C/2026/3795

16.7.2026 г.

ПРЕДУПРЕЖДЕНИЕ НА ЕВРОПЕЙСКИЯ СЪВЕТ ЗА СИСТЕМЕН РИСК

от 25 юни 2026 година

относно системните киберрискове, произтичащи от авангардни модели на изкуствен интелект

(ESRB/2026/3)

(C/2026/3795)

ГЕНЕРАЛНИЯТ СЪВЕТ НА ЕВРОПЕЙСКИЯ СЪВЕТ ЗА СИСТЕМЕН РИСК,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Споразумението за Европейското икономическо пространство ([1]), и по-специално приложение IX към него,

като взе предвид Регламент (ЕС) № 1092/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за пруденциалния надзор върху финансовата система на Европейския съюз на макроравнище и за създаване на Европейски съвет за системен риск ([2]), и по-специално член 3, параграф 2, буква в) и членове16 и 18 от него,

като взе предвид Решение ESRB/2011/1 на Европейския съвет за системен риск от 20 януари 2011 г. за приемане на процедурен правилник на Европейския съвет за системен риск ([3]), и по-специално членове 18 и 19 от него,

като има предвид, че:

(1) Водещите доставчици на изкуствен интелект (ИИ) са разработили авангардни модели на ИИ, които имат голям капацитет в областта на киберсигурността и са в състояние да извършват напълно автоматизирани кибератаки срещу сложни системи, включително чрез откриване на уязвими места и разработване и използване на експлойти като оръжие, което коренно променя съществуващите киберзаплахи.

(2) Авангардните модели на ИИ са значително по-добри от по-ранните модели на ИИ в намирането на начини за кибератаки, надминавайки по-ранните модели по разходи, бързина и точност и съперничейки си понастоящем с водещи човешки експерти.

(3) Авангардните модели на ИИ имат способността да застрашават системите, които са в основата на средите на информационните и комуникационните технологии (ИКТ), използвани от финансовата инфраструктура, като увеличават вероятността и сериозността на киберинцидентите със системно въздействие.

(4) Авангардните модели на ИИ доказаха способността си да откриват уязвими места и създават нови експлойти и така излагат на риск от кибератаки важните операционни системи и софтуер, използвани в ИКТ средите на почти всички организации.

(5) В исторически план откриването на уязвими места е рядкост; те най-често се откриват от учени в областта на сигурността, което дава възможност за целенасоченото им отстраняване. В тези случаи на доставчиците на софтуер често се дава стандартен срок — обикновено 90 дни — за отстраняване на уязвимото място преди публичното му оповестяване. Има вероятност обаче авангардните модели на ИИ да увеличат обема на откритите уязвими места.

(6) Настоящите практики за софтуерни корекции във финансовата система са предимно реактивни, като се използват периодични актуализации и ad hoc отговори на оповестените уязвими места. Този подход е успешно приложим в среда на заплахи, в която има достатъчно време за откриването и отстраняването на уязвимото място. С увеличаването на обема на уязвимите места обаче настоящите практики може да се окажат недостатъчни за поддържане на оперативната устойчивост.

(7) Това увеличение на обема също така излага настоящите процеси за софтуерни корекции на претоварване, тъй като корективните мерки в тях са подредени по значимост въз основа на риска, а софтуерните корекции трябва да бъдат тествани преди прилагането им, за да се гарантира оперативна стабилност. Ако в кратък срок бъдат открити толкова много уязвими места с критично въздействие, че броят на необходимите критични софтуерни корекции се увеличи значително, на финансовите институции може да се наложи да решават дали да се изложат на значителни киберрискове или да намалят изискванията за тестване на софтуерни корекции и по този начин да рискуват настъпването на оперативни инциденти и прекъсвания на дейността.

([1]) ОВ L 1, 3.1.1994 г., стр. 3, ELI: http://data.europa.eu/eli/agree_internation/1994/1/oj.
([2]) ОВ L 331, 15.12.2010 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2010/1092/oj.
([3]) ОВ C 58, 24.2.2011 г., стр. 4.

