in World Economy and International Economic Relations Doctoral Program
University of Economics - Varna

Abstract: This article is intended to provide a brief theoretical overview of the cyber vulnerabilities that affect small and medium-sized enterprises (SMEs), as well as the subsequent economic impacts. The main objective is to analyze the most common vulnerabilities in cybersecurity systems, and as a result, to formulate recommendations for improving digital protection. The approach includes an analysis of secondary sources, a thematic review of the available literature, and a risk assessment using a simplified economic model. By default, SMEs that do not implement basic cybersecurity measures are vulnerable to all types of emerging threats. Small and medium-sized enterprises often do not treat cybersecurity as a priority, which differentiates them from larger organizations that have substantial budgets and specialized teams.

Key words: cybersecurity, vulnerabilities, SME
JEL: F23, F59, M15
DOI: 10.58861/tae.grdier.2025.07

This article shall be cited in APA style as: Minkova, B. (2025). Vulnerabilities in the cyberspace and their impact on SMEs. *Global and regional dimensions of international economic relations*, (2), 92-104. DOI: 10.58861/tae.grdier.2025.07.

Въведение

Съвременната икономическа сцена представлява мултимодално поле на изява, в което множество независими играчи обменят информационни потоци в дигитален и аналогов формат. Същото съвремие, в което социално и икономически оставяме своята историческа следа, се характеризира с условия, доминирани от несигурност, турбулентност и агресивна конкурентност. Несъмнено последните десетилетия от най-новата ни история регистрират безпрецедентното влияние на Интернет и киберпространството като новите фактори на влияние, причиняващи непрекъснати подбуди за бърза адаптация. В тази глобална обстановка на интензивни промени и преливащи потоци от информация, бизнес средата предлага изобилие от възможности, но и същевременно безброй предизвикателства, които изострят вниманието на всички участници. Далеч от зоната на предсказуемото остават познатите методи на прогнозирането, като най-добрата подготовка за посрещането на пазарните предизвикателства е критичният поглед върху заобикалящата ни информация. Именно този аспект на нашето съвремие отваря нова страница за настоящите бизнес агенти, за които всекидневното оцеляване е плод не само на добро маркетингово планиране, но и на стратегическо управление на множеството рискове, произлизащи от новата дигитална реалност.

С усложняването на световния кибертерен предизвикателствата пред всички видове информация придобиват нови и нови измерения, принуждавайки бизнеса да подхожда все по-осторожно спрямо своята защита от потенциални атаки. Това от своя страна поставя акцента върху актуалността на информационната сигурност, която придобива все по-съществена роля в полезрението на множество и най-разнообразни международни организации.

Пример за това е именно докладът за глобалните рискове *The Global Risks Report* на Световния икономически форум, който още през 2018г. отразява съществения ръст на кибератаките, нареждайки ги на трето място по вероятност след промените в климата и природните бедствия (WEF, 2018). В същия документ

се посочва още, че киберзависимостта представлява втория най-значим двигател на глобалните рискове за следващите 10 години.

На този фон МСП не остават незасегнати, като тяхната уязвимост често се превръща в мишена за атаки на чувствителни данни и други нематериални активи.

1. Теоретична постановка на киберсигурността

Условията, в което функционират съвременните икономически агенти, са силно обвързани с обработката на информация в дигитален аспект. Това предизвиква появата на т.н. *кибер ера*, където водещи са електронните технологии и компютърните мрежи, свързващи милиарди устройства от цял свят посредством Интернет. Всичко това способства възникването на непознати досега икономически сектори и дори индустрии, които се характеризират с висок потенциал и трайни пазарни намерения. Едно от тях е именно полето на киберсигурността, което се оказва с главна роля в дигиталното благосъстояние на немалък брой икономически агенти. На представителите на този нововъзникнал дял на информационните технологии се приписват заслугите за организирането на ефективна и навременна сигурност, която е необходимо условие за съществуване на всеки, който желае да бъде активен участник в настоящите световни процеси. В този смисъл киберсигурността е необходима категория от най-новата история на света, която заема стратегическо място в дългосрочното и устойчиво на външни трусове управление на всяка структурна единица.

