инструмента, които трябва да са налични за всяка компания, независимо дали е МСП/МП или нестопанска организация, като университет. Това са инструментите за видеоконференции; управление на проекти и системи за управление на електронно обучение.

Инструментите за видеоконференции стават задължителни за свързване на членове на отдалечени екипи, включително екипи от бизнес компании, организации с нестопанска цел, университети, правителство и др. Тези инструменти могат да са изцяло безплатни или да предлагат безплатна версия с ограничена функционалност, като осигуряват свързаност в екипа чрез виртуални стаи. Някои от най-широко използваните платформи за видеоконференции са: Zoom, Google Meet, Cisco Webex Meetings, Microsoft Teams, Slack, GoToMeeting и други.

Платформите за управление на проекти позволяват проследяване на различни дейности по проектите и осигуряват гъвкаво решение, което комбинира различни набори от инструменти, възможности и функционалности. Те помагат за постигане на организационните цели чрез управление, проследяване, комуникация и отчитане на дейности по проекта, като време, ресурси, разходи и ограничения в обхвата. Много МСП от всички индустрии вече използват уеб-базиран софтуер за управление на проектите си. Този тип софтуер използва облачни технологии и се предлага от доставчиците като услуга (SaaS). Списъкът на популярните платформи за управление на проекти включва: Scoro, Zoho, Nifty, monday.com, ProofHub, Clarizen, Project Manager, JIRA и др.

Системите за управление на обучението са фокусирани върху обучението и стоят в основата на предоставянето на образователна или обучителна услуга. Управлението на графиците на учебната програма за всеки отделен човек е важна функционалност. Бизнесът може да извлече ползи от този тип софтуер, като предоставя обучителни курсове с цел по-добро разбиране на работните системи и процеси или за подкрепа на обучението в областта на киберсигурността. Някои популярни такива са: Moodle, TalentLMS, Forma LMS, Chamilo и т.н.

През последната година екип от ИИКТ работи активно по подготовката на курсове за сертифициране по киберсигурност и системна администрация.

Третото направление, върху което ГИМ трябва да се съсредоточи в рамките на COVID-19 пандемията, е свързано с осигуряване на сигурността на данните в условията на отдалечена работа. С помощта на правилните инструменти, които са устойчиви, сигурни и мащабируеми, ГИМ трябва да поддържа служителите на организацията свързани, продуктивни и в сътрудничество. Постигането на максимална ефективност и сигурност при оптимизиране на ефективността на разходите, изглежда невъзможно при тези нови мащаби. За да осигурят необходимата киберсигурност, ГИМ трябва да бъдат в тясно сътрудничество с главния служител по сигурността на информацията.

Главен мениджър по информационна сигурност

Главен мениджър по информационна сигурност (ГМИС) отговаря за сигурността на информацията и данните на организацията. Ролята на ГМИС е да създаде стратегия, която се фокусира върху непрекъснато нарастващата регулаторна сложност, създавайки политики, архитектура на сигурността, процеси и системи, които помагат за намаляване на кибер заплахите и запазване на данните. Спазването на стандарти е ключов елемент от ролята, както и разбирането и управлението на риска.

Съществува списък на технически умения, които ГМИС би трябвало да притежава, надграждащи основите на програмирането и системното администриране, каквито се очаква да имат всички квалифицирани специалисти във високите технологии. ГМИС също трябва да има разбиране за някои технологии, ориентирани към