(8) По-рано експлойтите, използвани като оръжие, се изработваха предимно ръчно, което отнемаше на човешките експерти дни и седмици, докато сега авантгардните модели на ИИ могат да ги изработят за няколко минути или часа. Това представлява срив на защитните времеви буфери, които са необходими за поддържане на непрекъснатостта на критичните и важните функции по време на отстраняването на уязвимите места.

(9) С разпространението на експлойтите с ИИ, използвани като оръжие срещу критичните уязвими места, и съответното намаляване на защитните времеви буфери, рискът за отделните критични или важни функции и институции рязко се увеличава. Ако тези рискове се реализират едновременно във всички тези функции и институции, това би могло да доведе до постоянно увеличаване на системния киберриск, за чието намаляване понастоящем не съществува напълно ефективна рамка. Поради силната взаимосвързаност както вътре във финансовия сектор на Съюза, както и между финансовия сектор и други сектори и юрисдикции, тази ситуация представлява систематичен риск и има потенциала да доведе до системни слабости.

(10) Освен това в момента авантгардните модели на ИИ се разработват само от малък брой доставчици на ИИ, някои от които изразиха опасения, че предстоящите модели може да са твърде мощни за неограничен публичен достъп.

(11) ИИ вече се използва от злонамерени лица за засилване на кибератаките. Вероятно е те в крайна сметка да получат, било чрез изтичане на информация, кражба, независимо разработване или свободен достъп, модели на ИИ с възможности, сравними с тези, които понастоящем се внедряват в контролирани защитни условия.

(12) Въпреки че авантгардните модели на ИИ могат значително да увеличат нападателните способности и вероятността от усъвършенствани кибератаки, те също ще укрепят защитните способности, по-специално по отношение на откриването на уязвими места, корелацията на данните и коригиращите действия от страна на отделните институции. В краткосрочен и средносрочен план обаче увеличаването на скоростта, мащаба и точността на нападателните способности вероятно ще надхвърли ползите.

(13) Бързото развитие на авантгардните модели на ИИ налага незабавно справяне с установените рискове за финансовата стабилност, за да се предотврати тяхното реализиране или поне да се смекчи потенциалното им въздействие. За да се гарантира финансова стабилност на финансовите пазари на Съюза, всички членове на Европейския съвет за системен риск (ЕССР) следва да вземат предвид последиците от тези модели за оперативния капацитет и устойчивостта на финансовите институции в контекста на действията им в областта на макропруденциалната и микропруденциалната политика. Това не засяга правомощията в областта на паричната политика на централните банки в Съюза. Сред предприетите от различни органи инициативи, например, ЕЦБ в ролята си на надзорен орган на банките поиска от значимите институции да оценят незабавно въздействието на постоянно променящите се заплахи и до 31 октомври 2026 г. да разработят цялостен план за действие, в който са изложени конкретните мерки срещу тези рискове ([4]).

(14) Предвид разпространението на технологиите с ИИ е важно да се гарантира, че цялата критична инфраструктура и особено финансовите институции са подготвени да се справят с кибератаки, осъществени с авантгардните модели на ИИ, и да предприемат навременни и подходящи подготвителни действия. Такива защитни усилия от страна на отделни лица обаче ще са недостатъчни. За ефективна реакция и намаляване на риска е необходим координиран отговор с участието на всички засегнати лица, включително доставчиците на ИИ, доставчиците на софтуер, охранителните дружества, лицата, поддържащи софтуер с отворен код, финансови институции, националните органи и органите на Съюза.

(15) При разглеждането на горепосочените въпроси е важно да се припомнят приложимите правни и политически рамки на Съюза, по-специално Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета ([5]), Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета ([6]), Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета ([7]) и Препоръка на Европейския съвет за системен риск (ЕССР/2021/17) ([8]).

([4]) Писмото до значимите институции е публикувано на уебсайта на банковия надзор на ЕЦБ www.bankingsupervision.europa.eu.

([5]) Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (ОВ L 333, 27.12.2022 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект) (ОВ L, 2024/1689, 12.7.2024 г., ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета от 23 октомври 2024 г. относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (Акт за киберустойчивост) (ОВ L, 2024/2847, 20.11.2024 г., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Препоръка на Европейския съвет за системен риск от 2 декември 2021 г. относно общоевропейска рамка за координация на системните киберинциденти за съответните органи (ЕССР/2021/17) (ОВ C 134, 25.3.2022 г., стр. 1).