Киберсигурността се основава на ефективно изграждане и поддръжка на активни и превантивни мерки с цел защита на информацията в дигитален формат. В основата на тази категория се намира намерението за гарантиране на конфиденциалността, целостта и достъпността на цифровата информация, което е по-познато като *CIA триада* (confidentiality - предотвратяване на неоторизиран достъп до информация; integrity - защита срещу неоторизирани промени по съдържанието и целостта на информацията; availability - осигуряване на мигновен достъп до информацията при необходимост от такъв).

Законът за киберсигурност на Р България дефинира киберсигурността като състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат

да нарушат работата им. В по-широк мащаб, позовавайки се на едни от докладите на Международния телекомуникационен съюз (International Telecommunication Union) от 2008 г., можем да определим киберсигурността като процес по събиране на инструменти, политики, концепции, предпазни мерки, насоки, подходи за управление на риска, действия, обучение, най-добри практики, осигуряване и технологии, които могат да бъдат използвани за защита на киберсредата, организацията и активите на потребителя (ITU, 2008).

С оглед на гореизложеното се предлага следната авторова дефиниция за киберсигурност: „*Комплекс от методи, техники и инструменти, насочени към обезпечаването и гаранцията сигурността мрежи, устройства и данни от неоторизиран достъп, атаки, повреди или унищожаване*“.

2. Предизвикателства пред сигурността на информацията

Предвид чувствителността на информацията като актив съществуват множество заплахи от дигитален и аналогов тип, които представляват потенциално зловредно действие върху нейните *конфиденциалност, цялост и наличност*. Точният брой на разновидностите им постоянно търпи промени поради развитието на нови и нови технологии, като често само техниката на действие разделя едни методи от други. Така или иначе общата цел е придобиването/изменението на информация от страна на трето лице, върху която извършителят няма регламентиран достъп, като това може да бъде направено с намерението за лична изгода или нанасянето на репутационни/финансови щети. В аспекта на киберсигурността най-често срещаните заплахи са именно тези, свързани с дигиталната защита на информацията, като не рядко инциденти се случват и поради човешка грешка или невнимание. На следващите редове са изложени най-често срещаните заплахи пред сигурността на информационните активи.

Зловредният софтуер (malware, съкращение от malicious software) представлява продукт на софтуерен код/програма, който е създаден с цел да нанесе поражения върху случайно или предварително дефинирана компютърна система и нейните потребители. Обикновено този процес е дело на хакери или други киберпрестъпници, които целят: получаването на неоторизиран достъп до чувствителна информация или дистанционното управляване на компютърни

системи (вкл. тяхното повреждане/ унищожаване). Най-често това се прави с идеята за: изнудване или изискване на подкуп за връщането на придобити файлове, получаване на неоторизиран достъп до чувствителни данни или цифрови активи, кражба на идентификационни данни за вход, номера на кредитни карти, интелектуална собственост или друга ценна информация, прекъсване на критични системи. Компаниите често притежават значителни количества лични данни, което се използва от хакерите като благоприятна среда за изнудване. Впоследствие придобитите лични данни могат да бъдат използвани за престъпления като кражба на самоличност или продажба в рамките на т.н. тъмна мрежа (dark web).

Фишингът (phishing) е един от най-популярните методи за кибератака, които се характеризират с висока степен на успеваемост. По същество терминът би могъл да бъде определен като имейл, текстово или гласово съобщение, което подвежда потребителите да споделят чувствителна информация, да отговарят съмнителни файлове, да изпращат средства или да изтеглят специфичен софтуер с нерегламентирани цели. В обществените среди вече са познати т.н. групови фишинг измами, които се проявяват в масово разпращане на измамни съобщения от името на познати брандове с молба към получателите да подновят паролите си или да въведат отново информация за плащане (най-често номера на кредитни карти). Съществуват и друг вид фишинг измами с корпоративна насоченост (BEC, business email compromise), които „атакуват“ служителите на организации с цел достъпване фирмените бази с клиентски данни. Би могло да се каже, че най-важните инструменти за изпълнението на успешната фишинг кампания са именно креативността на поднасяне на съобщението, както и нивото на психологическа манипулация, което зависи най-вече от доброто познаване на потенциалната жертва.

