ПРЕКИ И НЕПРЕКИ ИКОНОМИЧЕСКИ РАЗХОДИ ПРИ КИБЕРИНЦИДЕНТИ В МАЛКОТО ПРЕДПРИЯТИЕ

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

Резюме: Настоящата разработка изследва критичната необходимост от точно разграничаване на икономическите последици от кибератаки за най-уязвимата група пазарни играчи – малките и средните предприятия (МСП). Към днешна дата условията за правене на бизнес в дигитален аспект са изцяло белязани от все по-нови и по-усъвършенствани провокации от технологичен (AI-базирани заплахи, автоматизирани атаки и т.н.), както и регулаторен (прилагане на все по-нишови и стриктни изисквания като директивата NIS2) порядък, които поставят фирмите пред сериозни финансови предизвикателства. В това състояние на конюнктурата малкият бизнес нерядко се оказва финансово неподготвен поради своето изначално прагматично фокусиране върху преките и видими разходи след инцидентите. Основната цел на доклада е да предложи логическа рамка за диференциация на разходите, свързани с киберинциденти в МСП, която да позволи по-точно идентифициране, проследяване и оценка на икономическите последици в краткосрочен, средносрочен и дългосрочен план.

Ключови думи: киберинциденти, малки и средни предприятия, преки разходи, непреки разходи, киберриск

JEL: D81, F61, M15

DOI: 10.58861/tae.grdier.2026.04

Тази статия се цитира по APA стил, както следва: Минкова, Б. (2026). Преки и непреки икономически разходи при киберинциденти в малкото предприятие. *Глобални и регионални измерения на международните икономически отношения,* (3), 44-58. DOI: 10.58861/tae.grdier.2026.04.

DIRECT AND INDIRECT COSTS OF CYBER INCIDENTS IN THE SMALL ENTERPRISE

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: The present study examines the critical need for a precise differentiation of the economic consequences of cyberattacks for the most vulnerable group of market participants - small and medium-sized enterprises (SMEs). At present, the conditions for doing business in the digital sphere are entirely shaped by increasingly sophisticated technological challenges (AI-based threats, automated attacks, etc.), as well as regulatory pressures (the implementation of more niche and stringent requirements such as the NIS2 Directive), which place companies under significant financial strain. In this context, small businesses often prove to be financially unprepared due to their inherent pragmatic focus on direct and visible costs following such incidents. The main objective of this report is to propose a logical framework for differentiating

the costs associated with cyber incidents in SMEs, enabling more accurate identification, tracking, and assessment of economic consequences in the short, medium, and long term.

Keywords: cyber incidents, small and medium-sized enterprises, direct costs, indirect costs, cyber risk

JEL: D81, F61, M15

DOI: 10.58861/tae.grdier.2026.04

This article shall be cited in APA style as: Minkova, B. (2026). Direct and indirect costs of cyber incidents in the small enterprise. *Global and regional dimensions of international economic relations*, (3), 44-58. DOI: 10.58861/tae.grdier.2026.04.

Въведение

В съвременните динамични и крайно непредвидими икономически условия малките и средните предприятия (МСП) утвърждават ролята си на съществена, но силно уязвима точка от глобалните вериги на доставки. Докато големите корпорации инвестират мащабни ресурси в адаптивни защити, малките организации често биват маркирани като „лесна мишена“ поради няколко съпътстващи оперативната им дейност парадокса: висока технологична зависимост, съчетана с ниска киберхигиена и култура, както и ограничени финансови буфери при необходимост.

Пробивите в данните, дефинирани от Национален институт за кариери и изследвания в киберсигурността към САЩ (*NICCS, 2019*), като неразрешено движение или разкриване на чувствителна информация на неупълномощена страна извън организацията, се превръщат във все по-мащабен проблем за бизнеса. Това със сигурност е непренебрежим факт за малките предприятия, които са подчертано уязвими. Приблизително 43% от докладваните кибератаки са насочени към МСП, като според Šafár, Pekarcik, Morawiec, Rutecka, & Wieczorek-Kosmala (*2025*) това се дължи на ниските оперативни бюджети, които не са достатъчни за самозащита от атаки, чиято цел е да идентифицират, откраднат и нарушат важна информация, организационен капитал и интелектуална собственост. Това далеч надхвърля фирмения риск, тъй като в условията на дигитализирана международна икономика МСП се оказват ключов доставчик в рамките на глобалните вериги на стойността, трансграничните цифрови технологии и мрежи от клиенти.