(16) Регламент (ЕС) 2022/2554 съдържа цялостната уредба за установяване, управление, наблюдение и ограничаване на рисковете в областта на ИКТ, включително рисковете, произтичащи от кибератаки. Предвид взаимосвързаността на финансовия сектор и зависимостта му от системи на ИКТ и трети страни — доставчици на услуги, една успешна кибератака, засягаща една или повече финансови институции или техните критични доставчици на услуги, би могла да има значителни системни последици. Органите за финансов надзор следва да дадат подходящ приоритет на надзорните дейности в тази област, като вземат предвид потенциалното въздействие на такива кибератаки върху стабилността, целостта и надеждността на финансовата система, както и оперативните, финансовите и потребителските вреди, които могат да произтекат от тях.

(17) С Регламент (ЕС) 2024/1689 се създават хармонизирани правила за пускането на пазара, пускането в действие и използването на системи с ИИ и модели на ИИ с общо предназначение в Съюза, включително при определени обстоятелства на системи и модели, предоставяни от доставчици на ИИ, установени в трети държави, когато резултатът, получен от системата с ИИ, се използва в Съюза или даден модел на ИИ е интегриран в система, пусната на пазара на Съюза. Регламентът предвижда и специални правила, включително по-строг регулаторен режим, за моделите, класифицирани като модели на ИИ с общо предназначение, пораждащи системен риск.

(18) С Регламент (ЕС) 2024/2847 се въвеждат задължителни изисквания за киберсигурност за производителите, които обхващат планирането, проектирането, разработването и поддръжката на хардуерни и софтуерни продукти с цифрови елементи, пуснати на пазара на Съюза. С регламента също се налага задължение на производителите да отстраняват уязвимите места по време на жизнения цикъл на продуктите си. След като регламентът започне да се прилага в своята цялост през декември 2027 г., финансовите субекти, които пускат такива продукти на пазара на Съюза, също ще трябва да гарантират, че продуктите отговарят на тези изисквания.

(19) В Препоръка ЕССР/2021/17 на европейските надзорни органи (ЕНО) се препоръчва, съвместно чрез Съвместния комитет и заедно с Европейската централна банка (ЕЦБ), ЕССР и съответните национални органи, да разработят ефективен координиран отговор на равнището на Съюза в случай на съществен трансграничен киберинцидент или свързана с него заплаха, които биха могли да имат системно въздействие върху финансовия сектор на Съюза. Това доведе до създаването на общоевропейската рамка за координация на системните киберинциденти (ЕС-РКСКИ), която създаде ценна и оперативна платформа за обмен на информация и координация между финансовите органи.

(20) По тези съображения ЕССР приема предупреждение от общ характер, чийто предмет са значимите рискове за финансовата стабилност, засилени от развитието на авангардните модели на ИИ. Предупреждението взема предвид аналитичната работа в бележката на ЕССР относно граничните модели на ИИ с киберспособности от гледна точка на финансовата стабилност (Addressing Frontier AI Models with cyber capabilities from a financial stability perspective), публикувана през юни 2026 г. ([9]),

ПРИЕ НАСТОЯЩОТО ПРЕДУПРЕЖДЕНИЕ:

РАЗДЕЛ 1

Предупреждение

Нова рискова среда

Бързото развитие на авантгардните модели на ИИ с киберспособности води до съществени промени в рисковата среда за финансовата система на Съюза. Актуалните данни показват, че тези модели са в състояние да откриват уязвими места, да генерират работещи експлойти и самостоятелно да извършват пълномащабни кибератаки със скорост, мащаб и степен на точност, които значително надхвърлят способностите на по-ранните модели на ИИ. Това е промяна на парадигмата в областта на киберсигурността и повратен момент за капацитета на ИИ.