В най-общ план *социалното инженерство* (social engineering) представлява негативен резултат от човешка грешка или немарливост по отношение на информацията, като това най-често е с непреднамерен характер. Подвеждането може да се случаи по множество канали, като едни от най-често срещаните са свързани с доверяване на фалшиви истории (напр. превеждане на пари за социална кампания), плащане на фактури на лица с фалшива самоличност, предоставяне на физически и дигитален достъп до информация на лица без право на такъв и др. Би могло да се каже, че за киберпрестъпниците социалното инженерство

представлява един изключително привлекателен начин за осигуряване на иначе трудно проходим достъп до цифрови мрежи, устройства и акаунти без да се налага да инвестират техническо време в заобикалянето на защитни стени, антивирусен софтуер и други контроли за информационна сигурност. Представяйки се за нов служител на компанията или член на проверяваща комисия, този тип недоброжелатели могат да си осигурят достъп и до физически налична документация, което, разбира се, се случва благодарение на слабости във вниманието на служителите. Добре познати методи за „пробив“ са: представяне за доверен бранд/ популярно лице, представяне за правителствена агенция/ авторитетна фигура, предизвикване на страх/ чувство за неотложност, щедри обещания и предлагане на големи награди, покана за участие в проучване, призив за помощ и др.

С представянето на последните логично следва да се споменат и т.н. *вътрешни заплахи* (insider threats), които произхождат от упълномощени потребители, изпълнители и най-вече служители, които (не)умишлено злоупотребяват със законния си достъп или притежаването на акаунти, като ги предоставят на киберпрестъпници. Благодарение на това, този тип събития са по-трудни за откриване от другите заплахи, тъй като привидно не притежават подсказващи белези и не могат да бъдат засечени от софтуер, защитни стени или други решения за сигурност, предназначени за външните атаки. Най-често участници в подобен тип заплахи са недоволни бивши служители на компанията (чиито идентификационни данни за достъп не са били извзети), които умишлено злоупотребяват с достъпите си с цел отмъщение, финансова печалба или кражба на ноу-хау. В други случаи злонамерени настоящи служители „работят“ за трето лице (хакер, конкурент), като нарушават нормалното функциониране на бизнес процесите (инсталират зловреден софтуер или подправят файлове/приложения) или извличат информация за клиенти, интелектуална собственост, търговски тайни и т.н.

Друга често срещана заплаха е *кражбата на идентификационни данни* (credentials theft), което обикновено бива последвано от *злоупотребата с потребителски акаунти* (account abuse). Практиката показва, че атаките, базирани на самоличност, представляват най-честата входна точка в корпоративните мрежи. Доказателство за това са последните резултати на индекса за разузнаване на

заплахите X-Force, изчислен от IBM, според който кражбата на идентификационни данни/акаунти представлява 30% от всички дигитални атаки (IBM, 2024). Това се дължи на факта, че използваните за целта техники и технологии се развиват експоненциално за разлика от подготовката на потенциалните жертви, които в повечето случаи разбират за съществуването на процеса след появата на фактически резултат.

3. Киберсигурност и МСП

Все по-често срещано е схващането, че съществува назряваща фрагментация и неравенство между организациите, които инвестират в информационна сигурност и тези, които не го правят – явление, което се случва на фона на развиващите се технологии и различни нива на осъзнатост по отношение на въпросите, свързани с информационната сигурност. В тази посока на разсъждение доклад на Световния икономически форум (World Economic Forum), озаглавен „Перспектива на глобалната киберсигурност" извежда някои актуални към 2024 г. ключови констатации, а именно: (1) Дълготрайно обостряне на предизвикателствата, свързани с киберустойчивостта благодарение на непрестанното въвеждане на нови технологии; (2) Разширяване на празното пространство, свързано с недостига на подготвени кадри в областта на дигиталната сигурност; (3) Нарастващо неравенство между големите корпорации и МСП по отношение на информационната сигурност, като първите са значително по-подготвени и технически обезпечени; (4) Повече от половината анкетирани за целите на доклада МСП отбелязват, че не се чувстват уверени в притежаването на необходимите умения за справяне с киберпредизвикателствата; (5) 52% от анкетираните за целите на доклада обществени организации заявяват, че липсата на ресурси и умения е най-голямото им предизвикателство при проектирането за киберустойчивост; (6) 29% от анкетираните за целите на доклада организации съобщават, че са били съществено засегнати от инцидент, свързан със сигурността на информационните им активи през последните 12 месеца, като 41% от тях потвърждават, че инцидентът е бил предизвикан от трета страна; (7) 54% от анкетираните за целите на доклада организации регистрират недостатъчно разбиране относно последствията от киберуязвимостите за цялостта на веригите за доставка; (8) 90% от лидерите, присъствали на последната Годишна среща за

