НОВАТА (НЕ)СИГУРНОСТ! ВИРУСЪТ, КОЙТО „РАЗБОЛЯ“ ИКОНОМИКАТА! (ПОГЛЕД КЪМ СЛУЧИЛОТО СЕ ПРЕЗ ИЗМИНАЛИТЕ ШЕСТ МЕСЕЦА)

Тихомир БЛАГОВЕСТОВ*

THE NEW (IN) SECURITY! THE VIRUS THAT „SICKED“ THE ECONOMY! (A LOOK AT WHAT HAPPENED OVER THE PAST SIX MONTHS)

Abstract: *The New insecurity (uncertainty) presented in the topic, is caused by the virus that caused serious „stress“ and displaced the „tectonic plates“ in the economies of countries around the world. A global recession has occurred. Along the way, the virus affected important key places in the economics, which weakened the global industry, transport, etc., creating a precondition for cyber insecurity!*

Key words: *new insecurity, China, virus, Hubey, Covid-19, economics, „WHO“, Institute of International Finance (IIF), capital economics, petrol, GDP, global economics, World Bank, risk, perspectives, events, Harvard Business Review, real recession, financial crisis, recession of policy, container shipping, International transport forum, ASEAN, cyber security, SARS, MERS, cybersecurity risks, 5G, Europe, MSMEs in the context of Covid-19 crisis, Organization for the prohibition of chemical weapons (OPCW), „WannaCry“, „NotPetya“, „Cloud Hopper“*

Ако не вярвате в това или не го разбирате, нямам време да се опитвам да ви убедя, съжалявам.
Сатоши Хакамото

Светът стартира своята „перестройка“, като заплахите не са вече така взривоопасни в буквалния смисъл на думата, а са тихи, скрити, свързани с глобалното навлизане на телекомуникациите,

* Авторът е студент II курс в професионално направление „Национална сигурност“, специалност „Противодействие на тероризма“, във Висшето училище по сигурност и икономика – Пловдив.

киберпрестъпленията, хибридните войни и маньоври, използвани за насочване на общественото мнение, но най вече със зачестилите събития в здравно-хуманитарен аспект, причинени от фактори, за чието създаване все още се разпространяват конспиративни теории, но изводът е един – **вреда за човечеството и икономиката в глобален аспект.**

Средата на сигурност от началото на годината (2020) отбелязва силна динамика в аспекти, много по различни, и с прецеденти, невиждани от десетки години.

В тази статия ще наблегнем на синтез, източници на информация, като се придържаме към фактологията на случващите се събития през последните няколко месеца по света.

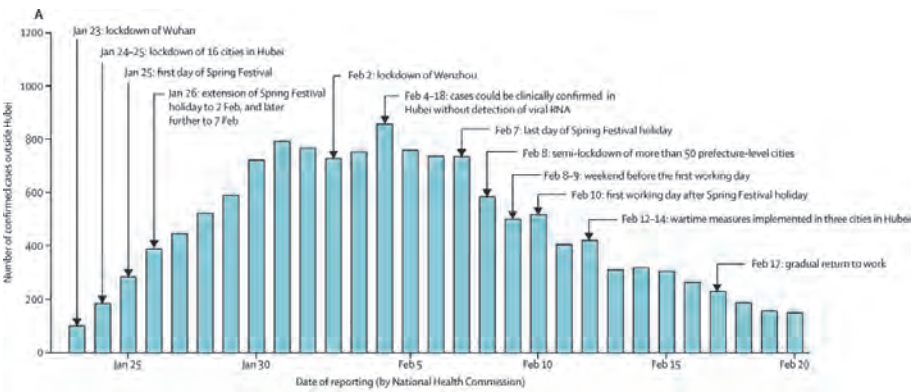
Ще обърнем внимание на изминали събития, а също така и на новите опасности и заплахи за сигурността – в кои сектори са насочени те, какви бяха и какви ще са последиците, какво решение трябва да се вземе от гледна точка на сигурността и функционирането отново на икономиката, както, разбира се, ще обърнем поглед и към сферата на **киберсигурността.**

НАЧАЛОТО

В края на 2019 г. в град Ухан, Централен Китай, е идентифициран коронавирус, наречен SARS-CoV-2. Това става, след като без ясни причини през **декември** хора развиват пневмония, която не се повлиява от известните методи на лечение. Има свидетелства за предаване на вируса от човек на човек, като най-бързо се разпространява **в средата на януари 2020 г.** Няколко държави в Европа, Северна Америка, и най-вече в Азиатско-Тихоокеанския регион съобщават за случаи на зараза [2].

През **третата седмица на януари 2020 г.** в Китай се прилагат масивни интервенции в областта на общественото здраве, за да се ограничи разпространението на коронавирусната болест (Covid-19) (вж. фигурите). Епицентърът на огнището (Ухан) е затворен от **23 януари,** като **16** от съседните му градове в провинция **Хубей** са включени в санитарния салон за кордони малко след това. Националният празник на пролетния фестивал е удължен с 8 дни – до 7 февруари, и повечето **училища остават затворени** до момента. С приключването на празника на пролетния фестивал **строгите мерки за социално дистанциране и ограниченията за мобилност бяха координирани и приложени от централните и местните власти** в много китайски мегаполиси, включително в Пекин –

северно от Ухан, Гуанджоу и Шънджън на юг, в Шанхай и Ханджоу на изток и в Чънду на запад. Например само на **жителите е разрешено да влизат в жилищни общности, носенето на маски за лице става задължително, а несъществените услуги в общността са закрити.** Въпреки че агресивните контрамерки, изглежда, са намалили броя на регистрираните случаи, липсата на стаден имунитет срещу Covid-19 предполага, че броят на заболелите може лесно да се възобнови, когато тези интервенции са отпуснати, тъй като бизнесът и училищата се възобновяват [3].

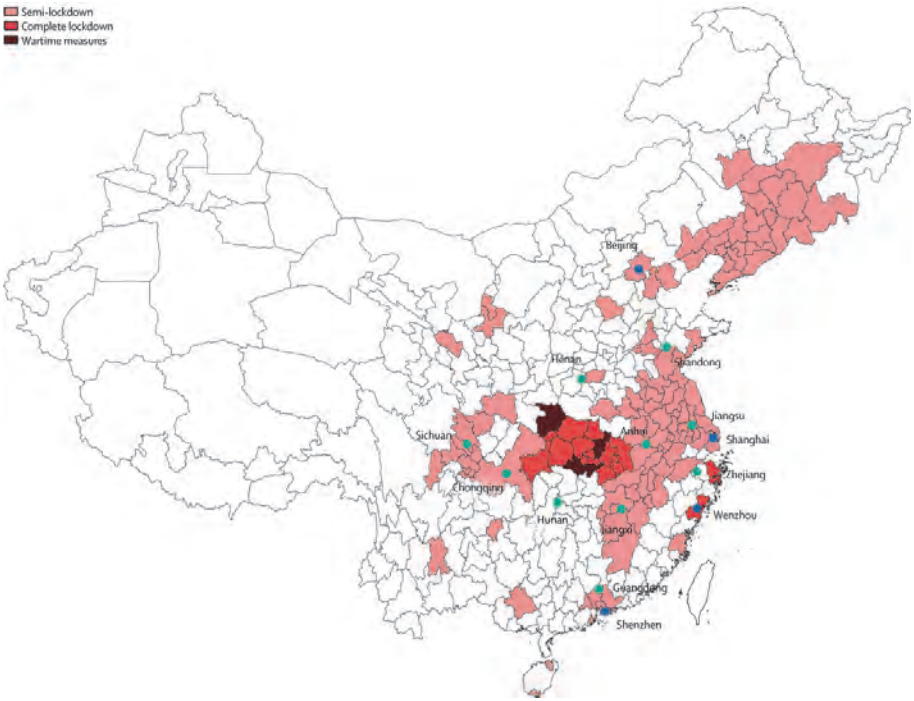


• Към **29 февруари 2020 г.** са регистрирани 411 в Пекин, 337 в Шанхай, 417 в Шънджън и 504 в Уънджоу лабораторно потвърдени случаи на инфекции с Covid-19 [4; 5; 6; 7].