ЕССР счита, че тези промени са източник на системни рискове за финансовата система, който може да породи значителни неблагоприятни последици за киберсигурността поради ускореното откриване на уязвими места, намаляване на наличното време за реакция и ефективна защита, увеличаване на мащаба и сложността на кибератаките и възникване на нови зависимости и рискове от концентрация във финансовата система. ЕССР отчита подобрените защитни способности, които авантгардните модели на ИИ ще предложат на финансовите институции, но тези способности вероятно ще се реализират постепенно през следващите няколко години, поради което финансовите институции ще трябва да извършват дейност през преходен период, характеризиращ се с повишен риск, висока несигурност и бързо развиваща се технологична среда. Като се има предвид силно цифровизираният и взаимосвързан характер на финансовата система, тези неблагоприятни последици за киберсигурността биха могли да се разпространят бързо, засягайки критични и важни функции във финансовите институции, което в крайна сметка ще доведе до системни смущения и загуба на доверие във финансовата система.

([9]) Достъпна на уебсайта на ЕССР www.esrb.europa.eu.

Новопоявилите се авантгардни модели на ИИ увеличават присъщия риск в областта на ИКТ, което води до отслабена оперативна устойчивост във финансовия сектор, особено в четири области: а) време, включително способността сложните системи да се поправят бързо, без да се причинява срив в дейността им, като се взема предвид сривът на защитните времеви буфери между откриването на уязвимото място и използването на експлойта като оръжие; б) способността на защитниците, включително способността им да провеждат автоматизирани и ръчни тестове за сигурност с помощта на авантгардните модели на ИИ, както и способността им да закрилят, разкриват и отвръщат на заплахи, произхождащи от авантгардни модели на ИИ, използвани с враждебна цел; в) концентрация, включително зависимост от ограничен брой доставчици на ИИ, които пък зависят от доставчици на компютърни услуги в облак, компоненти с отворен код и друг широко използван софтуер; и г) способността на органите, включително калибрирането на очакванията им, стрес тестовете и мерките за готовност в съответствие с развитието на авантгардните модели на ИИ, така че сривовете в дейността на системите да не се превръщат в източник на по-широка нестабилност.

Освен това създаването и поддържането на видимост при внедряването на ИИ във всяка финансова институция — включително пълно разбиране къде и как се внедрява ИИ — е предизвикателство, като се има предвид използването на ИИ в клиентските интерфейси, във вътрешните работни инструменти на персонала и в работните процеси, както и интегрирането на ИИ, предоставен от трети лица.

Системна оценка

Установените тенденции могат да променят съществено мащаба и структурата на киберриска, като увеличат както преките, така и непреките рискове за финансовата стабилност. Способностите на авантгардните модели на ИИ могат да поставят съществуващите рамки за устойчивост под значителен натиск, особено ако инцидентите са широко разпространени и възникват едновременно. Инцидентите могат да се разпространят бързо сред финансовите институции и пазари, ако бъдат засегнати критични трети страни — доставчици на услуги, споделени технологични екосистеми или широко използвани компоненти с отворен код, което увеличава риска от смущения със системни последици.

Авантгардните модели на ИИ изменят три източника на асиметрия във финансовия сектор: между юрисдикциите, между защитниците и нападателите и между финансовите институции с повече ресурси и оборудване и финансовите институции с по-малко ресурси и оборудване.

Първо, настоящата географска концентрация на водещи доставчици на ИИ извън Съюза излага Съюза на стратегическа зависимост и геополитически риск. За да се намали научната и технологична асиметрия между юрисдикциите, е необходимо да се приемат мерки за улесняване на адекватния и пропорционален достъп на Съюза и държавите членки до новоразработени авантгардни модели на ИИ. Тези мерки трябва да бъдат навременни, съгласувани и ефикасни, както от гледна точка на възприетата политика, така и от гледна точка на прилагането им, и да отчитат по подходящ начин различните финансови сектори на Съюза, като се възползват от експертния опит на съответните ЕНО. Това ще намали не само асиметрията между Съюза и третите държави, но и между финансовите институции, установени в различни държави членки, като се запазят еднаквите условия на конкуренция в Съюза и извън него и се сведе до минимум системният риск. Договореностите, улесняващи достъпа до авантгардни модели на ИИ само за определени категории институции или само в определени юрисдикции, ще допринесат за разпокъсаността на единния пазар на финансови услуги, намалявайки неговата ликвидност и дълбочина.