киберсигурност вярват, че неравенството в киберустойчивостта на компаниите изисква спешни действия (WEF, 2024).

Всичко дотук доказва, че информационната сигурност като услуга придобива все по-голяма актуалност за организации от всякакъв род, но докато големите корпорации могат да си позволят отделянето на финансов ресурс за поддържането на собствени единици, посветени на информационна сигурност, МСП предпочитат да спестят този разход. Това от своя страна резултира в проявата на ниска устойчивост на организацията, която при потенциална поява на инцидент, следва да заплати не само материални, но и репутационни разходи. Именно поради факта, че малките бизнес организации не инвестират достатъчно в своята информационна сигурност, лесно се превръщат в ярко оцветена цял за техните недоброжелатели.

От друга страна при адекватно приоритизиране на бюджета и инвестиране в информационна сигурност може да се очаква възвращаемост, породена най-вече от нарастващото потребителско доверие. Точно затова би могло да се каже, че сигурността на компанията може да се разглежда и като рекламен инструмент, особено в индустрии, където този аспект е с особен приоритет (финансово-счетоводни услуги, здравеопазване, държавна администрация и т.н.). Преди всичко, обаче, информационната сигурност представлява една добра застраховка срещу икономическите последици, които в повечето случаи се оказват пагубни за по-малките организации и подлагат на въпрос тяхното оцеляване.

4. Икономически последици за МСП в следствие на кибер уязвимости

Уязвимостите за МСП далеч не са имагинерно понятие от теоретичен характер, взимайки предвид презумпцията, че компании от този тип не разполагат с необходимото техническо, финансово, кадрово, но и информационно-образователно обезпечаване. Обикновено мениджърите, които в повечето случаи са и собственици, се концентрират върху звена, свързани с ежедневното функциониране на бизнеса като: производство, снабдяване и пласмент, дистрибуция и маркетинг, клиентско обслужване и т.н. Извън обсега на внимание остават аспекти като киберсигурността и застраховането срещу киберинциденти, които в повечето случаи се превръщат в необходимост след възникването на конкретен инцидент.

В контекста на киберсигурността уязвимостите представляват слабости в системите, процесите или поведението на служителите, които могат да бъдат използвани от злонамерени субекти за фактическо имплементиране на киберзаплахи и кибератаки. В най-общ план биха могли да бъдат разделени на следните три групи - технически, организационни и човешки. Най-често срещаните уязвимости са изобразени в табл. 1.

Таблица 1. Уязвимости в контекста на киберсигурността

Вид уязвимост	***Същност***	***Пример***	***Икономически последици***
I. Необновен или остарял софтуер	Оперативно използване на остарели версии на операционни системи и приложения без редовна актуализация.	Фирмен сайт е хакнат поради остаряла версия на PHP-базирана система, което води до подмяна на съдържанието със зловреден софтуер. Google блокира сайта, което води до рязък спад на посещаемостта от клиенти.	**Преки разходи**: възстановяване на уебсайта от ИТ специалист **Косвени разходи**: блокирани продажби, намалено онлайн присъствие
II. Липса на резервни копия	Липса на внедрени процедури и политики за създаване на резервни (бекъп) файлове на чувствителни данни от стратегическо значение, което означава, че при кибератака могат да бъдат заличени завинаги.	Счетоводна агенция става жертва на рансъмуер, с което всички клиентски данни са криптирани. Поради липса на бекъп, те са принудени да платят откуп със сериозна сума, но въпреки това не получават всички данни обратно.	**Преки разходи**: паричен откуп, разходи за възстановяване **Косвени разходи**: загуба на клиенти и обществено доверие
III. Слаби пароли и липса на двуфакторна автентика-ция (2FA)	Използване на предсказуеми и лесно генерирани пароли ("123456", "password", името на фирмата и др.), които в много случаи използват за достъп до множество системи, което увеличава риска при пробив. Допълнително, липсата на двуфакторна автентикация прави достъпа до акаунти още по-лесен за злонамерени лица.	Хакер получава достъп до управленски имейл чрез изтекла парола от предишен пробив в трета платформа. След това използва имейла за разпращане на фишинг писма от името на фирмата, което води до срив в доверието на клиентите.	**Преки разходи**: техническо възстановяване на собствеността върху имейла **Косвени разходи**: загуба на клиенти и обществено доверие

