ISSN 2738-7089 https://doi.org/10.11610/cybsec05bg

British Embassy Sofia

КИБЕРСИГУРНОСТ
ИНФОРМАЦИОНЕН БЮЛЕТИН

IICT Institute of Information and Communication Technologies

БРИТАНСКО-БЪЛГАРСКО ПАРТНЬОРСТВО В КИБЕРСИГУРНОСТТА ЗА МСП И ОРГАНИЗАЦИИ

февруари 2021 Брой 5

Цели и обхват

Съдържание:

Идеята за постигане на машинно-базирана имитация на човешкото познание, би звучала като футуристична мечта преди само няколко декади, но ето, че днес вече обсъждаме теми като потенциалното й въздействие върху неприкосновеността на човешките права и свободи. Макар и все още далеч от това да дадем категоричен отговор на въпроса, зададен от Алън Тюринг през 1950 г. „Може ли машината да мисли", областта на изкуствения интелект (ИИ) вече е достигнала ниво на зрялост, което позволява на хора от различни сфери да използват инструментите на ИИ, като машинно самообучение (МС), обработка на естествен език (ОЕЕ), компютърно зрение и автономни и експертни системи за редица приложения, включително и такива в здравеопазването, където ИИ се разпознава като технология с огромен потенциал. Този потенциал бе впрегнат и в борбата срещу, вече почти едногодишната, пандемия от COVID-19.

Макар и често използвана като "buzzword", темата за ИИ присъства на преден план в медийното пространство от началото на пандемията с вируса SARS-CoV-2. И не без причина - в рамките на нарастващия обем от изследвания в областта на ИИ и свързаните с него модели и технологии, често се коментират сериозни опасения, свързани с поверителността и сигурността на данните.

Инструменти на машинното самообучение са широко използвани за анализ на съществуващи данни, изготвяне на прогнози за разпространението на вируса, както и за разпознаване на модели, които да съдействат за диагностицирането на нови случаи и да обяснят резултатите от лечението. Друга посока на решенията, базирани на ИИ в подкрепа на борбата срещу SARS-CoV-2 вируса, е свързана с бързото филтриране на лекарствени компоненти, които биха могли да бъдат ефективни срещу вируса, както и за анализ на потенциалните им странични ефекти и цялостния им лекарствен ефект.

На фона на тези приложения, обаче, все по-често се съобщава за противоречиви употреби на ИИ, и особено такива, свързани с разпознаването на биометрични данни на лица под карантина и упражняването на контрол върху социалната дистанция. Тъй като, за да бъдат тренирани и интегрирани в конкретни приложения, ИИ-базираните модели се нуждаят от огромен обем данни, включително и такива, съдържащи лична и чувствителна информация, това ги прави съмнително етични и ги превръща в атрактивна мишена за атаки и злонамерени действия.

Този брой на бюлетина е посветен на анализ и дискусия върху приложенията на ИИ в борбата срещу COVID-19, но през призмата на киберсигурността и с практически предложения за компании и МСП относно етичната и безопасна употреба на ИИ средства, методи и инструменти. Като контекст ще представим и преглед на някои от последните развития и интересни приложения на ИИ, като ще се опитаме да убедим читателя, че сигурният изкуствен интелект предполага нов начин на мислене и нови нагласи за това какво е сигурност, и какво означава сигурността, в контекста на дигиталната зависимост и информационното общество, в което живеем.

Редактори на броя: ***д-р Георги Шарков, Кристина Тодорова***

На фокус: ИИ в борбата срещу COVID-19, ИИ и киберсигурност и Злоупотреби с ИИ

д-р Георги Шарков
Ръководител, ЕСИ ЦИЕ

Кристина Тодорова
Изследовател,
CySecResLab, ЕСИ ЦИЕ

„Новото нормално", наложено от пандемията от COVID-19, ускори внедряването на експериментални технологии, както в областта на здравеопазването, така и в областта на виртуалната колаборация и отдалечената работа. Освен това, ИИ получи и съществен тласък в резултат на експлозивния ръст на инвестициите в тези технологии през последното десетилетие.

По-малко известен факт обаче е, че това всъщност е третият бум на ИИ, който наблюдаваме от неговото зараждане през 1956 г. Тогава, в рамките на конференция в Дартмут, малка група посетители се съгласяват със смелата теза на Джон Маккарти, че „всеки аспект на обучението или всяка друга характеристика на интелигентността, може теоретично да бъде толкова точно описана, че може да бъде машинно симулирана". Велики имена като Клод Шанън, Марвин Мински, Норберт Винер допринасят за първия бум на ИИ в ерата на формалната логика, с обещаващи прототипи, последвани от първата "зима" на изкуствения интелект през 70-те години. С втория бум на ИИ в средата на 80-те години, все повече се приближихме до машинно вземане на решения, подобно на човешкото, благодарение на модели за представяне на знания и експертни системи, с признат успех в области като експерименталната медицинска диагностика и биохимията (например MYCIN, DENDRAL). България също демонстрира капацитет в приложни области на изкуствения интелект, като биофизиката (PREFES, KREBS в Института по биофизика). Въпреки това, успехът на експертните системи е силно зависим от изграждането на по-добра "обща култура", в допълнение към формалната логика, способността за работа с големи масиви от данни и огромната изчислителна мощ. Това са и основните причини за втората „зима" на ИИ през 90-те години.

Днес, за трети път, ИИ отново е „следващото голямо нещо". И все пак, в момента, това твърдение като че ли стои върху много по-солидни основи. Напредъкът, постигнат по отношение на изчислителни методи и мощ, анализ и управление на големи масиви данни, компютърно зрение и обработка на естествен език, съчетан с огромния технологичен напредък като цяло, направи възможно изграждането на колективен изкуствен „мозък", способен да победи Гари Каспаров (1997, Deep Blue), да спечели Jeopardy (IBM Watson, 2011), да победи световни шампиони на Го, като използва техники за дълбоко обучение (AlphaGo, 2016), наред с много други постижения. Всичко това подхрани нови надежди за бъдещето на изкуствения интелект и забележително увеличи инвестициите в него. През 2018 г. Европейската комисия обяви увеличение на средствата за научноизследователска и развойна дейност в областта на ИИ до 1,5 милиарда EUR до 2020 г., догонвайки Азия и САЩ. Малко след това, в началото на 2021 г., Европейската стратегия за изкуствен интелект си поставя за цел да увеличи инвестициите в ИИ (от публичен и частен сектор) до най-малко 20 милиарда EUR годишно през следващото десетилетие. Междувременно в САЩ, инвестициите в компании в областта на изкуствения интелект, се увеличиха от 300 милиона през 2011 г. до около 16,5 милиарда щатски долара през 2019 г. и над 25 милиарда през 2020 г. Не е изненадващо, че Китай е обявен за глобален лидер в изследванията на изкуствения интелект и обявява амбициите си да се превърне в ИИ суперсила на света с инвестиции от 150 милиарда щатски долара до 2030 г. Не на последно място, през 2020 г. България прие концепция за развитие на изкуствения интелект до 2030 г., фокусирайки се върху научния напредък и разработването на интелигентно земеделие и здравеопазването[1].

Независимо от всичко, пандемията даде тласък на цифровата трансформация на бизнеса, публичната администрация, образованието и социалния живот и активира планове за дигитализация, отлагани с години. Развитието на ИИ, макар и предимно в експериментална фаза, бързо навлиза в борбата срещу COVID-19. Несъмнено третият бум на изкуствения интелект ще окаже влияние не само върху здравеопазването, но и върху изцяло новата организация на живота в този „дигитализиран, за да оцелее" свят, в който живеем и който ще бъде предмет на дискусия в рамките на следващите страници.