• Справка към **18 март 2020 г.** съобщава за **13 415** потвърдени случая и **120 смъртни случая,** свързани с коронавируса в Китай, извън провинция **Хубей** – в епицентъра на огнището.

• Китайската национална здравна комисия (NHC) заявява **(юли 2020),** че не са регистрирани местни инфекции в страната. В изявление NHC посочва, че са открити 7 нови случая, но **„всички са внесени случаи".** Страната е потвърдила 1949 случая на внесени инфекции, от които 1877 са се възстановили. Китай е докладвал за общо 83 572 случая на Covid-19 от избухването му в Ухан – столицата на централната провинция Хубей, миналия декември [9].

• До момента общият брой на случаите с коронавирус в Китай е **85 022,** от които **80 126 са се възстановили.** Броят на **починалите** е **4636.** Общият брой на **потвърдените тестове** за Covid-19 са **90 410 000.** Населението на Китай за сведение е **1 439 323 776** [10].



Източник: *Thelancet.com.*

По всичко, описано по-горе, става ясно на пръв поглед, че цифрите са плашещи на базата на краткото време, през което се развива тази пандемия. Всъщност описвам случилото се като пандемия, защото по някои установени значения думата *„пандемия“* означава: изразен голям процент болни от населението на една държава, причинен от вирус (пример: испанският грип, Юстиниановата чума, Черната смърт засягат между 40 и 50 % от населението).

В Китай според броя на населението и регистрираните случаи процентът на заразените е под 1, или по-конкретно около 0,006 %.

Статистиката на заразените с Covid-19 в някои държави в Европа отбелязва следното:

- Германия – общ брой на потвърдените случаи 242 189;
- Франция – общ брой на потвърдените случаи 267 077;
- Италия – общ брой на потвърдените случаи 265 409;
- Испания – общ брой на потвърдените случаи 455 621;
- Русия – общ брой на потвърдените случаи 985 346;
- Австрия – общ брой на потвърдените случаи 26 985;
- Полша – общ брой на потвърдените случаи 66 239;

• България – общ брой на потвърдените случаи 16 065 [11].

Нито една от посочените 8 държави не преминава 1 % заразени от броя на населението си. Единствено Испания от посочените държави е близо до този 1 %, но да не се забравя все пак, че от този почти процент има и много, които са излекувани. Коронавирусът (SARS-CoV-2) не нанася щети (глобално) така, както испанският грип, Юстинианова чума, Черната смърт и т.н., и т.н., **но все пак е вирус, и то опасен.**

Тогава, ако не нанася такива поражения на населението по света, както познатите от миналото щамове, то какви са последствията от Covid-19 в други сфери, например в **икономиката.**

ВРЕМЕНА НА РАЗМИСЪЛ И НУЖДА ОТ ОСЪЗНАВАНЕ

Ако погледнем едно природно бедствие, като например цунами, земетресение, пожар, изригване на вулкан и т.н., ще забележим, че последствията и щетите след тях са катастрофални, мащабите са огромни, видими и оценявани след самото бедствие, и превенция трудно се предприема пред скритите намерения на майката природа.

Така, еквивалентно на природно бедствие, но с друга същност, сполетелият целия свят вирус Covid-19 отправи катастрофален удар над световната **икономика** с бавно „отмиваща“ се криза.

Светът прекара голяма част от вълната на удара на коронавируса, затворен и изолиран в собствените си къщи, апартаменти, градове, и дори държави. Бизнесът изпадна в летаргия, на места замръзна, а на други престана да съществува. С увеличаването на заразените мерките за предотвратяване на заразата ставаха по-строги и „облечени“ в закони и наредби от управниците на потърпевшите държави, водени от Световната здравна организация (СЗО).

Поглед назад показва предположенията на специалистите за спад в икономиката след установяване на голям брой заразени и последиците от него:

• Броят на хората, заразени с коронавируса, надхвърли 114 000 (март 2020) в световен мащаб. Вирусът, който **стартира в Китай** в края на миналата година, има **последици за всички големи икономики** с анулиране на полети, паническо пазаруване и строги карантинни мерки в някои случаи [12].

• **От Института за международни финанси (IIF)** заявяват в доклада си: „Обхватът на очакваните потенциални резултати е голям и зависи от разпространението на вируса и произтичащото от

това икономическо падение. Всички на този етап са много несигурни“ [12].

• „Има две основни причини, поради които щетите могат да бъдат по-големи, отколкото очакваме. **Първо,** самият вирус може да се разпространи по-широко, отколкото предполагахме. И **второ,** дори ако предположенията ни за вируса са в голяма степен правилни, **икономическият спад** може да бъде по-голям, отколкото си мислим“, заявява изследователската фирма Capital Economics [12].

• **Цените на петрола спаднаха** с повече от **20 %** в понеделник (март 2020) – най-лошото им представяне от 1991 г. насам, на фона на разделението между Русия и Саудитска Арабия заради съкращението на производството. Това може да добави допълнителен натиск върху световната икономика и да доведе до по-нататъшни низходящи ревизии [12].

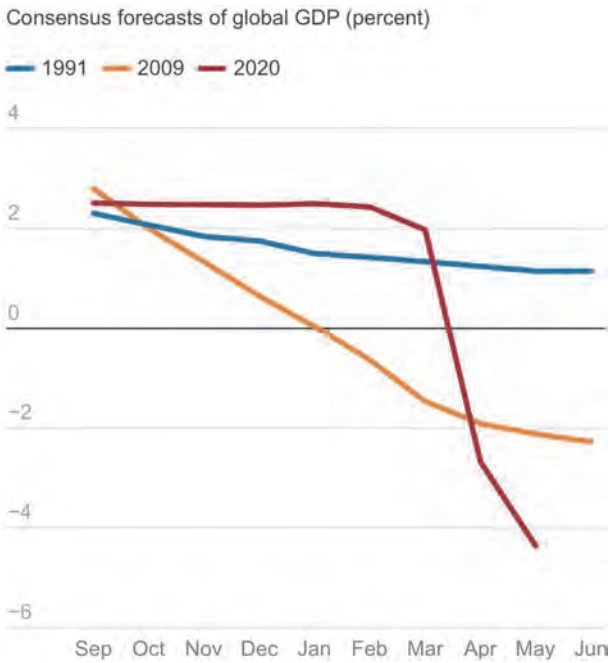
• „Намаляването на цените на петрола прави нещата още по-лоши за **глобалния БВП** в близко бъдеще, тъй като тези, които са засегнати от спада в цените на петрола (т.е. **производителите**), обикновено реагират на „болката“ по-бързо от онези, които се възползват от него (т.е. **потребителите**)“ – коментира Konstantinos Venetis – старши икономист в изследователската фирма TS Lombard (март 2020) [12].