	сигурността, като DNS, маршрутизация, удостоверяване, VPN, проксиране, техники за намаляване на DDOS заплахите, техники за кодиране, етично хакване и моделиране на заплахи, защитни стени и протоколи за откриване и предотвратяване на пробиви.
Отговорности на ГМИС	ГМИС управляват цялостната информационна сигурност на компаниите. ГМИС идентифицира слабостите в съществуващите технологии и програми за информационна сигурност. Чрез сътрудничество с ръководители и екипи от експерти по сигурността на ИТ, тези специалисти разработват политики за сигурност и практики за защита на информацията. ГМИС въвежда нови технологии и контролира образователните програми за сигурност на персонала. Допълнителните задължения включват изготвяне на бюджети и финансови прогнози за операции и поддръжка на сигурността. ГМИС разпределят финансови ресурси, координират усилията при разследване на проблеми и възстановяване на данни, извършват оценки на риска и одити, с цел да се гарантира спазването на приложимите разпоредби и закони.
ГМИС в условията на COVID пандемия	Работата от вкъщи по време на пандемията от COVID-19 поставя нови предизвикателства пред операциите по киберсигурност. Поради това, експертите по киберсигурност трябва да заемат по-стратегическа лидерска роля. Те трябва да преминат отвъд следенето за спазване на изискванията, като се интегрират по-добре с бизнеса, управлявайки стратегически информационните рискове и работейки за изграждане на култура за споделен кибер-риск в организациите. Ето някои въпроси, които ще повишат ефективността на въздействието между лидерите и ГМИС: • Ясно ли са дефинирани и ролите и отговорностите, свързани с киберсигурността на всяко ниво на организацията, вкл. изпълнителния директор и управляващия борд? • Разбират ли бизнес лидерите рисковете за киберсигурност, които се приемат? • Включена ли е информационната сигурност при проектирането, интегриране и експлоатиране на технологичните решения? • Бизнесът стимулира ли въвеждането на практики за проектиране с интегрирана сигурност за продуктите, в които се инвестира? • Ефективно ли се управляват рисковете въведени от трети страни? Огромно предизвикателство за ГМИС е защитата на дигиталната инфраструктура и активите на организацията, осигурявайки непрекъснатост на оперативните дейности. Например, екипите за киберсигурност трябва да адаптират програмите за сигурност и практиките за управление на риска, за да се даде възможност за масово преминаване към инструменти за работа от вкъщи и бързото приемане към облачни услуги.
Длъжностно лице по защита на данните  **Какво прави ДЛЗД?**	Наред с ГИМ и ГМИС, всяка компания (бизнес или с нестопанска цел) трябва да има **длъжностно лице по защита на данните** (ДЛЗД). ДЛЗД е лидерска роля в сигурността, изисквана от общия регламент за защита на данните (GDPR). ДЛЗД е отговорен за надзора на стратегията на компанията за защита на данните и нейното прилагане, гарантирайки спазването на GDPR. ДЛЗД е задължително за всички компании, които събират или обработват личните данни на гражданите на ЕС, съгласно член 37 от GDPR. ДЛЗД са отговорни за обучението на компанията и нейните служители относно спазването на изискванията, обучението на персонала, участващ в обработката на данни и провеждането на редовни одити за сигурност. ДЛЗД отговарят също за контактите между компанията и всички надзорни органи, които контролират дейности, свързани с данни. Ако няма назначени лица за ГИМ, ГМИС и ДЛЗД, то разумно би било, тези отговорности да се възложат на членове от изпълнителния екип или да се организират чрез външни услуги (аутсорсинг) от други МСП и организации.