[1] https://www.mtitc.government.bg/bg/category/157/koncepciya-za-razvitieto-na-izkustveniya-intelekt-v-bulgariya-do-2030-g

Впрягане на възможностите на ИИ в борбата срещу COVID-19

Въпреки че ИИ приложения са били използвани експериментално и преди, за проследяване на огнища на вирусни заболявания, безпрецедентното разпространение на COVID-19 мобилизира всякакви възможни средства за ограничаване на разпространението на болестта и търсенето на лечение.

Бързото адаптиране и предоставянето на ранни резултати показаха, че ИИ може да играе съществена роля в борбата срещу COVID-19 и бъдещите епидемични ситуации. Въз основа на методите и техниките за анализ на големи данни, МС и дълбокото обучение (ДО), методите на ИИ се оказаха полезни за анализа на моделите на разпространение на заболеваемостта, нейното географско позициониране и тенденции, за прогнозирането на бъдещи огнища и смъртност, подпомагане диагностиката и мониторинга на голям брой случаи, управление на ресурси и консумативи и, разбира се, улесняване на изследванията, превенцията и ефективното лечение. Повечето от приложенията еволюираха бързо от експериментална до практическа употреба и дори пилотните експериментални приложения се оказаха от голяма помощ в борбата срещу „неизвестното".

ИИ за прогнозиране на огнища на заболеваемост

ИИ се прилага в различни системи за прогнозиране на разпространението на вируса, за изготвяне на ранни предупреждения и предоставяне на полезна информация за огнищата на болестта и уязвимите региони, както и за прогнозиране на заболеваемост чрез наблюдение и анализ на публикации в социалните мрежи. На канадската стартираща компания BlueDot се приписва ранното откриване на вируса с помощта на ИИ, благодарение на способността му непрекъснато да преглежда над 100 бази данни с информация от новини, продажби на самолетни билети, демографски данни, климатични данни и популации на животни. Те забелязаха огнището на пневмония в Ухан, Китай на 31 декември 2019 г. и идентифицираха градовете, които най-вероятно ще бъдат засегнати от заболяването[2].

Умни устройства за пред-симптоматична диагностика

Коронавирусната инфекция често протича асимптоматично в продължение на 5 дни след заразата. В тази ситуация вирусът може лесно и безсимптомно да се разпространи сред по-голям кръг от хора. Интелигентният пръстен, произведен от финландския стартъп Oura, който регистрира температура, сърдечен ритъм, нива на активност и други показатели, се използва широко за тестване на множество ИИ алгоритми за ранно диагностициране на COVID-19 и ограничаване разпространението на вируса. Твърди се, че един от моделите разпознава в рамките на 24 часа симптоми на COVID-19 и регистрира повишена температура, преди реално температурата да се повиши. Oura може непрекъснато да регистрира графици за почивка, базирани на типове дейности и степента на тяхната натовареност, температурата на тялото и околната среда, както и колебания в пулса. Данните, събрани от 65 000 субекти като част от проучването TemPredict, ще се съхраняват в San Diego Supercomputer Center и ще бъдат достъпни за асоцииране с други набори от данни за по-нататъшни анализи. Очаква се, че моделите, базирани на ИИ/МС, анализиращи развитието и корелацията на множество параметри чрез данни от преносими сензори, ще помогнат за ранното откриване и на други инфекциозни заболявания, като грип.

Подобни изследвания бяха проведени и в U.S. Army Medical Research and Development Command с цел дистанционно наблюдение на здравословното състояние на персонала и ранно предсимптомно диагностициране, базирано на ИИ. Очаква се също така, че скоро изводите от това изследване ще осигурят почти непрекъснато ниво на подкрепа и устойчивост на всеки американски войник по целия свят[3].

Дистанционна диагностика и телемедицина

Сред по-широко разпространените ИИ решения, в контекста на COVID-19, са различните приложения за телемедицина. Чрез обработка на данни (като температура, сърдечна честота, дишане и кислород в кръвта) от отдалечени сензори, такива системи помагат на медиците да се грижат за пациенти от разстояние, и да оптимизират ресурсите си. Въз основа на тези и други параметри, като глас, тегло и дори ходене до тоалетна, ИИ моделите се използват за наблюдение и прогнозиране на появата на нежелани реакции и проследяване на заболеваемостта. ИИ се използва и за надграждане на възможностите на различни мобилни приложения, които използват интелигентни устройства, диагностика, ефективно наблюдение и проследяване на контактни лица.

[2] https://www.cnbc.com/2020/03/03/bluedot-used-artificial-intelligence-to-predict-coronavirus-spread.html

[3] https://www.army.mil/article/242364/for_the_pandemic_and_beyond_wearable_technology_points_the_way

Екип учени от MIT предложи нетрадиционен модел, базиран на ИИ, за ранна диагностика на COVID-19[4]. Моделът се базира на анализ на записи на кашлица, направени и обработени чрез специално мобилно приложение. Изследването сочи, че кашлицата на хора с асимптоматична коронавирусна инфекция се различава от тази на здрави хора, като тази разлика е недоловима за човешкото ухо. Моделът е трениран върху десетки хиляди записи на кашлица и говор и в 98.5% разпознава кашлица на хора с потвърдена коронавирусна инфекция, включително и кашлица на асимптоматично заболели но потвърдени случаи в 100% от тестовете. Учените са готови и с разработването на облачно приложение за по-нататъшно тестване на модела, като само първоначалните тестове са направени върху над 200,000 аудио записа на кашлица. Методи на МС са използвани и в предишни изследвания за разпознаване на дефекти в човешки гласни струни на база произнасяне на различни фрази, както и за ранна диагностика на болестта на Алцхаймер на база анализ на емоционални състояния, разпознаваеми в речта.

ИИ за оптимизация на логистиката и наблюдение на пациенти

Методи на ИИ бяха приложени и за наблюдение на пациенти в клинична обстановка, и прогнозиране на хода на лечението им. На база данни, получени от жизнени показатели и клинични параметри, методи на ИИ са приложени за подпомагане взимането на решения, оптимизация и приоритизация на разпределението на ресурси, като вентилатори и респираторно оборудване в отделения за интензивно лечение. ИИ може да се използва и за прогнозиране на хода на болестта, смъртността и за ежедневни актуализации, обработване и анализ на данни за хода на лечението.

Учени от Израел съобщават за разработването на ИИ модел, който прогнозира продължителността на хоспитализация при заболели от COVID-19. Учените използвали ИИ/МС, за да проследят клиничното състояние на хоспитализирани пациенти с COVID-19 и да съставят прогноза за очакваната продължителност на лечението в рамките на различните етапи на протичане на заболяването, чрез персонализиран модел. Системата е тренирана и валидирана върху голям обем данни, получен от Министерство на Здравеопазването на Израел и регистъра на заболелите от COVID-19, който включва данни за възраст, пол, здравен статус и информация от приема и изписването от болница на пациентите[5].

Изследвания на лекарства и ваксини

Поради непредсказуемия и силно заразен характер на коронавируса, изследвания, анализиращи структурата на вируса, с цел създаване на ваксини и ефективни лекарства, е един от основните приоритети в световен мащаб.

Подобни изследвания са твърде предизвикателни, поради това, че вирусът принадлежи на семейство обвити едноверижни РНК структури, които все пак, подобно на двуверижни вируси като ХИВ, ебола и други, COVID-19 мутира бързо, като по този начин затруднява анализа и разработването на лекарствени средства.

Успешното прилагане на алгоритъма Linearfold, съобщено от Baidy, се оказва в пъти по бързо от традиционните алгоритми за изследване на РНК структури в прогнозирането на вторични РНК вирусни структури. Учени от Baidu са използвали този алгоритъм, за да прогнозират вторичната структура на РНК последователността на COVID-19, намалявайки общото време за анализ от 55 минути на 27 секунди, правейки алгоритъма 120 пъти по-бърз от стандартния.