Актуалността на проблема се засилва от факта, че загубите в следствие на кибератака трудно могат да бъдат изчислени извън прякото отразяване на материалните щети. Скритите косвени разходи обикновено не са лесни за

разпознаване, което прави измерването им трудно, но въпреки това тяхното маркиране е важно за оцеляването и конкурентоспособността на бизнеса *(Wang, D'Cruze, & Wood, 2019)*. В настоящата разработка се застъпва тезата, че икономическата цена на инцидента в МСП има многомерен характер и следва да бъде анализирана комбинативно чрез подход, който отчита едновременно множество специфики. В допълнение на това практиката показва, че в хода на събитията много последици остават „под повърхността“, като в повечето случаи се набляга на фактическото възстановяване на причинените щети върху хардуера, софтуера и данните. Това само по себе си заслужава вниманието на мениджърите по отношение на коректния подход към кибератаките и разчета на съпътстващите ги разходи, които нерядко остават „невидими“ за традиционното счетоводство, тъй като се проявяват в различни направления и времеви хоризонт. Този вектор на мислене доказва, че липсата на диференциация води до създаването на илюзия за сигурност и системно подценяване на превантивните мерки, благодарение на които заплахите и прилежащите към тях разходи могат да бъдат избегнати. В тази връзка изграждането на ясен модел за диференциация и класификация на разходите е не просто задача от академичен порядък, а въпрос на бизнес далновидност в ерата на перманентна киберзаплаха.

Като обект на настоящото изследване са дефинирани икономическите измерения на киберинцидентите за малките предприятия, а предметът се фокусира върху подходите и критериите за идентифициране, разграничаване и класифициране на произтичащите от тях разходи. Целта на доклада е въз основа на критичен поглед и синтез на утвърдените методи в академичната литература да бъде предложен и обоснован авторски многомерен класификатор на разходите в следствие на киберинциденти, адаптиран към специфичните особености на малкото предприятие. Същият следва да послужи в полза на по-коректното управление на различните икономически последици във времевата линия на тяхното развитие.

1. Теоретичен обзор – специфика на киберриска в малкото предприятие

През последните години информационните и компютърни технологии (ИКТ), Интернет на нещата (IoT), а към днешна дата и изкуственият интелект (ИИ) са не само препоръчителен, но и почти задължителен компонент от бизнес модела

на всяка една организация, която преследва конкурентни позиции в дългосрочен план. Изключение за това не правят и малките и средните предприятия (МСП), които с течение на времето усвоиха внедряването на технологии от подобен порядък, предоставящи широк спектър от възможности не само за глобална комуникация в реално време, но и за оптимизиране на голяма част от бизнес дейностите. Иновациите и използването на новите технологии се разглеждат от МСП като условие за успешното им участие в глобалните вериги на стойността *(OECD, 2008)*. Но както допълват изследователите от ОИСР, по-големите възможности за малките предприятия идват заедно със сериозни предизвикателства и това можем да отбележим като валидно за всеки един аспект от тяхното съществуване.

По начало зависимостта от ИКТ вещае специфични провокации, които превръщат организациите в силно уязвими обекти към всички заплахи за информационната сигурност. Според Markopoulou, Papakonstantinou, & De Hert *(2019)* МСП, които се стремят към дигитализация и интернационализация, трябва да се ориентират в сложната среда на киберсигурността, което налага разработването на специфични стратегии за защита на техните дигитални активи.