Препоръки за МСП и организации

COVID-19: Преминаване на бизнеса от физически към дигитален	Преминаването на към дигитален бизнес крие някои нови рискове. Следователно, първо трябва да се установят какви са тези рискове.  **Нови зависимости:** Работата онлайн неизбежно означава по-голямо доверие на цифровите технологии, вкл. онлайн услуги като уеб хостинг, обработка на кредитни карти и инструменти за производителност като имейл, видео и чат. Вашите съществуващи договорености с партньорите могат ли да се използват за увеличение на капацитета и надеждността? Например, осигурен ли е необходимия капацитет на комуникационните канали, за справяне с увеличения уеб трафик? Има ли достатъчно място за онлайн съхранение? Редовно ли се архивират основните данни? Има ли достъп до ИТ поддръжка?  **Проверете споразуменията за поддръжка:** За наличните услуги може да има споразумения за ниво на обслужване или други договорености. Добре е да се прочетат, за да сме сигурни с какви ресурси разполагаме.
Оценка на киберсигурността на бизнеса	Сигурността на мрежата е важна, но трябва да се разглежда в контекста на цялостните бизнес нужди. Мерките, които се предприемат за справяне с пандемията от COVID-19, ще станат по-траен начин за работа. Например, ще се позволи ли работата да продължи в домашни условия, ще се търси ли експанзия на онлайн бизнеса? Ако е така, ще са необходими системи, които да са устойчиви, скалируеми и позволяват бизнеса да се адаптира и расте. Облачните услуги са проектирани да отговорят на тази потребност, като позволяват да се разширяват или свиват ИТ изисквания в отговор на пазарните условия, без големи инвестиции в хардуер или персонал. Те имат много предимства по отношение на сигурността, но все пак като краен потребител ще сме отговорни за собствените данни – как ще се осъществява достъпът до тях и от кого.
Какви технологии използвате?	Какви ИТ активи притежаваме, управляваме и използваме? Трудно е да се осигури технология, ако не можем да определим кой е отговорен за нея – фирмата, доставчика на услуги или това е съвместно усилие?
Успешно ли поддържате ИТ?	Тъй като се разчита все повече на цифровите услуги за правене на бизнес, то трябва да се помисли как бихме се справили, ако тези услуги станат недостъпни. Анализи на услугите, които се използват, идентифицирането на нивата на поддръжка и начините за ескалация на проблема, ще помогнат да се подготвим за неочаквани ситуации.
Какви мерки за киберсигурност предприемате?	Във Великобритания съществува ръководство за МСП от National Cyber Security Centre (NCSC), което е предназначено да помогне за установяване на основен набор от политики за сигурност на ИТ. "Cyber Essentials" предоставя мерки за добра киберсигурност.
Има ли регулации, които трябва да спазвате?	Правилата са си правила, дори в Интернет. Ако бизнесът е свързан с обработката на лична информация онлайн, ще трябва да се спазва GDPR. Ако се обработват данни за плащане с карта – прилага се стандартът за защита на данните, наложен от индустрията. Необходимо е да се изясни обхвата на правната и регулаторна отговорност между потребителя и доставчиците на ИТ услуги.
Имате ли „Кибер" застраховка?	Засегнати ли са някакви елементи от промяната в обстоятелствата, като например работа от вкъщи, „онлайн" управление на бизнеса или чрез възлагане на ключови бизнес функции?
Ако говорите директно със своя доставчик, съсредоточете се върху следните проблеми със сигурността	 **Актуализации:** Важно е доставчиците на Интернет и облачни услуги да поддържат актуализиран софтуер и да използват защитни актуализации, веднага след като станат достъпни. Колко често доставчиците правят актуализации на услугите, които използвате и дали при всички договори и/или споразумения за поддръжка сигурността е на ниво.

Резервни копия: Какви резервни копия са налице и колко често се тестват? Ако доставчикът на услуги е претърпял кибер атака, как би възстановил услугата и вашите данни? Трябва да определите колко често се архивират вашите данни, къде се съхраняват и кой има достъп до тях.

Достъп: Дали вашите данни и данните на другите, за които сте отговорни, са правилно защитени? Можете ли да поставите двуфакторна автентификация, за ограничаване на достъпа до вашите данни и услуги? NCSC предлага и насоки за въвеждане на две от най-разпространените решения за криптиране, използвани за защита на данни в Интернет: TLS и IPsec.

Логове: Съхраняват ли се логове за целите на сигурността? Записите могат да окажат съществена роля при диагностицирането на всички проблеми, пред които са изправени вашите системи. Логовете също могат да са безценни при реагиране и възстановяване от инциденти, свързани със сигурността.

Реакция при инциденти: Какво ще се случи, ако нещата се объркат? Доставчиците на услуги трябва да действат по презумпцията, че ще бъдат атакувани. Трябва да е ясно как и кога те ще се ангажират точно с вас по време на инцидент със сигурността.