Учени от MIT, демонстрираха приложения на МС за идентифицирането на лекарствени продукти срещу COVID-19[6]. Те разработиха подходящи набори от клетъчни култури, за да валидират хипотезата за съществуването на корелация между коронавирусната инфекция и стареенето на тъканите, допринасяйки към изследването на специфични модели за разработване на лекарства.

За да съдействат изследването на потенциални нови медикаменти срещу COVID-19, IBM приложиха иновативна генеративна рамка, базирана на ИИ, върху три COVID-19 цели, като по този начин успяват да генерират 3000 нови молекули. Учени от института Mila в Квебек, от друга страна, използваха граф невронни мрежи за търсенето на лекарствени комбинации, ефективни срещу COVID-19.

През 2020 г., ИИ беше основен помощник в борбата с COVID-19 и търсенето на ваксина срещу патогена. Изследователи от University of Michigan[7] използваха своята МС платформа за обратна ваксинология Vaxign, която разчита на контролирани модели за прогнозирането на възможни кандидати за ваксина срещу COVID-19. По този начин, ИИ се превърна в съюзник за ускоряването на разработването на две високоефективни иРНК ваксини (Moderna и Pfizer), което стана възможно, благодарение на

[4] https://news.mit.edu/2020/covid-19-cough-cellphone-detection-1029
[5] https://www.healthcareitnews.com/news/new-ai-model-can-predict-length-covid-19-hospitalization
[6] https://www.healthcareitnews.com/news/mit-researchers-use-ai-find-drugs-could-be-repurposed-covid-19
[7] https://www.frontiersin.org/articles/10.3389/fimmu.2020.01581/full

ИИ технологиите и колаборацията между учени и изследователи по целия свят[8]. Благодарение на AlphaFold2, ИИ системата, създадена от DeepMind, стана възможно прогнозирането на пространствената структура на предизвикателни за анализ на протеини, с голяма точност. Моделът също така е използван за моделиране на възможни мутации на вируса и, респективно, за подобряването на ваксините.

ИИ подпомогна не само откриването и подобряването на ваксините. Moderna и IBM планират съвместен проект за използването на ИИ и блокчейн за интелигентното управление на вериги за доставки и логистика, свързана с ваксините и ваксинационните планове.

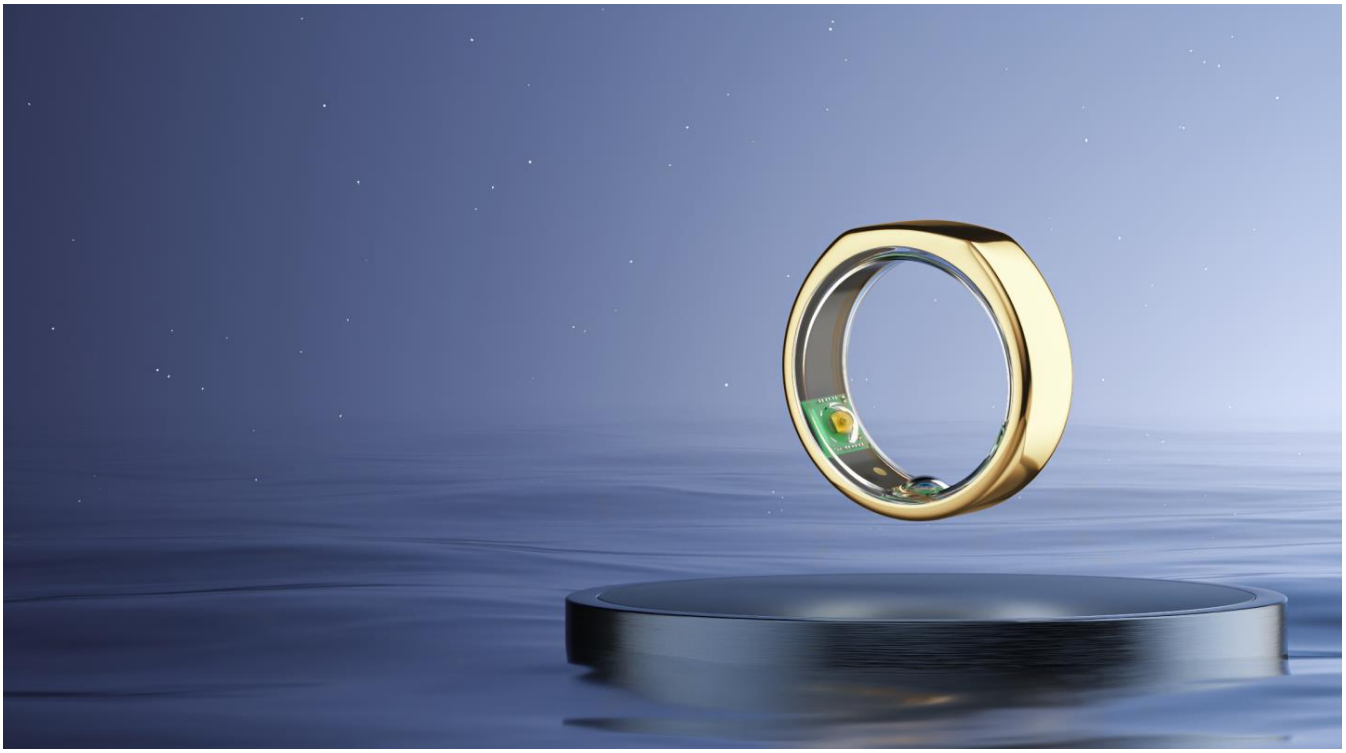
Чатботове и социални роботи

Поради лесната си адаптивност, чатботовете намериха широко приложение за разпространяването на информация, особено в условия на изолация и отдалечена работа, както и за наблюдение на симптомите, различни уведомления, психологична и обща здравна подкрепа.

Предоставянето на надеждна информация, основана на факти, е от решаващо значение в епидемична обстановка, но поради разминаване на препоръките от различни авторитети, координираната адаптация на информационни източници се оказа ключова. Освен това, чатботовете често предоставят връзки към услуги на трети страни, което би могло да доведе до нежелано разкриване на лични данни с непредвидими последици. Предвид това, че здравната информация се класифицира като чувствителна, компаниите са съветвани да действат с повишено внимание при имплементиране на технологии в тези чувствителни приложни области. Отделно, в това число влизат и така наречените социални роботи, които могат да разпознават промени в поведението на хората около тях, и които често се използват за предоставяне на основни услуги и рутинна помощ.

ИИ и анализ на данни

Пандемията необратимо промени начинът, по който ИИ се използва за анализ на данни. Предишни приложения на МС, до момента се използваха за анализ на големи масиви от данни, включително и с техники за ДС. Според Gartner[9], след COVID-19, организации, използващи традиционни методи за анализ на данни, които разчитат основно на голям обем от исторически данни, посочват традиционните модели за анализ като безполезни. Перспективните екипи, работещи с данни, все повече се отклоняват от традиционните ИИ техники, разчитайки на големи масиви от данни за анализ, като залагат основно на по-малък обем от разнообразни данни, които използват за машинно самообучение. Освен това, добрите практики сочат, че все по-съществено става прилагането на етични норми и принципи, при внедряването на ИИ.