IV. Липса на обучение и осведоменост сред персонала	Нерядко човешкият фактор представлява най-слабото звено в системата на организацията. Без основни познания по киберсигурност са способни да отворят фишинг линк, да изтеглят заразен файл или да разкрият чувствителна информация.	Служител получава имейл от „доставчик“, в който се изисква повторно потвърждение на плащане. След отваряне на прикачения файл или линк, мрежата на фирмата е компрометирана.	**Преки разходи**: неправомерен превод на средства, разследване на случая **Косвени разходи**: влошени отношения с реалния доставчик
V. Липса на политики и процедури по сигурност	Липса на официализирани процедури за реакция при инциденти, контрол на достъпа или правила за сигурна работа с информация, което затруднява идентифицирането и овладяването на заплахи.	Фирма е многократно атакувана поради наличие на уязвимости, но няма необходимите знание и опит към кого да се обърне и как да реагира, поради което инцидентите се повтарят.	**Преки разходи**: глоби за неспазване на регулации (GDPR, PCI – DSS, HIPAA и т.н.) **Косвени разходи**: Репутационни щети, особено при изтичане на данни

Източник: Авторова разработка

От своя страна уязвимостите се превръщат в проводници на неблагоприятни икономически последици за обектите на кибератаки, като най-често биват разделяни на *преки* (кражба на средства, откуп (в случаи на зловреден софтуер), разходи за възстановяване, глоби при неспазване на регулации) и *косвени* (прекъсване на дейността, спад в доверието на клиентите, нарушени партньорства и влошена репутация). В подкрепа на това доклад на британската застрахователна компания Hiscox от 2024 г. показва, че дори единична кибератака може да има разрушителен ефект върху малко предприятие, като в някои случаи води до временно или постоянно прекратяване на дейността (HISCOX, 2024). Според същия доклад средната стойност на киберинцидент за МСП в Европа възлиза на 25 000 EUR, а при тежки пробиви – над 80 000 EUR. В допълнение на това доклад на IBM от 2024 г., насочен към цената на пробива на данни сочи, че за едно средностатистическо МСП той струва около 28 000 USD, като за специфични индустрии като финанси и застраховане, здравеопазване и консултиране може да надхвърли 70 000 USD (IBM, 2024). Несъмнено подобни числа се оказват непосилни за организации от по-малък мащаб, което води и до тяхното рязко или постепенно заличаване. В тази посока Европейската агенция за киберсигурност ENISA отбелязва, че над 90% от анкетираните МСП, претърпели сериозен киберинцидент,

се сблъскват със сериозни последици още седмица след настъпване на събитието (ENISA, 2021). Сами по себе си тези данни са достатъчно красноречиви за необходимостта от адекватни и навременни мерки за киберзащита.