Сигурността като основа за бъдещ растеж

Преминаването на вашия бизнес от физически към дигитален сигурно не само ще помогне на бизнеса да расте сигурно и устойчиво, но също така ще допринесе за добра репутация сред клиентите. Важно е да се поддържа отворен диалог с доставчиците на ИТ услуги, изграждайки положителни отношения за по-добро разбиране за задълженията.

Кибер институции във Великобритания и България

National Cyber Security Centre (NCSC) – UK

Какво прави NCSC?

NCSC подкрепя най-критичните организации във Великобритания, широкия публичен сектор, промишлеността, МСП, както и обществеността. Когато се случват кибер инциденти, NCSC предоставя ефективен отговор, за да сведе до минимум вредата и да помогне за възстановяването от последствията, като трупа опит за бъдещето. По-конкретно NCSC:

- разбира киберсигурността и преобразува тези знания в практически насоки, които са общодостъпни и на разположение на всички;
- реагира на инциденти в киберсигурността, за да намали вредата, която причиняват на организациите;
- използва индустриални и академични познания, за да поддържа нивото в областта на киберсигурността;
- намалява рисковете чрез подобряване на сигурността на мрежи от публичния и частния сектор.

История на NCSC

NCSC стартира през октомври 2016 г. и има седалище в Лондон, като обединява експерти от CESG (отдел за информационна сигурност на GCHQ), Центъра за кибер оценяване, CERT-UK и Центъра за защита на националната инфраструктура. NCSC се явява единен посредник за контакт за МСП, по-големи организации, държавни агенции, широката общественост и ведомствата. Също така работи съвместно с други правоприлагащи органи, отбраната, агенциите за разузнаване и сигурност на Обединеното кралство и международните партньори.

Covid-19 и киберсигурност

През последните месеци NCSC издаде много материали, свързани с киберсигурността в контекста на Covid-19, включително:

- Съвместна консултация с американски и канадски еквивалентни агенции;
- Ръководство за организации с персонал, работещ от дома и как се разпознават фишинг имейли, свързани с COVID;
- Ръководство за организации, подпомагащо подбора, конфигурирането и прилагането на услугите за видеоконферентна връзка.

Практическа информация за МСП	Съвети и насоки: https://www.ncsc.gov.uk/section/advice-guidance/all-articles
Институт по информационни и комуникационни технологии към Българска академия на науките (ИИКТ-БАН)	**ИИКТ-БАН** е създаден на 1 юли 2010 г., като правоприемник на Институт по паралелна обработка на информацията, Институт по информационни технологии и Институт по компютърни и комуникационни системи. Изследователската и развойна дейност на ИИКТ обхваща следните направления: Изкуствен интелект и езикови технологии; Комуникационни системи и услуги; Информационни технологии в сигурността; Информационни технологии за обработка на сензорни данни; Информационни процеси и системи за вземане на решения; Интелигентни системи; Паралелни алгоритми; Моделиране и оптимизация; Научни пресмятания с Лаборатория по 3D дигитализация и микроструктурен анализ; Скалируеми алгоритми и приложения с Център по високопроизводителни пресмятания; Разпределени информационни и управляващи системи; Кибер-физични системи.