Пръстенът Oura. Изображение от: https://ouraring.com/

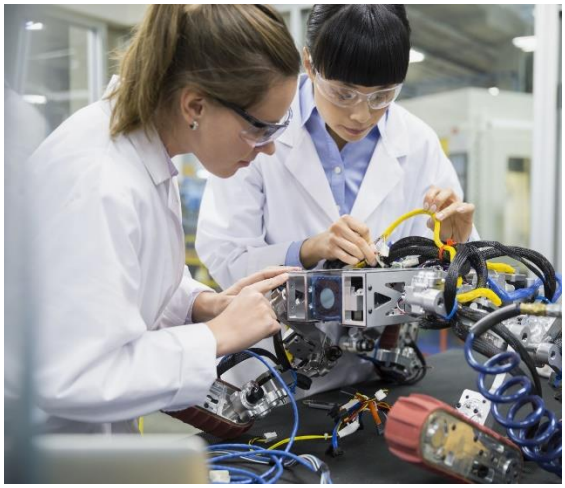
[8] https://www.swissinfo.ch/eng/artificial-intelligence-helps-bring-about-record-fast-vaccines/46256752
[9] https://www.gartner.com/smarterwithgartner/gartner-top-10-data-and-analytics-trends-for-2021/

ИИ срещу COVID-19: Основни моменти

ИИ за контрол над разпространението на COVID-19

"Изкуствения интелект (ИИ) се използва като инструмент в борбата срещу вирусната пандемия, засегнала света от началото на 2020 година. Медиите и научната общност споделят надеждата, че ИИ може да бъде използван за борбата срещу коронавируса и да укрепи слабите места в науката към момента."

Прочетете повече...



В търсене на лек: Как Baidu въведе ИИ в борбата срещу вируса

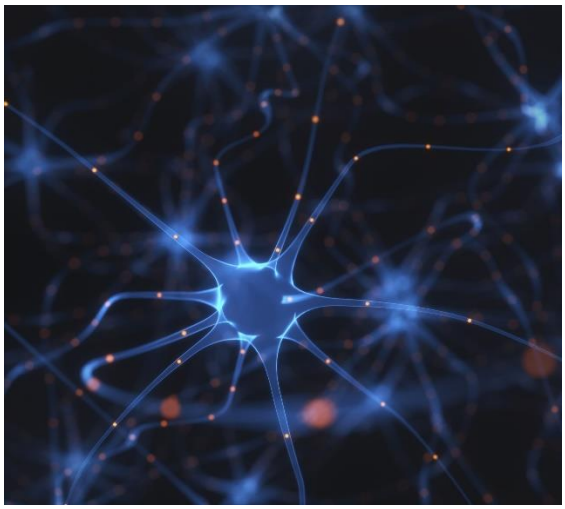
Китайската компания Baidu, в партньорство с Орегонския държавен университет и Университета в Рочестър, усилено работи по алгоритъма за прогнозиране Linearfold. Алгоритъмът изучава структурата на вторичната РНК на вируса, като по този начин има за цел да предостави на учените допълнителна информация за начина на разпространение на вируса и неговите еволюционни модели.

Прочетете повече...

ИИ за изчислителни прогнози на протеинови структури на COVID-19

DeepMind продължава да усъвършенства системата AlphaFold, като същевременно публикува своите структурни прогнози на няколко недостатъчно проучени протеина, свързани със SARS-CoV-2. Засега, експериментите потвърждават приложимостта на модела, пораждайки надежди за възможността да се направят биологично значими заключения от слепи прогнози и по този начин да се задълбочи нашето разбиране за недостатъчно изследвани биологични системи.

Прочетете повече...



IBM, Amazon, Google и Microsoft си партнират, за да предоставят изчислителни ресурси за изследване на COVID-19

AWS вече е отделили 20 милиона долара в подкрепа на изследванията на COVID-19, а Microsoft обявява редица инициативи, най-вече в подкрепа на бизнеса и справянето му с последиците от вируса.

Прочетете повече...

BlueDot: Прогнозиране еволюцията на вируса

Канадската компания BlueDot използва ИИ, за прогноза на еволюцията на вируса. Алгоритъм, който разглежда над 100 бази данни - включително и източници на новини, продажби на самолетни билети, демографски данни, климатични данни и популации на животни се използва за прогнозиране и проследяване на разпространението на болестта.

Прочетете повече...

ИИ за контрол на спазването на ограничителните мерки

ИИ намира широка употреба в подкрепа на политики за масово наблюдение, като мобилни устройства се използват за измерване на температурата и разпознаване на лица или за снабдяване на правоохранителните органи с „интелигентни" шлемове, способни да разпознават хора с висока телесна температура.

Прочетете повече...

ИИ за киберсигурност в контекста на COVID-19

Годината на COVID-19 пандемията ще остане в историята и като годината, в която киберсигурността стана водеща тема, и в която кибер инцидентите преобразиха начина ни на живот и работа. Със засилената употреба на виртуализационните технологии и технологиите за отдалечена колаборация, се увеличиха драстично и кибер инцидентите. Повече от 445 милиона кибератаки са отчетени през 2020 г., двойно повече в сравнение с 2019 г. Увеличиха се не само броят и интензивността на атаките, но и техният обхват, сложност и въздействието им, както и мотивацията и инструментите на атакуващите. От началото на пандемията ФБР отбелязва четирикратно увеличение на сигналите за кибер инциденти, а глобалните загуби в следствие на кибер престъпност, бяха оценени на над 1 трилион долара. Редица заглавия определиха 2020 г. като *„годината, в която COVID-19 предизвика киберпандемия"*.

Особено апетитни са всякакви данни и информация, свързани с изследванията на лекарства и ваксини срещу COVID-19, електронни здравни досиета на пациенти, както и друга здравна информация. Така например, през юли 2020 г., Националният център за киберсигурност на Обединеното кралство (NCSC) съобщава, че британски фармацевтични фирми и лаборатории са били обект на атаки, с цел достъп до информация за ваксини срещу COVID-19 от група, известна като APT29 (руски държавно-финансирани хакери).

Методите и инструментите на ИИ отдавна са намерили приложение в системите за откриване и предотвратяване на инциденти (IPDS), както и в по-сложните и усъвършенствани SIEM (системи за информация за сигурност и управление на събития) за наблюдение поведението на мрежи и системи, филтриране на фалшиви позитиви и бърз отговор.

Поради повишения интензитет на атаките и нарастващата сложност и повърхност за кибератаки, методите и инструментите на ИИ, обаче, се превърнаха в неизбежен инструмент за оценка на риска, ефективна киберзащита и устойчивост. Сред основните видове ИИ методи за защита и превенция на кибератаки през 2020 г. бяха:

- социално инженерство – една трета от пробивите в сигурността са в следствие на социално инженерство, като 90% от него са phishing атаки – ИИ/МС се използва за откриването на ИИ атаки, като "deep fakes" (за технологичното определяне на фалшифицирани изображения или видео). ИИ също така се използва за филтрирането на дезинформация и фалшиви ревюта (напр., статистики сочат, че 61% от ревютата в Amazon са фалшиви).
- ransomware (само за 22% от докладваните случаи, общата сума за откуп достига 1.4 билиона долара) – за откриване и бърз отговор на ransomware. Така например, германски болници станаха жертва на атака, която предизвика спирането на системи за грижа за пациенти, причинявайки смъртта на един пациент.
- DDoS атаките продължиха да бъдат водеща заплаха, с 4.83 милиона предприети DDoS атаки само през първата половина 2020 година. Тъй като атакуващите използват ИИ, за DDoS атаки, ИИ/МС модели за наблюдение на системите се оказват абсолютна необходимост при анализа на слаби места и особено, когато са замесени големи масиви от данни.
- софтуер от трети страни, корпоративна сигурност и вериги за доставки – ИИ се използва за анализ на "скрити заплахи", включително и в отдалечена работна среда.

ИИ за киберсигурност: Основни моменти

Филтриране на чувствително съдържание чрез ИИ: Facebook използва ИИ за филтриране на съдържание и по-бърза модерация

Facebook направи поредна стъпка в посока интеграция на изкуствен интелект за модериране на платформите си. Неотдавна, те обявиха поредната си цел – използване на МС за управление на процесите по модерация и ограничаването на необходимостта от ръчен преглед на съдържание.