Оценките на специалистите в момент на разразилата се ситуация в различни сфери на икономиката показват висок и рязък спад, като критичен потърпевш се предвижда производителят. **Експертите прогнозират,** че напредналите икономики ще се свият със **7 %.** Тази слабост ще обхване перспективите за развиващите се пазари и развиващите се икономики, за които се прогнозира, че ще се свият с **2,5 %,** когато се справят със собствените си вътрешни огнища на вируса. Това би представлявало най-слабото представяне на икономиката от поне 60 години.

Global Economic Prospects от юни 2020 г. описва както непосредствената, така и краткосрочната перспектива за въздействието на пандемията и дългосрочните щети, които тя е нанесла на перспективите за растеж. Базовата прогноза предвижда **свиване с 5,2 % на глобалния БВП през 2020 г.,** като се използват теглата на пазарния обменен курс – **най-дълбоката глобална рецесия от десетилетия,** въпреки изключителните усилия на правителствата да се противопоставят на спада с фискална и парична политика. В по-дълъг хоризонт се очаква дълбока рецесия, предизвикана от пандемията, да остави трайни белези чрез по-ниски инвестиции, ерозия на човешкия

капитал чрез загуба на работа и образование и фрагментация на световните връзки в търговията и предлагането [13].

Рецесията, създадена от Covid-19, отчита най-бързото и най-стръмно понижаване сред всички глобални рецесии от 1990 г. насам.



Източник: *Consensus Economics. World Bank [13].*

Регионалната икономика се очаква да се свие с **4,7 %,** с рецесии в почти всички държави, се посочва в доклад на **Global Economic за Европа и Централна Азия за юни 2020 г.**

• **Последни събития:** Пандемията Covid-19 се отрази неблагоприятно на **Европа и Централна Азия** чрез срив на световните цени на суровините, прекъсвания в глобалните и регионалните вериги за доставки и засилена неприязън към **риска на финансовите пазари.** Разширяването на вътрешните огнища на вируса засили спада на вътрешното търсене, влоши прекъсванията на предлагането и спря много дейности. Много от централните банки в региона отговориха на кризата, като увеличиха паричната подкрепа, а властите се намесиха на валутните пазари, за да стабилизират валутите си и да смекчат волатилността, като например в **Казахстан,** или използваха държавни фондове за благосъстояние, като например в

Азербайджан и Руската федерация. Тъй като възможностите за фискална политика са ограничени в много държави, политиците използваха съществуващите буфери или приоритизираха разходите за здравеопазване, мрежите за социална сигурност, подкрепата за частния сектор и противодействието на нарушенията на финансовия пазар. Докато редица държави обявиха пакети за фискална подкрепа, много икономики бяха зле подготвени за пандемията, като се има предвид ограниченият капацитет на здравеопазването.

• **Перспективи:** Регионалната икономика се очаква да се свие с **4,7 %,** с рецесии в почти всички държави. Перспективите предполагат, че правителствените ограничения постепенно ще се премахнат в началото на втората половина на годината. В сценарий, при който последиците от пандемията намаляват и търговията и инвестициите се възстановяват, растежът в Европа и Централна Азия ще нарасне с до 3,6 % през 2021 г. Икономическата активност в региона е уязвима към глобални разливи поради своята отвореност за търговия и финансови потоци, включително парични преводи. Освен това за износителите на енергия в региона, които включват **Русия, Казахстан и Азербайджан,** се очаква продължаващите ниски цени на петрола да тежат върху растежа. Очаква се **руската икономика да се свие с 6 %** тази година, което отразява скок в случаите на Covid-19 и срив в цените на петрола. Очаква се **турската икономика да се свие с 3,8 %** през 2020 г. при условие на спиране и продължаваща слабост в инвестициите. Очаква се икономическата активност да се свие във всички подрегиони през 2020 г., тъй като огнищата на вируса ограничават частното потребление и инвестициите: **Централна Европа с 5 %; Западните Балкани с 3,2 %; Южен Кавказ с 3,1 %; Източна Европа с 3,6 %; и Централна Азия с 1,7 %.** Въздействието върху икономическата дейност е силно несигурно и може да бъде по-сериозно, ако пандемията и свързаният с нея срив в дейността се увеличат. Най-тежко биха били икономиките със силни търговски и финансови връзки, включително парични преводи, към еврозоната или Русия.

• **Рискове:** Продължителната рецесия може да се отрази негативно на **вътрешните финансови сектори** и да увеличи **риска от финансова нестабилност.** Продължителното влошаване на инвестиционните отношения може да доведе до значителен спад на преките чуждестранни инвестиции [14].

Europe and Central Asia Country Forecasts
(Annual percent change unless indicated otherwise)

	2017	2018	2019e	2020f	2021f
GDP at market prices (2010 US$)					
Albania	3.8	4.1	2.2	-5.0	8.8
Armenia	7.5	5.2	7.6	-2.8	4.9
Azerbaijan	0.2	1.5	2.2	-2.6	2.2
Belarus	2.5	3.1	1.2	-4.0	1.0
Bosnia and Herzegovina[a]	3.2	3.7	2.6	-3.2	3.4
Bulgaria	3.5	3.1	3.4	-6.2	4.3
Croatia	3.1	2.7	2.9	-9.3	5.4
Georgia	4.8	4.8	5.1	-4.8	4.0
Hungary	4.3	5.1	4.9	-5.0	4.5
Kazakhstan	4.1	4.1	4.5	-3.0	2.5
Kosovo	4.2	3.8	4.2	-4.5	5.2
Kyrgyz Republic	4.7	3.8	4.5	-4.0	5.6
Moldova	4.7	4.3	3.6	-3.1	4.0
Montenegro	4.7	5.1	3.6	-5.6	4.8
North Macedonia	1.1	2.7	3.6	-2.1	3.9
Poland	4.9	5.3	4.1	-4.2	2.8
Romania	7.1	4.4	4.1	-5.7	5.4
Russia	1.8	2.5	1.3	-6.0	2.7
Serbia	2.0	4.4	4.2	-2.5	4.0
Tajikistan	7.6	7.3	7.5	-2.0	3.7
Turkey	7.5	2.8	0.9	-3.8	5.0
Turkmenistan	6.5	6.2	6.3	0.0	4.0
Ukraine	2.5	3.3	3.2	-3.5	3.0
Uzbekistan	4.5	5.4	5.6	1.5	6.6

Source: World Bank.
Notes: e = estimate; f = forecast. World Bank forecasts are frequently updated based on new information and changing (global) circumstances. Consequently, projections presented here may differ from those contained in other Bank documents, even if basic assessments of countries' prospects do not significantly differ at any given moment in time.
a. GDP growth rate at constant prices is based on production approach.