Полезна информация за ГИМ/ГМИС и предизвикателствата на COVID пандемията

Coronavirus (COVID-19) избухване: Краткосрочни и дългосрочни действия на ГИМ	ГИМ трябва да увеличат устойчивостта срещу бъдещи проблеми и да се подготвят за възстановяване и растеж. Въпреки че организациите оперират в кризисен режим, за да се справят с краткосрочните ефекти от COVID пандемията, съществуват и дългосрочни въздействия, които трябва да се вземат предвид. Когато традиционните методи и операции са повлияни от епидемията, стойността на цифровите канали и продукти става очевидна и ГИМ имат възможност да представят по-убедителна аргументация за нуждата от тях. Това е предупреждение за организациите, които се фокусират върху ежедневните оперативни нужди за сметка на инвестиране в дигитален бизнес и дългосрочна устойчивост.
COVID-19: Идеи за ГИМ и ИТ експертите	Технологичните ръководители имат съществена роля в управлението на организацията и екипа за ефективното функциониране в условията на COVID-19. Тази кризисна ситуация реално въздейства върху всяка дейност на предприятието – от оперативна и финансова до техническа и лична. За справяне с проблема, е разработен списък от непосредствени, средносрочни и дългосрочни мерки, които ИТ лидерите могат да се възползват при решаване на подобни предизвикателства в тази ситуация.
Успешната цифрова трансформация изисква трансформация на данните	Независимо дали организацията е стартирала официална инициатива за дигитална трансформация, няма съмнение, че повечето бизнес операции вече са неразделна част от ИТ инфраструктурата с която работят. Ако технологичният напредък се управлява правилно, той може да се превърне директно в бизнес напредък. Много компании се борят за преодоляване на пропастта между съществуващата ИТ инфраструктура и практики, и стойността на новите цифрови технологии. Има ясен начин за оптимизиране на усилията за дигитална трансформация и това е фокусиране върху данните. Дигиталната трансформация ще се окаже кратка, ако не се базира на солидна основа на „трансформация на данни“
Набор от инструменти за управление на ГИМ 2020 **COVID-19 променя приоритетите на ГИМ**	Длъжностите ГИМ и ГМИС са с постоянно развиващи се отговорности. Най-добрите в бранша се фокусират върху следните три области за по-ефективно управление: *Технологии – Хора - Инфраструктура*. Най-важните въпроси, върху които се препоръчва ГИМ и бизнеса да се фокусират са: управление на достъпа; работа от вкъщи; мобилни пресмятания; блокчейн; въздействие на социалните медии; сигурност и хакване; персонал; умения за нови технологии; управление на риска; поверителност на данните; възвръщаемост на инвестициите от новите технологии.

Как технологичните лидери реагират на кризата причинена от COVID-19	Пандемията ускори темповете на дигитална трансформация, така че технологиите играят ключова роля в преобразуването на бизнеса. Данните от проведено проучване показват, че инвестирането в разбирането на изискванията за дигитално клиентско преживяване и нови бизнес модели остават основните приоритети за ГИМ през 2020 и 2021 г. В същото време, инвестициите в ИТ инфраструктура са необходими, за да се гарантира киберсигурността и функционирането на цифровите инструменти на работното място. Балансирането на инвестициите във вътрешна ИТ инфраструктура и външни, насочени към клиента, дигитални възможности, оптимизирайки ИТ разходите е основното предизвикателство пред ГИМ.
Coronavirus: ГИМ трябва да обмислят нова Desktop IT стратегия	Ranjit Atwal, ръководител на научните изследвания в Gartner, отбеляза, че водещата прогнозата от Gartner рисува неблагоприятна картина за пазара. В последната си прогноза за пазара на устройства фирмата за анализи прогнозира, че продажбите на компютри ще намалеят с 10%, докато смартфоните ще намалят с 14.6%. Прогнозата на Gartner предвижда, че 48% от служителите вероятно ще останат да работят отдалечено, поне през част от времето след отминаване на COVID пандемията, в сравнение с 30% преди нея. Тази тенденция ще доведе до това преносимите компютри да изместят настолните компютри през 2021 и 2022 г.
ECSO Barometer 2020: "Киберсигурността в светлините на COVID-19"	От март до май 2020 г. Европейската организация за киберсигурност (ECSO) проведе проучвания между своите членове и общността на киберсигурността (големи компании, университети, клъстери, МСП, публични администрации, институции, агенции на ЕС, потребители, оператори, асоциации и други) с цел по-добро разбиране на въздействието на пандемията COVID-19 върху активността на участниците в киберсигурността през кризисния период, както и техните очаквани предизвикателства след кризата.
Cyber Security Response Package достъпен за доставчици на бизнес и здравеопазване	В разгара на пандемията COVID-19, ECSO представи пакет от мерки относно киберсигурността и COVID-19. Документът обобщава инициативи, инструменти и услуги за бързо реагиране от Европейската общност за киберсигурност, която включва членове и партньори на ECSO, както и други заинтересовани страни. Документът се актуализира редовно от общността, като част от кампанията за кибер солидарност. Мерките са в следните 5 области: 1) Ресурси за сектора на здравеопазването; 2) Общи ресурси за COVID-19; 3) Национални/регионални инициативи; 4) Работа от вкъщи; 5) Кибер атаки по време на COVID-19.
След COVID-19: ГИМ ръководство за възстановяване	Повечето ГИМ никога не са имали сценарий за пандемия от COVID-19. В период на несигурност е невъзможно да се предвиди бъдещето, важно е обаче да се оцени обхвата от възможности. Целта е не да се проиграят всички сценарии, а да бъдем по-гъвкави и готови за адаптиране към нови дори и непредвидени ситуации. В период на несигурност, това да не правиш нищо е също решение с разходи и с последствия. Някои от тях са директни и с непосредствени последици, други са с дългосрочни ефекти и могат да бъдат по-значителни и далеч по-трудни за прогнозиране.
COVID-19 Ръководство за действие: След голямата изолация	Този доклад предоставя рамка, организирана около 7 ключови императива, която би била полезна за изпълнителния екип на всяка организация. Тези области са: управление на отдалечена работна сила; виртуални преговори с клиенти; отдалечен достъп до всичко; увеличаване на гъвкавостта и ефективността; защита срещу нови рискове за киберсигурност; намаляване на оперативните разходи и подобряване на непрекъснатостта на веригата на доставки; подкрепа на здравните доставчици и правителствените услуги.