Прочетете повече...

Check Point Presents the First Autonomous Threat Prevention System

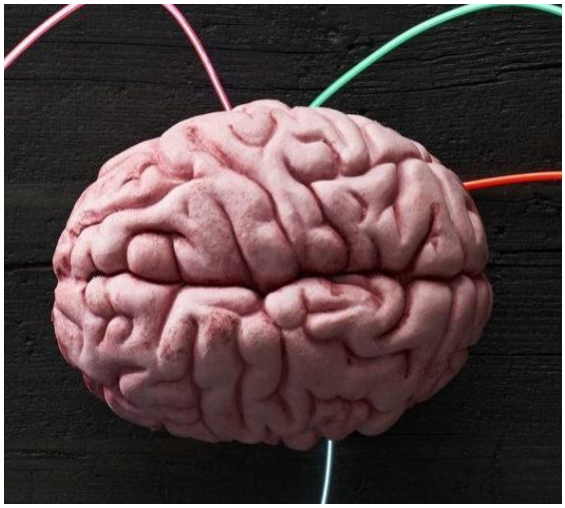
Check Point, водещ доставчик на решения в областта на киберсигурността в световен мащаб, представи своята унифицирана платформа, използваща ИИ, за киберсигурност. Платформата предоставя автономна защита срещу заплахи, разработена за компании с много отдели, разпределени между различни локации.

Прочетете повече...

Машинно самообучение: По-висока производителност, по-малко фалшиви позитиви

Изправени пред нарастващите разходи за съответствие и регулаторния натиск, финансовите институции бързо интегрират ИИ решения, включително и МС и автоматизация на процесите . за борба със сложни и еволюиращи финансови престъпления.

Прочетете повече...



Приложимост на механизмите на МС при филтриране на спам и phishing

МС моделите намират широко приложение сред доставчици на услуги за електронна поща като Yahoo, Gmail и Outlook за филтриране на нежелани съобщения.

Прочетете повече...

Изследване на приложимостта на МС за разпознаване на phishing URL

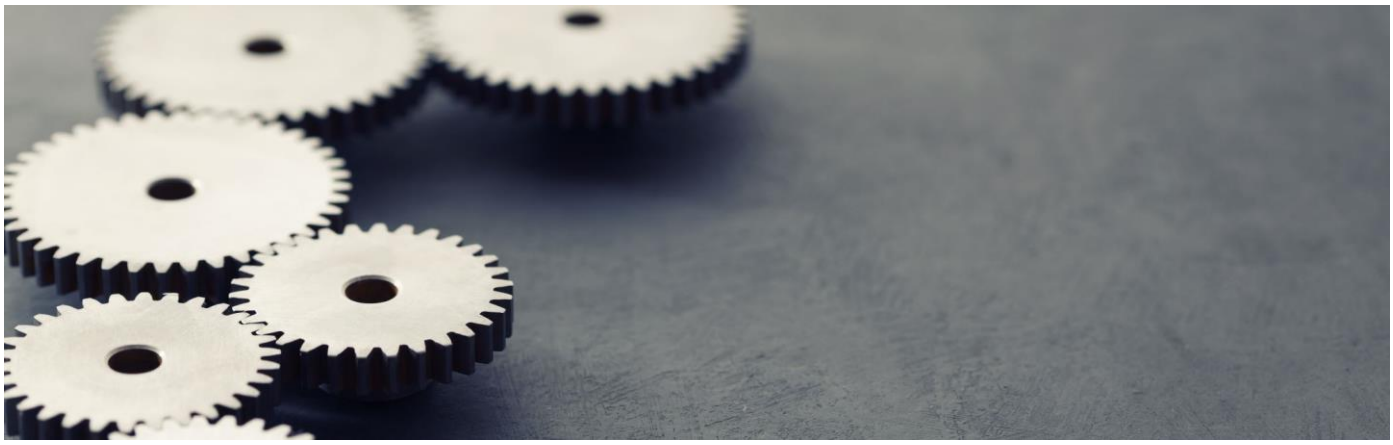
Когато целта е да се направи оценка на подозрителен URL, отсъстващ от стандартните черни списъци, МС предлага все по-надеждни решения.

Прочетете повече...

Подробен анализ за приложението на ИИ за разпознаването на злонамерени домейни

Анализирането на съществуващите корпоративни трафик логове, базирано на ИИ е ефективен начин за откриване на признаци за слабости. Логове от VPN и Active Directory могат да бъдат използвани за откриване на съмнителни дейности в потребителските профили. Логове за достъп до база данни или на ниво файл също могат да се използват за откриване на вътрешни заплахи за сигурността. Анализът на системни логове изисква различно подход на МС и методите за извличане на данни ще са контекстуално зависими.

Прочетете повече



Устойчив и сигурен ИИ: Киберсигурност за изкуствен интелект

Без съмнение, софтуерно-базираните ИИ системи, следва да отговарят на променящите се изисквания за киберсигурност. Само това, обаче, не е достатъчно, тъй като методите и инструментите на ИИ се основават на напълно различни от традиционните архитектури, технологии, алгоритми и данни. Подходът на ЕС към ИИ, както е очертан в Стратегията на ЕС за ИИ от 2018 г. и в отворена статия на ЕК от февруари 2020 г. дефинира ИИ като „етичен, сигурен и авангарден ИИ, създаден в Европа".

Изпълнителният директор на европейската агенция за киберсигурност ENISA Juhan Lepassaar казва още, че „киберсигурността е фундаментална за създаването на надеждни решения, базирани на ИИ. Общото разбиране за заплахите към ИИ, ще бъде от ключово значение за разпространението и интегрирането на ИИ приложения в Европа".

Докладът на ENISA, озаглавен "AI Cybersecurity Challenges" от декември 2020[10], дефинира обхвата на *сигурна екосистема на ИИ, както и на заплахите за ИИ*. В доклада е посочено, например, че „когато става въпрос за сигурност, в контекста на ИИ, трябва да бъде ясно, че техниките и системите, използващи ИИ, могат да доведат до неочаквани резултати, като например да бъдат подправени или самите те да манипулират информация и резултати. В частност, това е особено валидно при разработване на ИИ софтуер, който често се базира на изцяло black-box модели, или който може да бъде използван злонамерено, като например за средство за увеличаване на въздействието на кибер инцидент, или за фасилитирането на кибер атака". Това прави абсолютно наложително обезпечаването на самия ИИ. Стъпките за гарантиране на сигурността на ИИ са специално предназначени за МС, като имплементационният жизнен цикъл е очертан, както следва:

- постигане на разбиране за това какво трябва да бъде обезпечено (активи, обект на специфични заплахи за ИИ);
- постигане на разбиране за приложимите модели за управление на данните;
- управление на заплахите в многочленна екосистема по разбираем начин, като се използват общи таксономии и модели;
- разработване на специфични методи за контрол на сигурността на ИИ.

Заплахите за сигурността на ИИ, са описани както следва: "липса на устойчивост и наличие на уязвимости на ИИ моделите и алгоритмите, например, злонамерено въздействие върху системите или тяхната манипулация, атаки срещу ИИ-базирани кибер-физични системи, манипулация на данни, използвани в ИИ системи, експлоатиране на изчислителната инфраструктура, използвана за захранване на функционалностите на ИИ системата, „data poisoning", промени в средата, които биха довели до промени в естеството на данните, наличие или липса на достоверни и надеждни тренировъчни набори от данни, верификация и валидация на алгоритми (включително и интегритета на софтуерната верига за доставки), валидация на процесите на обучение и оценка на тяхната ефективност, надеждна и достоверна идентификация на функционалностите на модела, защита на данните и неприкосновеността, в контекста на ИИ системи и други".