Теоретичното осмисляне на киберсигурността в малкото предприятие изисква радикално разграничаване от добре познатите традиционни корпоративни модели. В академичната литература доскоро преобладаващо бе схващането, че киберсигурността може да бъде разглеждана като „скалируем“ проблем, а методите, прилагани в големите организации, могат успешно да бъдат пропорционално адаптирани за нуждите на малкия бизнес. Към днешна дата този подход се оказва крайно неактуален най-вече поради спецификите на средата, в която доминират все по-персонализирани атаки, които биват прилагани по автоматичен път спрямо параметрите на всяка таргетирана организация. Въпреки че МСП не винаги представляват основна цел, все пак биват засягани косвено, особено тези, които оперират във вериги за доставки, свързани с критични сектори или предоставят цифрови услуги *(Panko, Šafár, & Mešťan, 2025)*. Всъщност малките организации вече са сред предпочитаните цели на киберпрестъпниците поради връзките им с по-големи компании като техни клиенти, както и доказано по-ниските нива на защита.

Често практиците, а и академиците маркират малките предприятия като

„гръбнак на световната икономиката“ и това не е никак случайно. Според данни на Европейската комисия МСП съставляват 99% от представителите на пазара на ЕС, като цели 93.2% са микро предприятия. Именно това значително представителство на организации от подобен тип е един от поводите през 2021г. Европейската агенция за киберсигурност (ENISA) да изготви специализирано проучване с представителна извадка, включваща 56% микропредприятия (до 10 служителя и до €2 млн. годишен оборот), 28% малки предприятия (до 50 служителя и до €10 млн. годишен оборот) и 16% средни предприятия (до 250 служителя и до €50 млн. годишен оборот). Заложената цел е да бъдат дефинирани капацитетът и готовността на тази категория бизнеси, свързани с реакция към нарастващите кибериниценти. Според финалните резултати над 80% от допитаните респонденти обработват чувствителна информация, но на този фон едва 30% от тях разчитат на по-сериозни организационни и технологични контроли за предотвратяване на пробиви в сигурността *(ENISA, 2021)*. Това само по себе си подчертава ниските нива на готовност на МСП, които ги превръщат в една изключително обещаваща мишена за атака от страна на недоброжелателни лица, конкуренти или просто хакери, които упражняват своите умения без конкретна цел.

Дотук представеното извежда на преден план подчертано уязвимия профил на малките предприятия в рамките на все по-интегрирания дигитален свят. Според Panko, Šafár, & Mešťan *(2025)* МСП са жизненоважни за световната икономика, но остават силно уязвими към киберзаплахи поради ограничени ресурси, технически капацитет и осведоменост. В тази връзка през годините са правени множество опити за извеждане на основните предизвикателства пред малките предприятия. Amrin *(2014)* прави заключението, че най-често срещаните тенденции в ИТ уязвимостите включват социалното сътрудничество, разширеното използване на мобилни устройства, преместването на съхранението на информация в облак, дигитализацията на чувствителна информация, преминаването към интелигентни мрежи, както и възприемането на алтернативи за мобилност на работната сила. От съществено значение остава и проблемът с осведомеността и ангажираността на ръководството, което от своя страна определя бюджета, разпределението на ресурсите и ефективното прилагане на практиките за киберсигурност. Именно поради този факт списъкът с дигитални предизвикателства пред МСП, представен

от ENISA *(2021)* съдържа следните компоненти: (1) *Ниска или липсваща осведоменост на персонала относно киберсигурността* (киберкултура и киберхигиена); (2) *Недостатъчна защита на обработваната критична и чувствителна информация* (липса на специфични политики за архивиране, защита и актуализиране на всички видове устройства); (3) *Липса или оскъдност на бюджет за киберсигурност* (свързан с обучения на персонала, въвеждане на специализирани системи за киберсигурност и т.н.); (4) *Недостиг на специалисти по киберсигурност* (претоварване на служителите, ангажирани с други ИТ звена); (5) *Липса на подходящи насоки за киберсигурност, специфични за МСП*; (6) *Използване на лични устройства за работна цел, известно като BYOD (Bring Your Own Device)* поради липсата на достатъчен бюджет за цялостно техническо обезпечаване; (7) *Ниска подкрепа от страна на ръководството по отношение на необходимостта от инвестиции в киберсигурност*.