Източник: *World Bank.*

Омаловажавайки до голяма степен Covid-19, докато се разпространяваше в Китай, световните финансови пазари реагираха силно, когато вирусът се разпространи в Европа и Близкия изток, предизвиквайки страхове от глобална пандемия. Оттогава рисковете от Covid-19 се оценяват толкова значително, че някои се опасяват, че рецесията в световната икономика може да бъде предрешена. През периода на първите две тримесечия на 2020 г. (както отчитат и анализите) не се забелязва дори и възстановяване до първоначалните нива на икономиката.

Как би изглеждала предизвиканата от Covid-19 рецесия, посочена и от **Harvard Business Review** (списание, издавано от Harvard

Business Publishing – дъщерно дружество, притежавано изцяло от Харвардския университет) [15].

Рецесиите обикновено попадат в една от трите категории:

• **Истинска рецесия.** Класически това е бум, който се превръща в провал и „дерайлира“. Но тежките екзогенни шокове на търсенето и предлагането, като войни, бедствия или други смущения, също могат да тласнат реалната икономика към свиване.

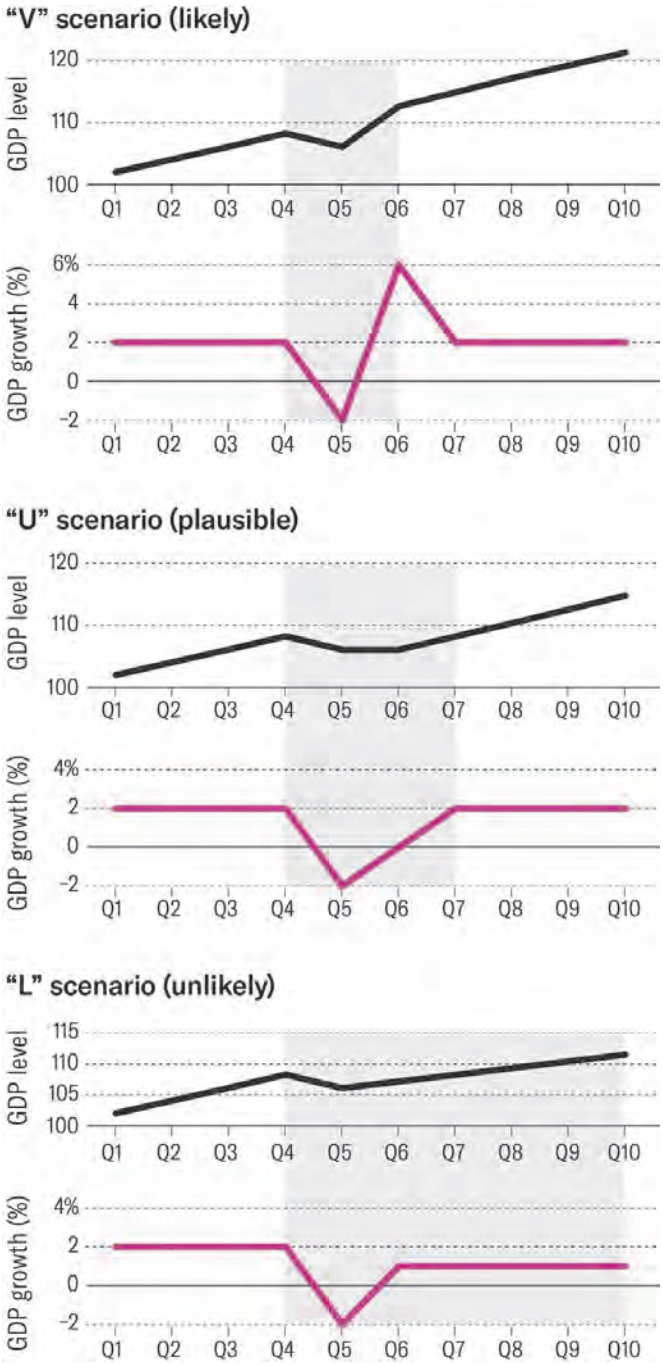
• **Рецесия на политиката.** Когато централните банки оставят лихвените проценти твърде високи в сравнение с „неутралния“ процент на икономиката, те затягат финансовите условия и кредитното посредничество и със закъснение спират експанзията. Този риск остава скромен – извън щатските ставки вече са на дъното или дори отрицателни, докато Федералният резерв направи изненадващо намаляване на 50 базисни точки. Министрите на финансите на Г-7 също обещаха фискална подкрепа.

• **Финансова криза.** Финансовите дисбаланси са склонни да се натрупват бавно и за дълги периоди от време, преди бързо да се развият, нарушавайки финансовото посредничество и след това реалната икономика. Има известни разлики в световен мащаб, но в критичната американска икономика е трудно да се посочат рисковете от финансовата криза. Трудно е да се види, че Covid-19 допринася за финансов дисбаланс, но стресът може да възникне от напрежение в паричния поток, особено в малките и средните предприятия (МСП) [16].

Според икономическата прогноза за 2020 г. икономиката на еврозоната ще се свие с рекордните 7 и 3/4 %. В ЕС се очаква равнището на безработица да се увеличи до 9 % през 2020 г., след което да спадне до около 8 % през 2021 г. Очаква се изключително висока степен на (НЕ)сигурност и рискове от влошаване на прогнозните стойности **(това са прогнозите на europa.eu – официален сайт на EU, към 6 май 2020 г.).**

Harvard Business Review разработва разширен сценарий, който описва като „V – U – L“:

• **V-образен.** Този сценарий описва „класическия“ шок в реалната икономика, изместване на производството, но в крайна сметка растежът се възстановява. При този сценарий годишните темпове на растеж могат напълно да поемат шока. Въпреки че може да изглежда оптимистично в днешния „мрак“, се смята, че сценарият е правдоподобен.



Източник: *BCG Center for Macroeconomics analysis.*

• **U-образен.** При този V-сценарий шокът продължава и докато първоначалният път на растеж се възобнови, има известна трайна загуба на продукция.

• **L-образен.** Този сценарий е най-грозната и лоша връзка на V и U. За да се осъществи това, ще трябва Covid-19 да нанесе значителни структурни щети, т.е. да наруши нещо в сферата на икономиката – пазара на труда, формирането на капитал или функцията на производителността.

Силният предизвикан спад или дори срив в икономиката предизвиква редица поводи за притеснение в различни сфери. Най-потърпевши остават производителите на суровини и продукти, тези, от които зависи формирането на БВП в една държава. Не на последно място са и услугите. Един от най-силно **засегнатите сектори е транспортният.**

КОНТЕЙНЕРНОТО КОРАБОПЛАВАНЕ В ГЛОБАЛЕН АСПЕКТ В МОМЕНТ НА КРИЗАТА COVID-19

Обемът на глобалната контейнерна търговия е намалял с **8,6 % през февруари 2020 г.** в сравнение със същия месец на 2019 г. Официалните данни за март 2020 г. вероятно ще отбележат по-голям спад. Спадът в търговията с контейнери беше особено **изразен в Далечния изток.**

В **Европа, Северна Америка и Океания** също е значително, докато все още не се забелязва в други нововъзникващи икономики **(Латинска Америка, Африка – на юг от Сахара и Индийския субконтинент, и Близкия изток).** Таблицата по-долу изброява промените през **януари и февруари 2020 г.** в различните световни региони [17].