Киберсигурността е фундаментален елемент от създаването на надежден и устойчив ИИ, но три ключови аспекта са изброени в „Насоките за етика за надежден ИИ"[11] от експертната група на високо равнище на ЕС, а именно: законност, етичност и стабилност (техническа стабилност и безопасност, сигурност и устойчивост, прозрачност, проследимост, обяснима способност и т.н.). Стандарти и схеми за сертифициране са в етап на разработване от стандартизационните органи (ETSI, CEN, ISO / ICE, други). Към момента е достъпен онлайн списъка за самооценка на стабилността на ИИ системи *"Assessment List for Trustworthy Artificial Intelligence"* (ALTAI)[12], който е специално предназначен за МСП.

[10] https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

[11] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

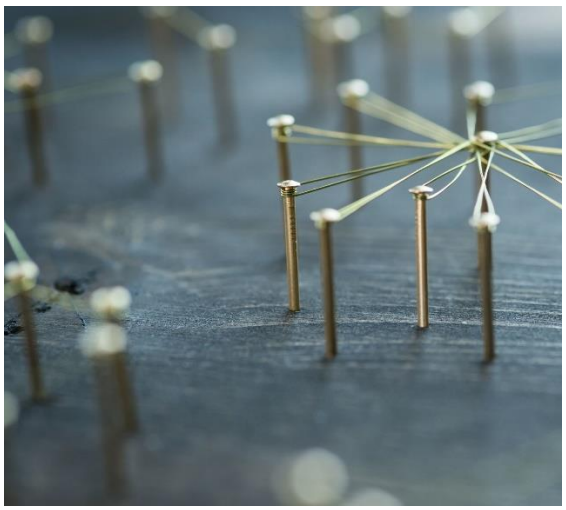
[12] https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

Киберсигурност за ИИ: Основни моменти

Microsoft обявява две ИИ-базирани технологии за борба с дезинформацията

Microsoft обявява две ИИ-базирани технологии за медиен анализ, които целят разпознаването на манипулирано съдържание и осигуряват автентичността на медийните артефакти. Едно от решенията предоставя екстеншън за браузър, който проверява сертификати и сравнява хешове, давайки информация за степента на точност и автентичност на разглежданото съдържание.

Прочетете повече....



Атакуване на ИИ: Сигурност и слабости на ИИ и какво може да се направи

Предвид това, че ИИ системите са интегрирани в приложения от критично значение, всякакви атаки срещу ИИ могат да доведат до изключително сериозни последици. Атаките срещу ИИ могат да се извършат по различен начин за постигането на различни цели. Този доклад предоставя препоръки на към съставителите на политики, относно осигуряването на ИИ.

Прочетете повече...

Скалируемо обучение с PATE

Федерирано обучение за подсигуряване на МС срещу атаки срещу неприкосновеността на данните.

Прочетете повече...

Криптографски техники за тренировъчни данни за МС

Тази статия предоставя метод за конвертиране на невронни мрежи в CryptoNets.

Прочетете повече...

ИИ базирана система за ранно предупреждение за дезинформация

Учени от University of Notre Dame работят върху проект за борба с дезинформацията онлайн, включващ медийни кампании за пораждане на омраза, насилие и намеса в демократичния изборен процес.

Прочетете повече...

Учени изразяват опасения и призовават за прозрачност и възпроизводимост на ИИ

Учени отправят призив към научните издания да придържат изчислителните изследователи към по-високи стандарти за прозрачност и призовават колегите им да споделят своя код, модели и изчислителна среда в публикации.

Прочетете повече...

Софтуер за сигурност за автомобилни превозни средства

Преди да станат участници в движението по пътищата, автономните превозни средства трябва убедително да докажат, че не представляват опасност за другите. Нов ИИ софтуер предотвратява пътни произшествия, като прогнозира различни възможни обстоятелства на всяка милисекунда.

Прочетете повече...

Създаване на надежден изкуствен интелект

Нов инструмент генерира автоматични индикатори, на базата на които анализира надеждността на данните и прогнозите, генерирани от алгоритмите, са надеждни.

Прочетете повече...

Злоупотреба с ИИ: Лошо приложение на добра технология

“Изкуственият интелект ще бъде или най-доброто, или най-лошото нещо, .случило се на човечеството” – Стивън Хокинг

В светлината на пандемията от COVID-19, осъзнаваме, повече от всякога, какво двуостро острие е изкуственият интелект. Загрижеността за неприкосновеността на личния живот, особено предвид последиците от някои приложения на ИИ, като например такива, проследяващи спазването на противоепидемичните мерки, излезе на преден план в медиите, превръщайки потенциалната употреба на ИИ като оръжие във все по-реална и по-страшна възможност.

От използването на ИИ за дистанционно изпълнение на интелигентни, саморазпространяващи се атаки, до използването на ИИ за имитиране поведението на определени системни компоненти, станахме свидетели на много злоупотреби с механизми на изкуствения интелект през 2020 г. и както никога досега, сме убедени в това, че изкуственият интелект ще бъде или най-доброто, или най-лошото нещо, което някога се е случвало на човечеството.

Интелигентно наблюдение

С последните разработки в областта на изкуствения интелект за анализ на видео и аудио, се промени самото естество на това какво представляват охранителните технологии и видеонаблюдението. Експерти се тревожат за това, че освен някои положителни приложения на ИИ, като камери, разпознаващи закононарушения или хора, представляващи непосредствена опасност за околните, някои от най-притеснителните прогнози се превръщат в реалност. Данните, получени в следствие на анализите, проведени от мощни алгоритми, които бързо и точно идентифицират хора, могат допълнително да бъдат свързани с други данни за същия човек, което осигурява един много недискретен поглед в живота на хората, техните мотивации и поведенчески модели. Освен това, все по-евтините и достъпни облачни и хардуерни ресурси, правят възможно съхранението на видео, аудио и други артефакти за всяка наша стъпка, за все по-дълги периоди от време, правейки много лесно „изравянето“ на компрометираща информация.

Лицево и гласово разпознаване

Със стотиците ботове, които автоматично събират от интернет пространството изображения, аудио и видео записи на хора, огромни количества данни се обработват и анализират непрекъснато, без нашето знание и съгласие, създавайки огромни бази данни за трениране на разнообразие от МС модели за разпознаване на лица или глас.

Това събиране на лични и чувствителни данни без съгласието на собствениците на тези данни, слага край на неприкосновеността на личния живот, ако попадне в злонамерени ръце или бъде използвано за съмнителни цели. Освен това, с напредването на deep fake технологиите, да видиш нещо, не означава, че може да му се има доверие, което прави обстановката все по-напрегната и обезпокоителна, с все по-трудното разпознаване на фалшиви новини, кадри, записи и информация.

Фалшифициране на медицински данни и изображения

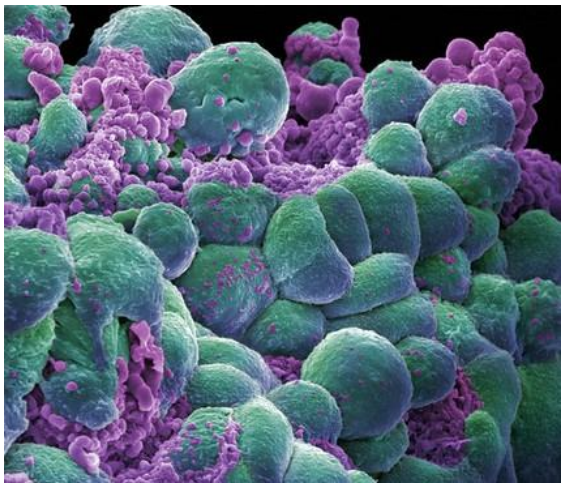
Примери за ИИ базиран зловреден софтуер бяха тествани конкретно в медицински контекст, разкривайки огромно разнообразие от възможни интелигентни атаки срещу изображения, като промяна на изображения от ядрено-магнитен резонанс, или, още по-плашещо, промяна на диагнозата на пациентите, чрез премахване на тумори от изображения от ядрено-магнитен резонанс. Възможността за безпроблемно изпълняване на интелигентни атаки, базирани на изкуствен интелект, върху цели системи от системи, чрез имитиране на компоненти от вериги за доставки, направи 2020 година още по-плашеща, както за експерти в областта на информационната сигурност, така и доставчиците на здравни услуги.