Гореизброеното представлява добра основа за поставяне на някои основни положения от профила на МСП като таргет на кибератакуващите. Въпреки това, през призмата на своята практика, авторът на настоящата разработка допълва списъка с още едно актуално предизвикателство, свързано със *системното подценяване на риска в МСП и синдрома на „малката мишена“*. Често мениджърите на МСП страдат от когнитивното изкривяване, според което поради своя размер трудно биха попаднали в обсега на потенциална атака. В реалността, обаче, престъпниците са рационални субекти, които предприемат действия, когато преценят, че ползата е по-голяма от възможността да бъдат заловени или атакувани обратно, а в контекста на малка организация, тези шансове са сведени до минимум.

Всичко дотук подсказва, че пред малките предприятия на дневен ред са нови предизвикателства от особен род, вещаещи разходи, които до този момент са били позиционирани в зоната на хипотезата. Тяхното подценяване, обаче, вече е съществен проблем, като минимизирането на разходите за възстановяване предполага инвестициите в киберсигурност да бъдат с превантивен, а не реактивен характер.

2. Разходи в следствие на киберинцидент - същност и видове

Широката общественост поставя разходите, свързани с киберзащита, в едно

заключено пространство, което намира място в планирането на фирмените бюджети ad hoc или в случай на необходимост. Това важи с особена сила за МСП, чиито мениджъри често попадат в погрешното схващане, че този тип разходи включват единствено и само непосредствени плащания за техническо възстановяване, външни експерти или правни услуги. Но икономическата, а и техническата същност на събития от подобен род е значително по-широкомащабна, тъй като един инцидент в сигурността може да породи както преки, така и непреки последици за бизнеса, част от които се проявяват незабавно, а други са с ефект на натрупване. Именно поради тази причина оценката на реалната цена на кибератаката изисква дуален подход – преглед както на счетоводно отчетимите внезапни разходи, така и на загубите от прекъсване на дейността (downtime), отслабване на доверието, пропуснати приходи, организационно напрежение и дългосрочни репутационни ефекти. При малкото предприятие този въпрос е от особено значение, тъй като ограниченият ресурсен резерв, зависимостта от непрекъсваемост на дейността и по-тясната връзка между имидж и приходи увеличават чувствителността към загуби от подобен род. Точно затова МСП често възприемат киберсигурността като разход, макар самите те да посочват, че сериозен инцидент, водещ до недостъпност на ИКТ системите, би имал голям негативен ефект върху бизнеса *(ENISA, 2021)*.

В литературата се открояват няколко основни подхода за диференциране на разходите при киберинциденти, като най-общият и концептуално изчистен се състои в разграничението между две основни категории - *преки и непреки разходи*. Подобен метод е използван в доклада на Vergara Cobots & Cakir *(2024)*, изготвен в полза на Световната банка, според който преките разходи, свързани с киберинциденти, обхващат осезаемите финансови загуби, щети и трудности, понесени от жертвите след подобни събития. Те включват, но не се ограничават до незаконните финансови печалби, натрупани от киберпрестъпниците (познати още като откупи). От друга страна, непреките разходи са маркирани като свързани с реакциите на фондовия пазар и щетите върху репутацията, прекъсванията на производствената верига, ефектите на разпространение и систематичните рискове, породени от киберинциденти, разходите, свързани с реагиране и киберриск. Авторите Krausz и Walker *(2013)* също разделят разходите на две основни групи, но подходът предполага групиране по следния начин: (1) *Директни*

и косвени разходи - всички разходи, пряко свързани с инцидента, включително отделено работно време, извънреден труд, външни разходи, разходи за оборудване и правни услуги, както и всички разходи, възникнали в резултат на инцидента, включително разходи за загубена производителност и санкции от клиенти в случай на атака тип „разпределен отказ на услуга“ (DDoS); (2) *Репутационни разходи, рискове за трети страни и свързаните с тях разходи* – всички разходи в резултат на загуба на данни, доверие и авторитет сред клиентите и широката общественост, както и всички разходи, свързани с рисковете за сигурността на трети страни, хостинг на приложения, услуги и инфраструктурни компоненти при доставчици на облачни услуги.