Table 1. Changes in container trade volume by world region, 2020

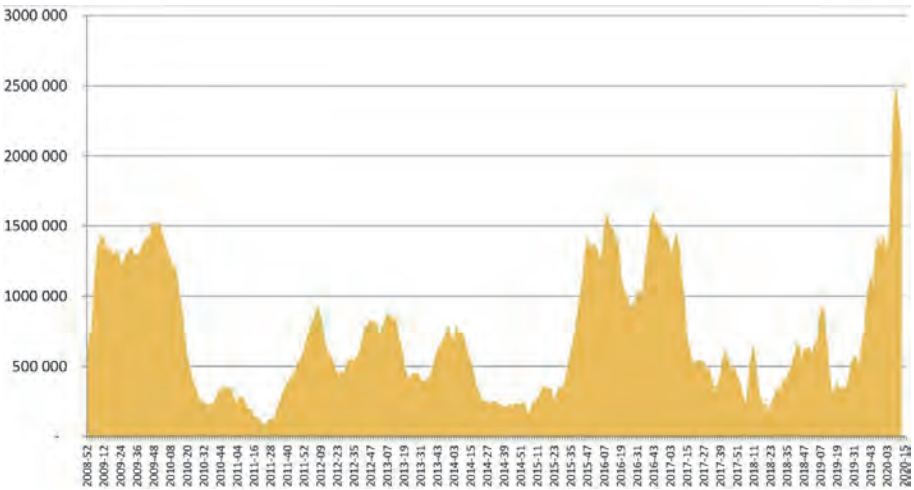
	Change Jan 2019 to Jan 2020 (%)	Change Feb 2019 to Feb 2020 (%)
Far East	0.0	- 17.5
Europe	0.7	- 4.0
North America	- 0.3	- 7.0
Australasia and Oceania	- 6.5	- 2.8
Indian Subcontinent and M. East	3.7	6.1
South and Central America	2.4	2.8
Sub-Saharan Africa	5.4	7.4

Източник: *International Transport Forum. CTS.*

Главният отговор на превозвачите на намаляващото търсене е намаленото предлагане. Корабните оператори отчитат силен спад и бездействие на плавателните съдове, като зачестява отмяната на услуги. Тези „празни“ плавания са се увеличили значително в сравнение с предходни години – със **188 през февруари/март 2020 г., от които 85 са в Северна Азия** [17].

Обявени са още анулирания. Те се отнасят до **30 %** от капацитета за обслужване в далечна **Източна Европа** и до **20 %** от капацитета за обслужване на **Тихия океан.**

Делът на **празните ходове** на контейнерните кораби достига **2,5 млн. (TEU),** или 10,6 % от капацитета в началото на **март 2020 г.** [17]**.**



Източник: *International Transport Forum. Alphaliner.*

КОЛКО ЛОШО КРИЗАТА С КОРОНАВИРУСА ЩЕ ЗАСЕГНЕ ГЛОБАЛНИТЕ ТОВАРНИ ПРЕВОЗИ

Мобилните ограничения в момент на Covid-19 могат да намалят глобалния товарен транспорт с до **36 % до края на 2020 г.** според симулация на **Международния транспортен форум** (ITF).

Градският транспорт на стоки е по-устойчив, тъй като увеличеното онлайн пазаруване добавя доставки. Емисиите на CO_2, свързани с товарни превози, значително намаляват [18].

Настоящите ограничения по отношение на мобилността по света вероятно ще доведат до силно **намаляване на глобалния обем на товарния транспорт през 2020 г.** с повече от 1/3. Като

цяло товарният транспорт, измерен в тон-километри, се очаква да бъде с **36 % под нивото, предвидено без Covid-19 за тази година.** Извънградската товарна дейност, т.е. националните и международните превози на стоки извън градовете, може да бъде с **37 %** по-ниска като цяло в сравнение с прогнозата за глобални обеми на товарни превози през 2020 г. Регионалните различия са значителни. Прогнозира се **намаление** с повече от половината за държавите от **ASEAN (Association of South-East Asian Nations), Русия/Централна Азия и Индия.** За **Китай** въздействието е малко над **1/4 по-малко** товарни превози. **Европа и Америка** са в средата на диапазона, с **намаления от около 40 %**; само държавите от **Андите** се очаква да бъдат засегнати по-силно – с **50 % спад** в извънградската товарна дейност [18].

Прогнозирано въздействие на Covid-19 върху товарите и свързаните с тях емисии на CO_2 за 2020 г. (по регион и вид товар, процентно изменение на прогнозите преди Covid-19) [18]

Regions	Urban freight activity	Inter-urban freight activity	CO_2 emissions urban freight	CO_2 emissions inter-urban freight
ASEAN countries	-16	-53	-22	-42
China	-3	-27	-10	-23
India	-14	-51	-20	-46
Japan and Korea	-10	-33	-17	-26
Russia and Central Asia	-6	-53	-13	-54
Other Asia	-5	-32	-12	-25
Oceania	-3	-42	-10	-41
Middle East	-6	-36	-13	-31
North Africa	-15	-36	-21	-25
Southern Africa	-12	-32	-19	-41
Other Africa	-10	-50	-16	-38
South America (Andean)	-14	-50	-20	-37
South America (South Cone)	-5	-35	-12	-31
Caribbean	-15	-43	-21	-39
Central America	-12	-39	-19	-35
North America	-10	-37	-17	-35
Scandinavia	-15	-41	-21	-37
Western Europe	-12	-43	-19	-37
Eastern Europe	-14	-40	-20	-36
Global	-8	-37	-14	-30

Източник: *Urban freight activity. https://www.itf-oecd.org/sites/default/files/global-freight-covid-19.pdf.*

Товарният транспорт в градовете може да се очаква да бъде засегнат значително по-малко от националния и международния превоз на товари. Актуализираните прогнози показват, че градската товарна дейност е с 8 % под прогнозата, което все още не отразява никакво въздействие на Covid-19. Една от причините за това е **ръстът на онлайн пазаруването** по време на блокирането в много държави, което води до повече **доставки на покупки чрез електронна търговия.** С това явление е свързан и повишеният брой превозни средства, доставящи стоки в градовете въпреки все още значителния спад в обема.

Прогнозираното въздействие на Covid-19 върху товарната дейност през 2020 г. би довело до намаляване на свързаните с това емисии на CO_2 от 28 %. Емисиите на въглероден диоксид от националните и международните товарни превози ще бъдат близки **до 1/3 (30 %) по-ниско** от прогнозираното без въздействието на Covid-19. За градските товарни превози спадът е наполовина по-голям **(14,5 %),** но все пак значим. **Най-силно намаление на емисиите ще се случи в Руската федерация и Централна Азия – с 54 %.**

Във всички останали региони намаленията на CO_2 не достигат 50 %, въпреки че все още са големи. Само в **Китай** се регистрира **по-малко от 25 % намаление на емисиите на CO_2** от извънградски товарни превози. За градските доставки спадът на CO_2 варира от 10 % до малко над 20 %, като повечето региони са в горния диапазон [18].

ДА „ВНЕДРИШ“ БЪДЕЩЕТО ВЪВ ВРЕМЕ НА (НЕ)СИГУРНОСТ. (КИБЕРСИГУРНОСТ)

На 15 април 2020 НАТО призова съюзниците, изправени пред икономическите трудности, породени от епидемията от **Covid-19,** да не се изкушават да продават критична инфраструктура и производства на съперници. Генералният секретар на Алианса **Йенс Столтенберг** отбелязва, че дългосрочните геополитически последици от епидемията могат да бъдат значителни.