Злоупотреба с ИИ: Основни моменти

ИИ базиран зловреден софтуер фалшифицира медицински изображения

ИИ базиран алгоритъм успешно проникна в здравна организация и успя да заблуди както хората, така и системата с подправени медицински изображения. Алгоритъмът проникна в типична PACS инфраструктура и подправи изображения от ЯМР и КТ, използвайки МС, внедряващи фалшиви тумори в изображенията или премахващи истински рак от данните и изображенията на пациентите.

Прочетете повече....



ИИ предизвиква хаос в обществото, за който не сме подготвени.

Количеството deep fake съдържание онлайн нараства с бързи темпове. В началото на 2019 съществуваха приблизително 7,964 deep fake видеа онлайн, според доклад на стартъпа Deeptrace; като само 9 месеца по-късно, тази цифра скача до 14,678. Още по-притеснително, вече е сигурно, че deep fake материалите ще затруднят разграничаването на истина от фалшификат – ситуация, от която злонамерени страни непременно ще се възползват.

Прочетете повече...

Охранителна компания злоупотребява със служителите си, използвайки технология за лицево разпознаване

Стартираща охранителна компания бе обвинена в сексизъм и дискриминация, след като мениджър продажби от компанията използва система за лицево разпознаване, злоупотребявайки с жени, служители на компанията. Миналата година, мениджърът продажби е осъществил достъп до тези камери, за да направи снимки на жени, работещи в компанията, които в последствие е публикувал в Slack канал #RawVerkadawgz, заедно с явни сексуални шеги.

Прочетете повече....

ИИ превръща видеонаблюдението в автоматизиран ужас

ИИ може да маркира хора, на базата на тяхното облекло, поведение, да идентифицира емоции и да идентифицира хора, които демонстрират необичайно поведение.

Прочетете повече...

Clearview AI спира продажбите на лицево разпознаване в Канада след разследване

Clearview AI спира продажбите на своя софтуер за лицево разпознаване в Канада, според официални представители, участващи в разузнаването срещу компанията. Краят на продажби на Clearview AI в Канада означава и край на договорните взаимоотношения на компанията с правораздавателните органи в Канада.

Прочетете повече...

Защита на умни машини срещу умни атаки

В серия изследвания, екип учени изследва злонамерени тактики срещу ИИ системи и как те могат да заблудят системи за ефективност на трафика, за да предизвикат блокиране и манипулиране на здравни приложения, или да спомогнат разкриването на лична медицинска информация на пациенти.

Прочетете повече ...

Атаки срещу сигурността на МС модели за анализ на данни

Преглед на най-често срещаните рискове за сигурността и атаки.

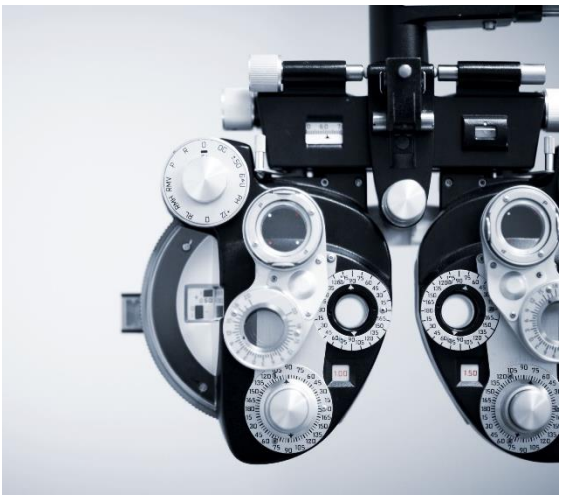
Прочетете повече...

Последно в киберсигурността

Как 30 реда код взривиха 27-тонен генератор

In October, the US Department of Justice unsealed an indictment against a group of hackers known as Sandworm. The document charged six hackers working for Russia's GRU military intelligence agency with computer crimes related to half a decade of cyberattacks across the globe, from sabotaging the 2018 Winter Olympics in Korea to unleashing the most destructive malware in history in Ukraine.

Прочетете повече.



HAFNIUM атакува Microsoft Exchange с 0-day exploits

Microsoft откри множество 0-day exploitи, използвани за атакуване на локални версии на Microsoft Exchange Server в ограничени и таргетирани атаки. В наблюдаваните атаки, злонамерените страни се възползват от тези слабости, за да получат достъп до локални Exchange сървъри, позволяващи достъп до мейл акаунти и позволяващи инсталацията на допълнителен зловреден софтуер, с цел дългосрочен достъп до средата на жертвите.

Прочетете повече...

Засегнати са над 2800 е-магазини работят с неактуални версии на Magento

Изследване на RiskIQ идентифицира скимера на Magecart „Ant and Cockroach" като общ знаменател за септемврийските атаки на Magento 1 и съобщава за скорошна активност на заплахата.Инжектирането на е-магазини се прави с цел кражба на финансови данни и е изпробван метод на Magecart, консорциум от хакерски групи, които атакуват системи за е-пазаруване

Прочетете повече...

Безпрецедентни ransomware атаки на болници

Безпрецедентна вълна от ransomware атаки, насочени срещу почти две дузини болници и здравни организации в САЩ всяват смут в ситуация на пандемия. Троянският кон Trickbot и ransomware-ът Ryuk са основните инструменти за осъществяване на атаките. Анализатори сигнализират, че атаките представляват координирани действия на руска престъпна организация.

Прочетете повече...

Севернокорейски хакери използват шпионския софтуер „Torisma" за атаки на обяви за работа

Софтуер за кибершпионаж, използван в организирана акция, насочена срещу аерокосмическия и отбранителния сектор, целящ инсталирането на агенти за събиране на данни, бе свързан със Северна Корея. Атаките включват непознат до момента инструмент, наречен „Torisma".

Прочетете повече...

Две нови 0-Days слабости в Chrome са активно експлоатирани

Google отстрани още две 0-day слабости на уеб браузъра Chrome за десктоп, превръщайки ги в, съответно, четвъртата и петата активно експлоатирани уязвимости, адресирани от компанията в последните седмици.

Прочетете повече...

Институции и инициативи на фокус: ЕСИ ЦИЕ, CyResLab, GCHQ-UK и Лаборатория по киберсигурност в София Тех Парк

Европейски Софтуерен Институт – Център Източна Европа (ЕСИ ЦИЕ)

Европейски Софтуерен Институт – Център Източна Европа (ЕСИ ЦИЕ), е основан през 2003 като публично-частно партньорство и център за върхови постижения от Европейски Софтуерен Институт, Испания (вече **Tecnalia**), **Българска Асоциация на Софтуерните Компании (BASSCOM)** и партньори от индустрията.

Информационната сигурност и устойчивост е ключова направление на научноизследователската и приложна дейност в ЕСИ ЦИЕ. През 2013 ЕСИ ЦИЕ постави начало на **CyResLab (Cyber Resilience Lab)** в стратегическо партньорство с **CERT в Carnegie Mellon University**, Питсбърг, Пенсилвания, САЩ.

ЕСИ ЦИЕ извършва одити и консултации по информационна сигурност, заедно с различни публични и частни организации, в следните области като: финанси и застраховане, транспорт (вкл. морски), петролно-газова индустрия, разработване на софтуер, ИТ услуги и образование. От 2015 г. ЕСИ ЦИЕ ръководи създаването и развитието на **Лабораторията по киберсигурност в София Тех Парк**, проект, финансиран от Европейския фонд за регионално развитие и държавен бюджет.