По-детайлен поглед предлагат изследователите от американския Национален институт за стандарти и технологии (NIST), според чиито виждания разграничението трябва да бъде направено между *вътрешните разходи, външните последици и пропуснатите ползи*. Тук акцентът е поставен върху последователността на икономическите ефекти – разходите не се възприемат като еднократен ефект, а като последователен процес, в който загубите се проявяват в каскаден ефект в следствие на фазовото възстановяване на бизнеса. Според Bartock et al. *(2016)* част от цената на инцидента възниква вътре в самата организация под формата на разходи за откриване, разследване, ограничаване и възстановяване, докато друга част се проявява отвъд структурата посредством загуба на информация, прекъсване на дейността, намаляване на приходите и неблагоприятни пазарни последици. Особено съществен е приносът на идеята за пропуснатите ползи, тъй като по този начин могат да бъдат отчетени нереализираните възможности, отказаните сделки и загубения потенциал за растеж. За малкото предприятие именно тази перспектива е от съществено значение, тъй като дори кратко нарушение на нормалния бизнес цикъл може да се отрази не само върху текущите приходи, но и върху бъдещото позициониране на пазара.

Друга по-подробна гледна точка на Anderson et al. *(2012)* разглежда различните категории разходи по следния начин: (1) *Директни* - паричният еквивалент на загуби, щети или други жертви в резултат на киберпрестъплението, като това включва загуба на парична стойност и свързаните с нея неудобства, загуба на време и усилия, изразходвани за възстановяване на данни, емоционален

стрес и загуба на клиентски трафик; (2) *Косвени* - паричният еквивалент на загубите и алтернативните разходи за обществото или институциите като цяло, което включва загуба на потребителското доверие в онлайн бизнеса, водеща до намалени приходи и пропуснати бизнес възможности, както и разходи за усилия за възстановяване от кибератаки; (3) *Разходи за защита* - паричният еквивалент на превантивните мерки, включително разходите за разработване, внедряване и поддръжка на продукти и услуги за сигурност, мерки за обучение и повишаване на осведомеността, откриване и възстановяване на измами, както и разходите за правоприлагане, неудобства и пропуснати възможности; (4) *Разходи за обществото* - сбор от преките загуби, косвените загуби и разходите за отбрана. Тук е важно да спомена гледната точка на колектива, според която преките разходи са относително по-ниски в сравнение с непреките разходи и разходите за защита. Подобно схващане споделят и авторите *Vergara Cobots & Cakir (2024)*, които отбелязват, че косвените разходи могат да бъдат поне толкова съществени, колкото и преките такива, поради постепенно възникващите ефекти, които се генерират след инцидента.

Подходът на Wang et al. *(2019)* показва нов, още по-задълбочен метод за класифициране на разходите, според който те се разделят на две категории – преки и непреки, които могат да бъдат приложени спрямо гледната точка на два отделни сегмента – бизнеси и потребители. Така видовете разходи се разделят на общо четири групи, а именно: (1) *Директни за бизнеса* – кражба на финансови средства, прекъсване на оперативната дейност, разходи за разследване и правна дейност, отделено работно време, регулативни глоби, и т.н.; (2) *Индиректни за бизнеса* – спад в продажбите и продуктивността, загуба на потребители, намален растеж, загуба на инвестиции, време на престой за бизнеса (downtime), репутационни щети и т.н.; (3) *Директни за потребителите* – кражба на лични данни и финансови средства, плащане на откупи, разходи за водене на съдебни дела и т.н.; (4) *Индиректни за потребителите* – загуба на време за разследване на казуса и оценка на щетите, причинено неудобство и стрес, и т.н. Това, от своя страна, доказва, че разходите могат да бъдат разгледани и през призмата на потребителите, които в крайна сметка заплащат цената за пропуските в сигурността на бизнеса.