5. Практически насоки за намаляване на уязвимостите

Темата за информационната сигурност на организациите, независимо от техните мащаб и дейност, отдавна вече е част от новите програми за развитие на множество световни организации, което от своя страна поставя акцент върху необходимостта от скоростна адаптация на пазарните участници. Съвсем логично най-подготвени се оказват големите корпорации, които притежават необходимата материална и нематериална подготовка за ответна реакция. Несъмнено това не важи за МСП, които в повечето случаи се характеризират като пазарни последователи, а това от своя страна косвено оказва влияние и върху тяхната степен на подготвеност при наличие на заплахи. Във връзка на следващите редове е изложен кратък и неизчерпателен списък с основополагащи стъпки за придобиване на известна стабилност за МСП по отношение на въпросите, свързани с киберсигурност;

- Изграждане на вътрешнофирмена култура по отношение опазването на данни и активи от стратегическо значение – организационно внедряване на темата за киберсигурността като част от развитието на организацията, както и делегиране на отговорности и задължения на персонала;
- Изготвяне на основни политики за сигурност – официализиране на единни процедури и документация при използване на фирмени устройства и активи, инциденти и изтичане на данни, достъп до системи, работа от разстояние и др.
- Редовно обучение на персонала – регулярно предоставяне на актуална информация относно най-новите видове заплахи и начини за тяхното избягване на лесен, достъпен и запомнящ се от всички възрастови категории език;
- Въвеждане на вътрешни правила относно пароли и автентикация – забрана на пароли с малко и еднородни символи, както и внедряване на

многофакторна автентикация за достъп до критични системи (имейл, облак, база данни и т.н.);

- Внедряване на антивирусни програми и защитни стени (firewalls) - инсталиране на антивирусен софтуер на всички машини, както и използване на защитни механизми при достъп до интернет;
- Поддържане на актуални версии на софтуерните продукти – настройване на автоматични ъпдейти на всички устройства, както и използване единствено на софтуер, който е лицензиран.

С гореизложеното може да се обобщи, че киберсигурността не следва да бъде фокус единствено и само на ИТ експертите, а на всички служители на една организация, и най-вече на нейното ръководство. В потвърждение на това следва да се допълни, че основните уязвимости на МСП не рядко произтичат не от сложни хакерски атаки, а от неволни пропуски и липса на достатъчна дигитална грамотност. Всичко дотук потвърждава необходимостта от кумулативни мерки с цел митигиране на всички възможни предизвикателства на онлайн пространството.

Заключение

В ерата на дигитализацията, киберсигурността се превърна в ключов фактор за устойчивото развитие на бизнеса. Макар че темата обикновено се свързва с големи корпорации и международни институции, именно малките и средни предприятия (МСП) са сред най-уязвимите участници в икономиката. Липсата на достатъчно ресурси, ограничен административен капацитет и недостатъчна осведоменост по отношение на киберрисковете, често правят тези организации лесна мишена за киберпрестъпници. Кибератаките срещу МСП могат да имат сериозни последици – от директни финансови загуби, през прекъсване на оперативната дейност, до дългосрочно увреждане на репутацията и доверието на клиентите. В същото време, голяма част от тези инциденти са предотвратими чрез базови мерки за сигурност и стратегическо планиране. Разбирането на често срещаните уязвимости и оценката на икономическите щети, които те могат да предизвикат, е от съществено значение за информираното управление на риска при МСП.

* * *

Настоящата статия разглежда, но не изчерпва напълно всички аспекти на уязвимостите в киберпространството, като представената информация може да послужи като стабилна основа за надграждане и последващо задълбочено изследване в под формата на дисертация.

За целите на разработката, освен представените по-долу източници, са използвани лични наблюдения и опит на автора, свързани с управлението на бизнес в сферата на информационна сигурност.

Източници:

ENISA. (2021). *SMEs Cybersecurity*. Свалено от ENISA: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/smes-cybersecurity.

IBM. (2024a). *Cost of a Data Breach Report 2024.*

IBM. (2024b). *IBM X-Force Threat Intelligence Index 2024.*

ITU. (2008). *Overview of cybersecurity.*

Tu, Z., & Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review. *20th American Conference on Information Systems*, 1874-1886.

WEF. (2024). *Global Cybersecurity Outlook 2024.*

WTO. (2018). *The Global Risks Report.*

Кръстев, Д., (2021). *Правни основи на киберсигурността. Теоретични и международноправни аспекти.* Варна: СТЕНО.

МТСП на Р България. (2018). *Закон за киберсигурност*. Свалено от http://mlsp.government.bg/uploads/3/zakonodatelstvo/za-kibersigurnost.pdf.