„Някой може да използва новите икономически трудности, за да се опита да инвестира в инфраструктура и производства. Това може да доведе до заплаха за нашата сигурност“ – посочва Столтенберг [19].

Един от най-големите военни историци – **Joseph V. Micallef,** е на мнение, че свързаните по-специално с коронавируса грипоподобни заболявания имат последствия от геополитически характер.

А познатите ни вече щамове **SARS и MERS** бяха само предупреждение за потенциално пагубните ефекти и **Covid-19** е още едно напомняне. Германският професор обаче допълва, че тепърва човечеството го очакват по-големи изпитания от пораженията на **коронавируса.**

Само няколко седмици бяха необходими в началото, за да се убедим, че икономическите последствия придобиват лавинообразен характер. Но трябваше ли едва сега да констатираме, че повечето големи компании и правителства реално нямат план „В“ за справяне с такива огнища или въздействия върху своите вериги, мрежи за доставки, пазарни операции, градове и държави?

Няма достатъчна координация между различните държави за това как да се реагира в подобна ситуация, и то навреме, за да се избегнат огромните загуби и погубващата икономиките рецесия.

Избухването на Covid-19 е обявено за пандемия от **СЗО,** което води до огромно въздействие върху живота на хората, семействата и общностите. Това е оказало незабавен ефект върху организациите, променяйки начина на работа на служителите и донасяйки със себе си нови **рискове за киберсигурността.**

Тъй като международният отговор продължава да се развива, знаем, че организациите са изправени пред потенциално значими предизвикателства, на които трябва да реагират бързо. Много организации и служители се нуждаят от преосмисляне на начина на работа в светлината на значителни оперативни и финансови предизвикателства. Без подходящи съображения това може фундаментално да увеличи риска от атаки за киберсигурността.

Виждаме както увеличаване на вероятността и въздействието от кибератаки, така и добри практики в областта на киберсигурността, които е възможно да са незначителни, тъй като организациите стават по-зависими от всякога от технологиите. Също така започваме да наблюдаваме промяна на характера на заплахата, тъй като нападателите използват **(НЕ)сигурността,** безпрецедентни ситуации, бързи ИТ и организационни промени [20].

Само ще отворя една скоба за няколко важни момента, които ще разгледаме по-подробно в темата, като внедряването на **5G** мрежата например. Мащабите на нейното реализиране по света са огромни. Очаква се **5G** да се използва с търговска цел в Европа, като инвестициите възлязат на над **1 млрд. €.**

Приходите в Европа, които се очакват от употребата на новата, пета, генерация мрежа, се прогнозират на **250 млрд. € до 2025 г.**

Сами си даваме сметка каква „битка“ ще се разразява тепърва в сферата на телекомуникациите и борба за обезпечаване на сигурността за спокойно и сигурно ползване на услугите. **Както посочват експерти, най-важното предварително условие преди внедряването на 5G е киберсигурността.**

Еврокомисарят по сигурността Джулиан Кинг заявява: *„Устойчивостта на нашата цифрова инфраструктура има ключово значение за правителствата, бизнеса, сигурността на нашите лични данни и за функционирането на демократичните ни институции. Трябва да изработим европейски подход за защитата на интегритета на 5G, който ще представлява цифровото скеле на взаимносвързания ни живот*“ [21].

Организациите трябва да предприемат три ключови действия за смекчаване на тези възникващи рискове и възможни хакерски заплахи:

- опазване на своите новоприложени дистанционни работни практики;
- осигуряване на приемствеността на критичните функции за сигурност;
- противодействие на опортюнистичните заплахи, които е възможно да търсят да се възползват от ситуацията.

Поддържането на бизнес операции ще бъде приоритет в условията на криза.

Приоритетите ще се изместят, тъй като много организации се подготвят или опитват различни финансови и оперативни предизвикателства. Това може да доведе до деприоритизиране на ИТ и киберсигурността, намаляване на бюджетите или поне до несигурно бъдеще. Това може да повлияе на планираните програми за сигурност и подобряване на ИТ и може да забави важни дейности, включително тези, които правят организациите по-устойчиви на киберзаплахи.

По-малкият брой на работната сила може да намали ефективността.

Тъй като въздействието на Covid-19 върху обществото се увеличава и нивата на инфекция нарастват, вероятно е по-голям брой работещи да отсъстват, особено когато се насочваме към пикови периоди на инфекции. Онези, които остават, вероятно ще бъдат по-малко ефективни поради увеличаване на допълнителния натиск или общите притеснения относно ситуацията.

Работната сила бързо ще премине към работа от разстояние и ще се нуждае от технология в подкрепа на това.

Преминаването към отдалечена работа както в мащаб, така и темпово, вероятно ще доведе до значително въздействие, променяйки както изискванията на ИТ инфраструктурата, така и направлението на атаката. Това ще доведе до значителен натиск върху екипите за сигурност, които могат да бъдат пренасочени към подкрепа на общите ИТ операции или към бързо модифициране на процеси и технологии, за да се адаптират към променящия се риск.

Критичните доставчици ще намалеят, което потенциално ще прекъсне ключови дейности по сигурността.

Веригите на доставки на организациите също ще бъдат засегнати и това може да доведе до смущения в предоставянето на услуги. Това вероятно ще включва критични елементи от веригата за доставки на сигурност, например изнесени експлоатационни центрове за сигурност, екипи за управление на промените и защитна „стена".

Организациите ще стават все по-зависими от технологията за отдалечен достъп, включително от технологията, с която служителите им не са запознати.

Тъй като организациите се отдалечават от физическите си помещения и стават все по-зависими от технологията за отдалечен достъп, всяко прекъсване, причинено от атаки към киберсигурността или прекъсвания на ИТ, ще има значително по-голямо оперативно въздействие. Освен това обичайните физически решения, използвани за преодоляване на тези проблеми, е възможно да не са налични [22].

Как всичко това може да повлияе на риска за киберсигурността на организациите?

Работници, намиращи своя нормален сигурен метод за споделянето на файлове за неприемливо бавен при работа от вкъщи, могат да прибегнат до използване на безплатни и непроверени услуги като алтернатива. Служителите могат да бъдат по-податливи на атаки, тъй като нападателите се възползват от увеличеното натоварване на служителите, непознатите начини на работа и повишените нива на стрес. Широкоразпространената работа от разстояние ще накара служителите да разчитат на невербални начини на взаимодействие с колеги, което означава, че съществуващите неформални методи на потвърждаване на легитимността на комуникациите са по-малко ефективни.

Разчитането на системи за отдалечен достъп може да направи организациите по-уязвими към разпределени атаки за отказ на услуга (DDoS) – „отказ от обслужване". Поддържането на надежд-

ността на системите за отдалечен достъп ще стане критично за бизнес операциите, тъй като служителите работят отдалечено. Системите за отдалечен достъп могат да бъдат насочени към нападатели с атаки за отказ на услуга, които искат да нарушат бизнес операциите или да пристъпят към изнудване.