Представените по-горе методи потвърждават, че икономическата тежест на киберинцидента далеч не се изчерпва с разходите за внезапна реакция. В

практиката, макар и често пренебрегвани, ясно заявяват мястото си и категории като загуби от прекъване на дейността, отпадане на клиенти, репутационни щети и последващи разходи за възстановяване. Това показва, че непреките последици не са периферен елемент, а съществен компонент от общата калкулация на инцидента. Именно тук се открива и една от най-съществените особености на малкото предприятие - когато клиентската база е по-концентрирана, организационният капацитет е ограничен, а зависимостта от текущите приходи е висока, скритите разходи от подобно събитие могат да се окажат поне толкова значими, колкото и непосредствените преки разходи. А това налага нуждата от коректен и детайлен отчет на всички последствия.

3. Класификация на разходите в контекста на малкото предприятие

Съпоставянето на представените по-горе подходи позволява да се изведе заключението, че липсва всеобщо приет модел за класификация на разходите, възникнали в следствие на киберинциденти. Още повече следва да бъде отбелязан факта, че всяко предложение за разделение е плод на субективния поглед на автор-а/-ите, както и натрупания практически опит. Но определящ фактор се явява и областта на приложение, а контекста на МСП изисква отчитането на някои специфики, които различават тази група бизнеси от всички останали икономически играчи. Проверката на академичната литература не установява наличието на утвърдена класификация, разработена специално за малките предприятия. Наличните изследвания предлагат или по-общи модели за разграничение, или емпирични анализи на въздействията върху МСП без да изграждат конкретна таксономия. Това налага разработването на обобщен класификатор на разходите, който да съчетае добрите практики от вече утвърдените подходи с нуждите на малкия бизнес.

На тази основа в настоящия доклад се предлага синтетична авторска визия за класификатор, който комбинира три аналитични измерения: (1) *Основно разграничение между преки и непреки разходи*; (2) *Времеви хоризонт на тяхното проявление*, тъй като част от разходите възникват непосредствено след инцидента („светкавични разходи“ - T+0 до 48ч), а други се развиват в средносрочен („остатъчни разходи“ - T+7 дни до 1 месец) и дългосрочен („ерозионни разходи“ - T+6 месеца и повече) план; (3) *Сфера на въздействие върху МСП*, която може да бъде

техническа, правна, оперативна, търговска, репутационнна, стратегическа и т.н. Авторовото решение да бъдат включени споменатите три категории може да бъде аргументирано по следния начин:

Първата категория, а именно разграничението между преки и непреки разходи, е най-пряко подкрепена от академичната общност, като всички разгледани по-горе подходи изхождат от този тип основно разделение по оста „първични и вторични разходи“.

Втората категория, свързана с времевия хоризонт на проявление, е обоснована от чисто техническия курс на възстановяване след инцидент, който предполага поетапно разходване на средства (особено когато те са оскъдни). Друга причина се корени във факта, че ефекти като отлива на клиенти и загубата на репутационни позиции не се случват в цялост, а по-скоро имат каскаден ефект на проява, което предполага и различно времево планиране на разходите.

Третата категория, обусловена от сферата на въздействие, е необходим елемент, тъй като последиците от инцидентите в сигурността никога не са еднородни – част от тях се проявяват като технически проблеми, други като правни и регулаторни ангажименти, трети като оперативни прекъсвания, търговски загуби, репутационни щети или стратегически ограничения за бъдещото развитие. Подобна многоаспектност се вижда както в подхода, предложен от NIST (където се посочват ефекти, свързани с хардуер, софтуер, правни регулации, човешки ресурси и т.н.), така и в този на Световната банка (където се посочват ефекти, свързани с отговор на атаката, производствени загуби, репутационни щети, вериги на доставки и т.н.). В допълнение на това логиката от страна на практиката загатва за една сериозна организационна характеристика на малкия бизнес. При МСП рядко по-горе изброените функции са ясно вътрешно обособени за разлика от големите корпорации, където съществуват отделни звена и отговорни лица за всяка област (Например: В малка счетоводна фирма от семеен тип собственикът отговаря за управление, счетоводна отчетност, финанси, реклама, ИТ поддръжка, работа с юристи и т.н.). Това предполага сериозна концентрация на оперативна дейност в рамките на едно или няколко лица, при което мисловното разделение на разходите би се оказало трудоемко предвид многото заложени компетентности. Поради това разграничаването на разходите според сферата на въздействие има не само

аналитична, но и управленческа стойност, тъй като позволява по-високи нива на проследяемост и контрол на „засегнатите зони“.