Как отдалечената работа променя приоритетите на ГИМ по време на COVID-19	Проучване, проведено в средата на март с повече от 200 ГИМ в САЩ, очертава най-големите приоритети и предизвикателства пред технологичните лидери и къде планират да инвестират в бъдеще. Не е изненадващо, че областта на киберсигурността е основен приоритет на ГИМ в условията на и след пандемията, като 7 от 10 организации очакват да увеличат своите финансови инвестиции в технологии за сигурност. Публичният облак, инфраструктурата, изкуствения интелект и машинното обучение също ще получат финансови стимули в много организации.

Връзки към институции и инициативи

Връзки към органи и инициативи на България, Великобритания, ЕС и НАТО	• ИИКТ-БАН • National Cyber Security Centre (UK) • Съюз за стопанска инициатива • Cyberwatching.eu • NCIA/Cyber Security Centre • DIGILIENCE 2020

Обратна връзка

За въпроси и препоръки	E-mail: acerta@bas.bg

Редакционен съвет

Академична CERT (ACERTA) организация съгласно споразумение, подписано от група академични органи (ИИКТ, ИО-МО, ЕСИ-ЦИЕ, като начало), за засилване на сътрудничеството в изследванията, свързани с киберсигурността	1. доц. д-р Велизар Шаламанов – зам. Директор на ИИКТ-БАН 2. проф. д-р Тодор Тагарев – ИИКТ-БАН 3. проф. д.н. Даниела Борисова – ГИМ, ИИКТ-БАН 4. доц. д-р Златогор Минчев – ГМИС, ИИКТ-БАН 5. полк. доц. д-р Николай Стоянов – зам. Директор на Института по отбрана към МО 6. д-р Георги Шарков – управител на фондация Европейски софтуерен институт – Централна и Източна Европа 7. Светлин Илиев – Съюз за стопанска инициатива

Публикуването на бюлетина се реализира с финансовата подкрепа на Британското посолство в София.

British Embassy Sofia

ИИКТ Институт по информационни и комуникационни технологии

Институт по отбрана - МО

ESI European Software Institute Center Eastern Europe

СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА
UNION FOR PRIVATE ECONOMIC ENTERPRISE