СТОПАНСКА АКАДЕМИЯ „ДИМИТЪР А. ЦЕНОВ” - СВИЩОВ
DIMITAR A. TSENOV ACADEMY OF ECONOMICS - SVISHTOV

ГЛОБАЛНИ И РЕГИОНАЛНИ ИЗМЕРЕНИЯ НА МЕЖДУНАРОДНИТЕ ИКОНОМИЧЕСКИ ОТНОШЕНИЯ

БРОЙ 2
Свищов, 2025 г.

GLOBAL AND REGIONAL DIMENSIONS OF INTERNATIONAL ECONOMIC RELATIONS

ISSUE 2
Svishtov, 2025

ISSN: 2738-8573 (online)

miojournal.uni-svishtov.bg

Адрес на редакцията:
Ул. Емануил Чакъров 2, Свищов 5250, България
Главен редактор:
Проф. д-р Галина Захариева, e-mail: g.zaharieva@uni-svishtov.bg
Технически секретар:
Гл. ас. д-р Ивайло Петров, e-mail: mio.conf@uni-svishtov.bg

За всички представени за публикуване текстове се прилага процедура на двойно анонимно рецензиране.

Публикациите отразяват личните виждания на авторите. Авторите носят пълна отговорност за съдържанието на разработките, изразените мнения, използваните данни, цитираните източници, както и за езиковото оформление на текстовете.

Условията и сроковете за приемане на текстове са посочени на адрес:
miojournal.uni-svishtov.bg
www.mioconference.eu

Адреси на електронното издание: miojournal.uni-svishtov.bg
dlib.uni-svishtov.bg
Алтернативен адрес: www.mioconference.eu

ISSN 2738-8573

Списание „Глобални и регионални измерения на международните икономически отношения“ (съкратено **ГРИМИО**) е правоприемник на изданията с научните резултати от ежегодната *студентска научно-практическа конференция*, организирана от *катедра „Международни икономически отношения”* при Стопанска академия „Димитър А. Ценов” – Свищов. До 2020 година изданията са сборници със самостоятелни ISBN номера, а от 2021 до 2023 година са периодичен сборник с постоянен ISSN номер – достъпни във Виртуалната библиотека на Стопанската академия на адрес dlib.uni-svishtov.bg.

Първата конференция е проведена през 1996 година по идея на проф. д-р ик. н. Иван Стойков и на гл. ас. д-р Симеон Момчев, преподаватели към катедрата. Участници са студентите от трети курс на специалност МИО към Стопанската академия, а тематичният фокус е върху международните инвестиции.

От 2014 година към събитието се присъединяват преподаватели и студенти от *катедра „Международни икономически отношения”* при Икономически университет – Варна, а през 2015 година и от *катедра „Икономика и международни отношения“* при Русенски университет „Ангел Кънчев“.

През годините конференцията се утвърди като форум за научна изява на студентите и докторантите извън учебната аудитория и създаде възможност за разчупване на формалните отношения лектор-обучаем, обмяна на опит в провеждането на мероприятия, свободно споделяне на творчески идеи. Постепенно тематиката се разшири и обхваща широк спектър от области, влизащи в сферата на международните икономически отношения и международния бизнес.

Пленарната сесия на *Двадесет и деветата конференция* се проведе на 10 май 2025 г. присъствено в Базата за обучение на Стопанска академия в с. Орешак и в дистанционен формат чрез платформата BigBlueButton.

Journal “Global and Regional Dimensions of International Economic Relations” (abbreviated **GRDIER**) is the legal successor of the publications with the scientific results of the annual *student scientific-practical conference*, organized by *the Department of International Economic Relations* at Dimitar A. Tsenov Academy of Economics - Svishtov. Until 2020, the editions are conference proceedings with independent ISBN numbers, and from 2021 to 2023 they are periodical collections with a permanent ISSN number - available in the Academy’s Virtual Library at dlib.uni-svishtov.bg.

The first conference was held in 1996 on the idea of Prof. Ivan Stoykov and Head Assistant Simeon Momchev, lecturers at the department. The first participants were the 3rd year IER students at the Tsenov Academy of Economics, and the thematic focus was on international investments.

Since 2014, the event has been joined by professors and students from *the Department of International Economic Relations* at the University of Economics – Varna, and in 2015 from *the Department of Economics and International Relations* at the Angel Kanchev University of Ruse.