Във връзка с гореизложеното на следващите редове е представен синтезирания резултат от поставената теоретична основа и контекстуалната приложимост за МСП под формата на класификатор на разходите (табл. 1). Матрицата илюстрира, че преките разходи са по-видими и обикновено се концентрират в краткосрочния етап непосредствено след инцидента докато непреките разходи имат по-разтеглено във времето проявление и засягат по-широк кръг от бизнес функции. Именно чрез сферите на въздействие се открояват някои първоначално скрити за мениджърите области на засягане, които акумулират значителни средства. По този начин предложеният класификатор изпълнява дойна функция. От една страна, той систематизира основните видове разходи, които съпътстват киберинцидента в МСП. От друга страна, той дава аналитична основа за по-прецизно проследяване на засегнатите бизнес функции и за по-реалистична оценка на дългосрочната икономическа тежест на подобни събития. Това го прави подходящ инструмент не само за теоретичен анализ, но и за коректна оценка на разходите, която е безпрецедентен фактор за стратегическа устойчивост.

Таблица 1. Матрица на разходите за МСП в следствие на кибератака

Времеви хоризонт	***Преки разходи***	***Непреки разходи***
Краткосрочен (T+0 до 48ч.)	***Техническа сфера на въздействие:*** • Техническо овладяване на инцидента; • Форензика; • Наемане на външни специалисти. ***Оперативна сфера на въздействие:*** • Плащане на откупи; • Откраднати финансови средства. ***Правна сфера на въздействие:*** • Правни консултации; • Заплащане на глоби според регулаторните изисквания.	***Оперативна сфера на въздействие:*** • Откраднати фирмени и клиентски данни (при наличие); • Престой на дейността (downtime); • Загуба на производителност; • Затруднено обслужване на клиенти; • Прекъсване на ежедневните бизнес процеси; • Вътрешно организационно напрежение. ***Пазарна сфера на въздействие:*** • Пропуснати текущи приходи. ***Репутационна сфера на въздействие:*** • Уведомяване на засегнатите страни и съответните органи.

Средносрочен (T+7 дни до 1м.)	***Техническа сфера на въздействие:*** • Въвеждане на решения за дигитална защита; • Одити и разходи за съответствие. ***Оперативна сфера на въздействие:*** • Повторно въвеждане на услуги и процеси. ***Репутационна сфера на въздействие:*** • Комуникационни и PR дейности.	***Оперативна сфера на въздействие:*** • Затруднено възстановяване на работния ритъм; • Постепенно намаляване на оборота; • Повишени организационни разходи; • Неефективност поради пренасочване на ресурси за защита. ***Пазарна сфера на въздействие:*** • Спад в продажбите, отпадане на сделки и загуба на клиенти. ***Репутационна сфера на въздействие:*** • Постепенна ерозия на доверието на клиенти и партньори.
Дългосрочен (T+6 месеца и повече)	***Техническа сфера на въздействие:*** • Поддържане на решенията за дигитална защита. ***Правна сфера на въздействие:*** • Съдебни и регулаторни процедури (при наличие на такива).	***Пазарна сфера на въздействие:*** • Трайни загуби на пазарни позиции и достъп до нови пазари; • Ограничени възможности за растеж и финансиране; • Затруднено привличане на нови клиенти и партньори; • Отслабена конкурентоспособност. ***Репутационна сфера на въздействие:*** • Трайно влошен публичен и пазарен образ.

Източник: Авторова разработка въз основа на Vergara Cobots & Cakir (2024), NIST SP 800-184 и ENISA (2021).

От практическа гледна точка изложеното позволява да бъде формулирана и препоръката към бизнеса за разбиране на структурата на разходите не само като аналитично уравнение, а като предпоставка за по-висока организационна устойчивост. Целта е насочването на ресурси за превантивни, а не реактивни мерки в името на дългосрочната информационна сигурност за всички заинтересовани страни.