ЕСИ ЦИЕ има експертиза и в:

- Разработване на стратегии за киберсигурност и стратегическо планиране в ИТ компании
- Електронно управление
- Модели за киберсигурност, ситуационна осведоменост, обучение и образование в областта на информационната сигурност
- Модели и стандарти за подобряване на процесите и качеството на софтуера
- IoT и образователна роботика

CyResLab (Cyber Resilience Lab) – The Cybersecurity Division of ESI CEE

CyResLab е екипът по киберсигурност към ЕСИ ЦИЕ. Мисията на CyResLab е да повиши конкурентоспособността на дигиталните предприятия и устойчивостта на дигиталните екосистеми, предоставяйки ресурси и услуги в помощ на ИТ сектора, софтуерната разработка и информационната сигурност. От основаването си през 2013 г., екипът на CyResLab разработва серия от практически обучения, инструменти и консултации, които се предоставят на клиенти от публичния и частния сектор. Обученията и консултантските услуги са фокусирани в следните области:

- Управление на устойчивостта и зрелостта на процесите, на базата на изчерпателни и пълни референтни модели в подкрепа на организациите, включително и тези, поддържащи съответствие с различни стандарти. Обученията и консултациите включват теми като управление на риска, зрялост на процесите (CMMI DEV / CMMI SVC); управление на устойчивостта (на база CERT-RMM) и други.
- Симулации на уеб заплахи (основни и комплексни), включващи най-разпространените заплахи, но и по-комплексни атаки в теми като crypto Network and Crypto threats, SQL injection, Broken session, and Authorization management, XSS, CSRF, Secure coding и други.
- Мобилна сигурност (съответно за iOS и Android), включваща теми като Insufficient Transport Layer Protection; Unintended Data Leakage; Broken Cryptography; Poor Authorization & Authentication и други.
- Мрежова сигурност: DDOS и методи за превенция и защита, включително DDOS и DDOS методи за атака, Network/content service provider infrastructure; RTBH; Self-adaptive systems и други.

Екипът на CyResLab има експертиза и интерес в различни аспекти на информационната сигурност, като IoT, криптография, сигурни архитектури, сигурна разработка на софтуер, моделиране на заплахи и други.

Government Communications Headquarters (GCHQ) – United Kingdom

GCHQ е организация за разузнаване и сигурност, сред чиито отговорности е представянето на разузнавателна информация на правителството и въоръжените сили на Великобритания. Първоначално, GCHQ е създаден малко след Първата световна война, като Правителствено училище по кодиране и шифриране (Government Code and Cypher School) а по време на Втората световна война, отговарят за разбиването на шифровъчната машина Енигма.

Понастоящем, GCHQ има две основни звена, а именно 1) Композитни сигнали (CSO), което е отговорно за събирането на информация, и 2) Национален център за киберсигурност (NCSC), отговорен за обезпечаването на киберсигурността на Великобритания. Сред основния капацитет на GCHQ днес е и изкуственият интелект, и по-специално, неговите приложения за:

- Валидиране на факти и откриване на deep fake медийни артефакти;
- Проследяване на международни канали за трафик на хора, наркотици и оръжия;
- Анализ на чат стаи за предотвратяването на сексуално насилие и сексуален тормоз над деца;
- Изследване и анализ на мащабна дейност, за идентифицирането на злонамерен софтуер и защита на Обединеното кралство от кибератаки.

В началото на 2021 г., GCHQ първия по рода си доклад, описващ плановете и поетите отговорности, свързани с употребата на ИИ за осигуряване и защита на Обединеното кралство[13], Описвайки рамката за етика на ИИ на GCHQ и как те възнамеряват да ползват ИИ в своята дейност.

CySecResLab – Лабораторията по киберсигурност в София Тех Парк

През 2015, **Сдружението за научноизследователска и развойна дейност** на **София Тех Парк** и **ЕСИ ЦИЕ** обединяват усилия в името на общата инициатива за основаване на **Лабораторията по киберсигурност** и нейното реализиране като водещ изследователски център в областта на киберсигурността. В момента, дейността на лабораторията се състои в създаването, разработването и координирането на национален капацитет в следните области:

- Кибер устойчивост и гъвкавост на информационни системи;
- Ситуационна осведоменост за нивата и въздействието на дигиталната зависимост на обществото и икономиката, и произтичащите от нея рискове, слабости, уязвимости, както и модели за тяхната защита, както за развиването на обща готовност и подготвеност;
- Изследване на слабости, моделиране на заплахи и репликация на кибер-физични модели с потенциално хибридно въздействие;
- Разработване на стандарти и методи за проектиране, разработване и защита на кибер-зависими системи от критичната инфраструктура, както и ресурси, цифрови екосистеми и цялостно подобряване на сигурността на ИТ-интензивни системи.

Приложните изследвания на Лабораторията се фокусират върху развиването на съвременни обучения и симулации, практически занимания, упражнения и услуги в областта на кибер-устойчивостта на публичния и частния сектор.

MonSys – Български монитор за наличността на уеб-базирани услуги

MonSys е монитор, следящ достъпността на уеб-базирани услуги, разработен от **Лабораторията по киберсигурност** в периода между 2019 и 2020, с финансиране от **Сдружението за научноизследователска и развойна дейност** в **София Тех Парк** и **Немечек България**, с подкрепата на **ЕСИ ЦИЕ** и **CyResLab**.

MonSys предлага гъвкава, стабилна и скалируема платформа за мониторинг на уеб услуги, както и персонализируеми нотификации и информация и за подобряване на общата ситуационна осведоменост, гранулирана на секторно и национално ниво. Поради своята гъвкавост и скалируемост, платформата е особено ефективна в някои предизвикателни области като:

- Наблюдение на огромен брой IoT устройства в push или pull режим;
- Събиране на данни за наличността и/или сигурността на цели хоризонтални или вертикални сегменти от вериги за доставки;
- Извличане на данни в реално време от тясно специализирани услуги, изискващи специфични тестови установки, настройки, процеси или инфраструктура.

MonSys предоставя и персонализируеми тестове за наличност и достъпност за различни видове инфраструктура, като разполага с различни black-box, grey-box, и white-box тестове и метрики за наличност.

[13] https://www.gchq.gov.uk/files/GCHQAIPaper.pdf

Институции в сферата на информационната сигурност от България и ЕС

Връзки към български, британски и международни органи и инициативи в областта на киберсигурността

- **Европейски Софтуерен Институт – Център Източна Европа (ЕСИ ЦИЕ)**
- **CyResLab към ЕСИ ЦИЕ**
- **Лаборатория по киберсигурност в София Тех Парк**
- **European Union Agency for Cybersecurity (ENISA)**
- **The ECHO Project (European Network of Cybersecurity centres and competence Hub for Innovation and Operations)**
- **EU High-Level Expert Group on Artificial Intelligence**
- **The European AI Alliance**
- **ETSI Technical Committee CYBER**
- **ETSI ISG "Securing AI"**
- **ENISA Working Group "AI Cybersecurity"**
- **CERT BG**

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 киберсигурност

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 Институт по отбрана към МО
6. д-р Георги Шарков – Управител на Европейски Софтуерен Институт – Център Източна Европа
7. Светлин Илиев – Съюз за стопанска инициатива

Публикуването на бюлетина се реализира с финансовата подкрепа на Британското посолство в София. Бюлетинът отразява гледната точка единствено на авторите му.

British Embassy Sofia

IICT Institute of Information and Communication Technologies

ESI European Software Institute Center Eastern Europe

СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА UNION FOR PRIVATE ECONOMIC ENTERPRISE