От служителите ще се изисква да работят с технологии, с които не са запознати (напр. инструменти за дистанционно сътрудничество), което може да доведе до въвеждане на нови рискове за сигурността, повишени нива на стрес, докато работят по начин, по който не са свикнали. Това може да доведе до нови рискове, тъй като технологиите се използват неподходящо, неправилно са конфигурирани или не се използват с нужните мерки за сигурност, които са били предвидени при проектирането им.

Организациите е възможно да не откриват ефективно кибератаките, тъй като екипите за сигурност не разполагат с персонал или са пренасочени да извършват други дейности, оставяйки сигналите за сигурност неразследвани. Организациите е възможно да не са в състояние ефективно да реагират и да не могат да се възстановят от атаки на киберсигурността, тъй като ключови служители от сигурността, доставчици на ИТ и по-широкият бизнес могат да не са на разположение, за да подкрепят вземането на решения и усилията за реагиране. Това вероятно е особено вярно за организации с по-ниска зрелост, които разчитат на ключови индивиди, вместо да имат напълно документирани и широко репетирани процеси.

Дистанционната работа в краткосрочен и средносрочен план вероятно ще доведе до промени в поведението и културата на организациите в бъдеще и в техните подходи към дистанционната работа. Технологията ще бъде от ключово значение за това, тъй като организациите вероятно ще преместят повече от своите приложения в облака за е-поща, съхранение на файлове и т.н. Тези технологии носят със себе си нови рискове, но също така позволяват на екипите за сигурност да проектират сигурност в самото начало и да се отдалечат от наследените ИТ [22].

Основни рискове за киберсигурността на микро-, малки и средни предприятия (ММСП) в контекста на кризата Covid-19

За да осигурят непрекъснатост на бизнеса, да защитят работниците и да продължат да обслужват клиентите по време на пандемията **Covid-19,** много организации преместват значителни части от своите операции онлайн. След кризата се наблюдава нарастване на използването на онлайн и цифрови инструменти предимно за подпомагане на комуникацията. Това създава нови възможности за

злонамерени участници да се възползват от разрушителните ефекти на кризата и да се насочат към **микро-, малки и средни предприятия** за кибератаки.

Още преди настоящата криза **ММСП** все по-често са ставали обект на **кибератаки** поради липсата на ресурси за прилагане на цялостни решения за киберсигурност. Неотдавнашен доклад предполага, че **малкият бизнес е обект на над 40 % от кибератаките, със средна загуба на атака от над 188 000 щатски долара.** Киберпрестъпниците са се възползвали от използваните инструменти на части от **ММСП** за защита на своите операции и са използвали **ММСП** като „най-слабото звено" за използване на връзките им с по-големи компании от веригата на доставки. **През 2019 г. се изчислява, че едно от пет ММСП е станало жертва на атака на рансъмуер (ransomware). Фишинг (phishing) атаките също са достигнали най-високото си ниво от 3 години насам,** като малки организации получават злонамерени имейли с по-висок процент.

Мащабното използване на технологии от вкъщи, повишената активност в мрежите, насочени към клиентите, и по-широко използване на онлайн услуги от **ММСП** в отговор на мерките за блокиране на **Covid-19** влошиха тези рискове, предизвиквайки огромен стрес за контрола на киберсигурността, който киберпрестъпниците са използвали бързо. Сега с повишени рискове за сигурността е жизненоважно компаниите да могат да идентифицират заплахите за киберсигурността и ефективно да управляват своите информационни системи по време на настоящата криза като част от плановете им за непрекъснатост на бизнеса [23].

Лесни стъпки за ММСП за защита на бизнеса от заплахи за киберсигурността по време на кризата Covid-19:

Да се повиши информираността в рамките на организацията **– служителите трябва да са първата линия на защита срещу кибератаките.**

През 2018 г. над 50 % от инцидентите с пробив в сигурността са резултат на човешка грешка, а не на умишлена атака. Освен това много инциденти със сигурността, които са резултат от умишлена атака, могат да бъдат избегнати, ако хората предприемат подходящи стъпки. **Служителите трябва да разбират ежедневните си отговорности при работа, защита и подкрепа на фирмени данни и мрежи.** Това включва прости стъпки, като:

- избор на надеждни пароли и осигуряване на отговорно използване на имейли;

• важно е служителите да бъдат информирани за възможни измами и злонамерен софтуер, за да разпознават, да се въздържат от споделяне и да докладват навреме за злонамерен материал;

• ММСП трябва също да прилагат политики за цялата компания, които създават култура на информационна сигурност, която забранява използването на нелицензиран софтуер, да актуализират редовно целия софтуер, за да помогнат за отстраняване на недостатъците в сигурността, и да установяват правила за безопасно сърфиране.

Укрепване на политиката и процедурите за управление на отдалечения достъп на работа – ММСП трябва да се борят с все по-сложна среда за отдалечен достъп в светлината на бързия ръст на работата от разстояние и разпространението на устройства (телефони, лаптопи, таблети, независимо дали са собственост на компания, лични, споделени, обществени или комбинация от тях), както и с различните начини на свързване с интернет (домашен или обществен wi-fi, предоставена от компанията гореща точка) и за достъп до фирмени данни (виртуална частна мрежа, облачна технология или др.). Ето защо е важно ММСП да определят ясни насоки за своите служители по отношение на правилното използване на отдалечен достъп. **Като общо правило издадените от компанията устройства трябва да се предпочитат пред лични или обществени устройства.** По същия начин частните мрежи и издадените от компанията горещи точки трябва да бъдат предпочитани пред публичните мрежи, като се **забранява използването на VPN.** За достъп и споделяне на документи трябва да се използват системи, базирани на облак, централизирани системи за споделяне на файлове или специален сайт за споделяне на файлове с фирмен надзор.

Сигурни портали за доставчици и други външни системи.

От решаващо значение е **ММСП да картографират, оценят и управляват всички входни точки с основна цел да направят информационните системи непробиваеми за външно манипулиране.**

Бързите практически стъпки включват:

• актуализиране и корекция на софтуер;

• актуализиране на пароли и насърчаване на многофакторно удостоверяване. Това също така води до по-добра комуникация с бизнес партньори за осигуряване на мрежи по веригата на доставки;

• показването на лидерство в киберсигурността може да повиши цялостната устойчивост по веригата на доставки и да укрепи

пълномощията на ММСП със съществуващи или потенциални бизнес партньори.

Актуализиране на плановете за реагиране при инциденти в поразпределена среда.

Поради еволюционния характер на киберзаплахите **дори добре защитени компании могат да получат пробиви в сигурността.** Фирмите работят в среда, в която рискът може да бъде сведен до минимум, но не напълно отстранен. **Бързата реакция** е от решаващо значение за смекчаване и където е възможно, ограждане на разрушителните ефекти от атака. **Успешното управление** на инциденти включва ясна комуникационна стратегия както с вътрешни, така и с външни заинтересовани страни, както и подкрепа от специализирани трети страни за подпомагане на овладяването и отстраняването на инцидента. **ММСП** трябва също така да се ангажират активно с правоприлагащите и специализираните агенции за надзор, за да помогнат за справяне с все по-сложните киберзаплахи.