Заключение

Настоящата разработка подчертава, че икономическите последици от киберинцидентите рядко биват оценявани единствено чрез преките разходи по техническо овладяване и възстановяване. В подкрепа на това анализът на разгледаните подходи, както и предложеният авторски класификатор потвърждават, че реалната цена на подобни събития има многопластов характер и включва както непосредствени финансови загуби, така и непреки ефекти,

проявяващи се във времето посредством прекъсване на дейността, загуба на клиенти, репутационни щети и т.н. Именно в контекста на МСП тези последици придобиват особена значимост, тъй като ограничените ресурси, липсата на вътрешна специализация и високата зависимост от непрекъсваемост на постоянни парични потоци усилват икономическата тежест на инцидента.

Направеният преглед на литературата показва също, че макар да съществуват различни подходи за разграничаване на разходите, липсва утвърдена и специално адаптирана към МСП класификационна рамка. В този смисъл предложеният модел има за цел да предостави именно това, като съчетае три аналитични измерения в услуга на по-комплексния поглед върху всички явни и скрити последици за различните аспекти на бизнеса.

* * *

Настоящият доклад разглежда, но не изчерпва напълно всички аспекти на изложената тематична област, като представената концепция служи като основа за последващо усъвършенстване в рамките на дисертация на тема „Оценка на икономическите последици за МСП в следствие на кибератаки и киберпрестъпления“.

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:

Amrin, N. (2014). *The Impact of Cyber Security on SMEs.* University of Twente.

Anderson, R., Barton, C., Bohme, R., & Clayton, R. (2012). Measuring the Cost of Cybercrime. *11th Workshop on the Economics of Information Security (WEIS).*

Bartock, M., Cichonski, J., Soppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). *Guide for Cybersecurity Event Recovery*. NIST - National Institute of Standards and Technology, U.S.A.

ENISA. (2021). *CYBERSECURITY FOR SMEs*. Challanges and recommendations.

Krausz, M., & Walker, J. (2013). *The true cost of information security breaches and cyber crime*. IT Governance Publishing.

Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law and Security Review.*

NICCS (National Initiative for Cybersecurity Careers and Studies). (2019). *Explore Terms: A Glossary of Common Cybersecurity Terminology*. Retrieved from https://niccs.cisa.gov/resources/glossary.

OECD. (2008). Enhancing the role of SMEs in global value chains. OECD Publishing.

Panko, M., Šafár, L., & Mešťan, M. (2025). Small Firms, Big Threats: Cybersecurity Research and the Role of Public Policy in the SME Sector. *Cent. Eur. J. Public Policy, 87-110.*

Šafár, L., Pekarcik, M., Morawiec, P., Rutecka, P., & Wieczorek-Kosmala, M. (2025). Mapping Cybersecurity in SMEs: The Role of Ownership and Firm Characteristics in the Silesian Region of Poland. *Information MDPI.*

Vergara Cobots, E., & Cakir, S. (2024). A Review of the Economic Costs of Cyber Incidents. *World Bank.*

Wang, P., D'Cruze, H., & Wood, D. (2019). Economic costs and issues of business data breaches. *Issues in Information Systems, 162-171.*

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

ГЛОБАЛНИ И РЕГИОНАЛНИ ИЗМЕРЕНИЯ НА МЕЖДУНАРОДНИТЕ ИКОНОМИЧЕСКИ ОТНОШЕНИЯ

БРОЙ 3
Свищов, 2026 г.

GLOBAL AND REGIONAL DIMENSIONS OF INTERNATIONAL ECONOMIC RELATIONS

ISSUE 3
Svishtov, 2026

ISSN: 2738-8573 (online)

miojournal.uni-svishtov.bg

Адрес на редакцията:
Ул. Емануил Чакъров 2, Свищов 5250, България
Главен редактор:
Доц. д-р Драгомир Илиев, e-mail: d.iliev@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 *Тридесетата конференция* се проведе на 16 май 2026 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 Thirtieth conference* was held on May 16, 2026 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 3, 2026 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 3, 2026
miojournal.uni-svishtov.bg

ISSN: 2738-8573 (online)