Over the years, the conference has established itself as a forum for the scientific expression of students and doctoral students outside the classroom and has created an opportunity to break the formal lecturer-student relationship, exchange experience in conducting events, and freely share creative ideas. Gradually, the topics have expanded and cover a wide range of areas, entering the sphere of international economic relations and international business.

The plenary session of *the Twenty-ninth conference* was held on May 10, 2025 at Dimitar Tsenov Academy’s Training and Recreation Center in the village of Oreshak and online through the BigBlueButton platform.

СЪДЪРЖАНИЕ / CONTENT:

ИЗИСКВАНИЯ КЪМ АВТОРИТЕ

- Допустимост на авторите: настоящи студенти бакалаври, магистри и докторанти в български или чуждестранни висши училища, обучаващи се в икономически специалности.
- При съавторство, поне един от авторите трябва да отговаря на условието да е настоящ студент. Съавтори могат да бъдат и специалисти от практиката, които не са в трудово-правни отношения с българско или чуждестранно висше училище и членуват в алумни клуб на висше училище, организатор/съорганизатор на конференцията.

Формални критерии към структурата на разработката:

- Обем - до 27 000 символа с включени интервали (до 15 стандартни страници).
- Заглавие – ясно и точно формулирано, до 100 символа (с включени интервали).
- Пълно име на автора (авторите), е-поща, специалност и година на обучение, висше учебно заведение.
- Резюме – до 1500 символа (с включени интервали), да има характер на обобщение и да включва изследователски цели, методология и резултати.
- Ключови думи – от три до пет.
- JEL класификация - до три кода, поне един да попада в раздел F. International Economics (ideas.repec.org/j/index.html).
- *Ако основният текст е на български език - следват заглавие, данни за автора (авторите), резюме, ключови думи и JEL,* ***преведени на английски език****.*
- Текстът на доклада следва да бъде оформен в части, като се следва формата за писане на научни текстове **IMRAD** (Introduction, Methods, Results, Discussion). Допускат се допълнителни раздели, ако отговарят на концепцията на изследването.
- Допълнителните бележки, разяснения и коментари - под линия.
- Списък с цитираната литература - по APA style.

Технически изисквания за оформяне на материалите:

- Написани под Word for Windows.
- Размер на страницата: A4, 29–31 реда и 60–65 знака на ред.
- Полета: Top – 2,5 см; Bottom – 2,5 см; Left – 2,5 см; Right – 2,5 см.
- Наименование на статията: Cambria, 14 pt, с големи букви, Bold, центрирано.
- Имена на автора (ите), висше учебно заведение: Cambria, 12 pt, центрирано.
- За резюме, ключови думи и JEL: шрифт Cambria, размер 11 pt.
- За основния текст: шрифт Cambria, размер 12 pt.
- Разстояние между редовете: 1,5 lines.
- Номерация на страницата: долу вдясно.
- Текст под линия: размер 10 pt.
- Графики, фигури и таблици: вграждат се софтуерно в текста.
- Формулите се създават с Equation Editor.

Пълните и актуални изисквания са представени на miojournal.uni-svishtov.bg.

СТОПАНСКА АКАДЕМИЯ „ДИМИТЪР А. ЦЕНОВ" - СВИЩОВ
DIMITAR A. TSENOV ACADEMY OF ECONOMICS - SVISHTOV

ГЛОБАЛНИ И РЕГИОНАЛНИ ИЗМЕРЕНИЯ НА МЕЖДУНАРОДНИТЕ ИКОНОМИЧЕСКИ ОТНОШЕНИЯ

Академично издателство „Ценов"
Ул. Емануил Чакъров 2, Свищов 5250, България

БРОЙ 2, 2025 г.
miojournal.uni-svishtov.bg

GLOBAL AND REGIONAL DIMENSIONS OF INTERNATIONAL ECONOMIC RELATIONS

Academic Publishing House "Tsenov" – Svishtov
2, Emanuil Chakarov street, Svishtov 5250, Bulgaria

ISSUE 2, 2025
miojournal.uni-svishtov.bg

ISSN: 2738-8573 (online)