По отношение на риска от кибератаки в настоящата криза е важно също така **ММСП** да следват правителствените насоки и препоръки, издадени от националните екипи за реагиране при извънредни ситуации. **Политиците се призовават да предоставят актуална и изчерпателна информация за местните специфични заплахи за киберсигурността, с които се сблъсква бизнесът** [23].

ГАРАНТИРАНЕ НА КИБЕРСИГУРНОСТТА ПО ВРЕМЕ НА КОРОНАВИРУСА В ЕС

С разпространението на пандемията от коронавирус по света Европейският съюз и неговите държави членки са свидетели на киберзаплахи и злонамерени действия, насочени срещу основни оператори в държавите членки и техните международни партньори, включително в сектора на здравеопазването. От началото на пандемията са установени значителен брой кампании за разпространение на фишинг и зловреден софтуер, разкрити са дейности по сканиране и разпределени атаки, тип „отказ от обслужване“ (DDoS), някои от които засягат критични инфраструктури, които са от съществено значение за управлението на тази криза.

Европейският съюз и неговите държави членки споделят обща визия за киберзаплахите и са решени да ги предотвратяват, обезкуражават, възпират и да им отговарят, по-специално чрез непрекъснат обмен на информация и сътрудничество при инциденти,

както и чрез използването на рамката за съвместна дипломатическа реакция на ЕС срещу злонамерени действия в киберпространството. За тази цел Европейският съюз и неговите държави членки допълнително ще засилят сътрудничеството си на техническо, оперативно, съдебно и дипломатическо равнище, включително със своите международни партньори. Европейският съюз и неговите държави членки призовават всички държави да извършват надлежна проверка и да предприемат подходящи действия срещу онези, които извършват такива дейности на тяхна територия, в съответствие с международното право и консенсусните доклади от 2010, 2013 и 2015 г. на групата държавни експерти на ООН в областта на информацията и телекомуникациите в контекста на международната сигурност [24].

ЕС налага първите по рода си санкции срещу инициатори на кибератаки (30 юли 2020 г.).

• Съветът реши да наложи ограничителни мерки срещу шест физически лица и три образувания, отговорни за различни кибератаки или участвали в такива. Сред тях са опитът за кибератака срещу **ОЗХО (Организацията за забрана на химическото оръжие)** и известните в публичното пространство като **WannaCry, NotPetya и операция „Cloud Hopper“** [25].

• Наложените санкции включват **забрана за пътуване и замразяване на активи.** Наред с това на лицата и образуванията от ЕС е забранено да предоставят средства на вписаните в списъка със санкции [25].

• Санкциите са една от възможностите, които предоставя **инструментариумът на ЕС за кибердипломация за предотвратяване, възпиране и реагиране на злонамерени действия в киберпространството, насочени срещу ЕС** или неговите държави членки, и **днес ЕС използва за първи път този инструмент** [25].

Целенасочените ограничителни **мерки** имат **превантивен и възпиращ ефект** и трябва да се разграничават от възлагането на отговорност на трета държава.

ЕС запазва ангажимента си за глобално, отворено, стабилно, мирно и сигурно киберпространство и във връзка с това отново изтъква необходимостта от укрепване на международното сътрудничество с цел насърчаване на основания за правила и ред в тази област [25].

Изчитайки всичко, написано дотук, и проследявайки хронологично събитията през периода, се наблюдава тенденциозна (НЕ)сигурност на икономиката, хората и това какво ново бъдеще всъщност

ни очаква. Ние всички подготвени ли сме вече за него, за да можем плавно и сигурно да навлезем в тази нова ера, без да бъдем изненадани, но да бъдем информационно защитени? Правителствата готови ли са, оценяват ли рисковете при евентуални подценявания на новото бъдеще, което ни чука на вратата? Бизнесът готов ли е да обезпечи и той с достатъчно съвременни методи и техника за сигурност новите дистанционни методи на работа на най-значимия си капитал – работниците?

Това са въпроси, на чиито различни отговори дълго време ще попадаме поради гъвкавостта на неуморното развитие на телекомуникациите и в частност на цифровизацията, която видимо или невидимо ни обгръща.

За първи път човечеството живее в ситуация, когато хоризонтът на овеществения свят се променя няколкократно в рамките на един човешки живот.

Тази ситуация е уникална. Как да се ориентираме в произхождащото и още по-трудното – как да надникнем в бъдещето, което е все по-неочаквано, бързо пристигащо и все по-често ни заварва неподготвени? Сблъскваме се с маса проблеми, но безусловно един от тях е водещ и той е този за сигурността [1].

Литература

1. **Радулов,** Н. Сигурност 4.0. Сигурност и четвърта промишлена революция Security 4.0. Сигурност и Четвъртата индустриална революция. – В: *Сигурност* 4.0. Сигурност и четвърта промишлена революция. Сборник доклади от научна конференция на НБУ – ВТ 25 – 26.10.2018. София: НБУ, 2018. ISSN 2367-7465.
2. *https://bg.m.wikipedia.org/wiki/Пандемия_от_коронавирус_(2019_–_2020)*
3. *https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(20)30746-7/fulltext#fig1*
4. *http://wjw.beijing.gov.cn/*
5. *http://wsjkw.sh.gov.cn/*
6. *http://wjw.sz.gov.cn/*
7. *http://wjw.wenzhou.gov.cn/*
8. *https://www.researchgate.net/publication/340521939_First-wave_COVID-19_transmissibility_and_severity_in_China_outside_Hubei_after_control_measures_and_second-wave_scenario_planning_a_modelling_impact_assessment*
9. *https://www.aa.com.tr/en/asia-pacific/covid-19-surges-in-australia-no-local-cases-in-china/1903456*
10. *https://www.worldometers.info/coronavirus/*
11. *https://www.worldometers.info/coronavirus/*

12. *https://www.google.com/amp/s/www.cnbc.com/amp/2020/03/10/coronavirus-analysts-cut-global-growth-forecasts-as-epidemic-spreads.html*
13. *https://www.worldbank.org/en/news/feature/2020/06/08/the-global-economic-outlook-during-the-covid-19-pandemic-a-changed-world*
14. *http://pubdocs.worldbank.org/en/344691588788182868/Global-Economic-Prospects-June-2020-Regional-Overview-ECA.pdf*
15. *https://en.m.wikipedia.org/wiki/Harvard_Business_Review*
16. *https://www.google.com/amp/s/hbr.org/amp/2020/03/what-coronavirus-could-mean-for-the-global-economy*
17. *https://www.itf-oecd.org/sites/default/files/global-container-shipping-covid-19.pdf*
18. *https://www.itf-oecd.org/sites/default/files/global-freight-covid-19.pdf*
19. *https://m.dir.bg/dnes/politika/izvanredna-sreshta-na-voen-nite-ministri-v-nato-v-tarsenena-strategii-sreshtu-covid-19*
20. *https://www.pwccn.com/en/issues/cybersecurity-and-data-privacy/covid-19-impact-mar2020.pdf*
21. *https://ec.europa.eu/commission/presscorner/detail/bg/*
22. *https://www.pwccn.com/en/issues/cybersecurity-and-data-privacy/covid-19-impact-mar2020.pdf*
23. *https://iccwbo.org/content/uploads/sites/3/2020/05/2020-icc-sos-cybersecurity.pdf*
24. *https://www.consilium.europa.eu/bg/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/*
25. *https://www.consilium.europa.eu/bg/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/*