Второ, що се отнася до асиметрията между нападателите и защитниците, авантгардни модели на ИИ улесняват работата на нападателите. Те ще ги използват все повече за технически по-сложните и трудоемки части от офанзивните операции, което ще намали разходите им. Защитниците, от друга страна, са обвързани от оперативни изисквания, зависимости и регулаторни задължения, ограничаващи ефекта и степента, в която могат да се възползват от авантгардните модели на ИИ в краткосрочен и средносрочен план, и в крайна сметка ще са им необходими по-дълги периоди за адаптация.

Трето, съществуват разлики в ресурсите и оборудването, с което финансовите институции разполагат, за да се справят с предизвикателствата, породени от авантгардните модели на ИИ. Тези разлики могат да бъдат породени от разходи, които са с фиксиран размер за всички финансови институции, а не пропорционални на големината им, от ресурсни ограничения и от ограничен достъп до специалисти. Ако има асиметрия в способността за справяне с тези предизвикателства, най-слабото звено от веригата може да засегне стабилността на системата.

Последици

От съществено значение е да се гарантира, че системно важните платежни системи, системите за сетълмент и инфраструктурите на финансовите пазари ще продължат да бъдат защитени от уязвими места, произтичащи от използването и развитието на авантградните модели на ИИ. Публичните и частните оператори трябва да направят задълбочен преглед на рамките за киберсигурност и да ги актуализират, за да вземат предвид тези уязвими места. Органите, отговарящи за надзора, трябва да приемат мерки, за да гарантират, че системите са защитени по подходящ начин. Трябва да се търси сътрудничество между органите и частните финансови институции винаги когато това е необходимо за повишаване на сигурността и устойчивостта на финансовата система на Съюза.

В своя доклад от 2020 г. относно системния киберриск ([10]) ЕССР определи скоростта, мащаба и злонамереността на киберзаплахите като възможни източници на разпространение на системен риск. Органите трябва да са наясно, че авантгардните модели на ИИ представляват нов източник на разпространение на системен риск, засилващ въздействието на вече съществуващите източници, и трябва да включат тази информация в управленските си действия. Като се имат предвид всички рискове за финансовата стабилност, произтичащи от оперативната експозиция на киберриск във финансовия сектор, е важно да се гарантира, че опасенията, изложени в настоящото предупреждение, са отразени в надзорната дейност и в управленските позиции, приети от съответните органи в рамките на правомощията им.

Съответните органи, в рамките на правомощията им и по-специално съгласно уредбата, създадена с Регламент (ЕС) 2022/2554, трябва да са запознати с гореизложените три източника на асиметрия, появили се в резултат от навлизането на авантгардните модели на ИИ във финансовия сектор. За да се намалят тези асиметрии, наред със съществуващите рамки за тестване следва да се обмислят договорености за сътрудничество и секторна координация ([11]). Финансовите органи следва да гарантират също, че управителните органи на частните финансови институции са поели изцяло задачата да смекчават киберрисковете, породени от авантгардните модели на ИИ, че са въведени ясни рамки за управление и отчетност и че по подходящ начин се планират своевременни отговори заедно със съответните вътрешни инвестиции.

Няколкото възможни промени, разгледани в настоящото предупреждение — независимо дали това е системното въздействие, геополитическият риск или промененият баланс между нападателите и защитниците — могат да окажат въздействие върху функционирането на финансовата система и доверието в нея. За да ги оценява непрекъснато, ЕССР ще разгледа необходимостта от отразяването им в оценките на риска, рамките за тестване и надзорните очаквания, както и при разработването на бъдещи сценарии. ЕССР също така ще наблюдава използването и развитието на авантгардните модели на ИИ и тяхното въздействие върху финансовия сектор от гледна точка на системния риск. Освен това ЕССР ще прави нова оценка на промените във всяка тримесечна оценка на риска на равнището на Генералния съвет и ще обмисли други действия, когато е необходимо.

РАЗДЕЛ 2

Определения

За целите на настоящото предупреждение се прилагат следните определения:

1) „доставчик на ИИ“ означава доставчик съгласно определението в член 3, точка 3 от Регламент (ЕС) 2024/1689;

2) „авангардни модели на ИИ“ означава усъвършенствани модели на ИИ с общо предназначение, които могат съществено да засегнат нападателните или отбранителните кибероперации;

3) „кибератака“ означава кибератака съгласно определението в член 1 от Регламент (ЕС) 2019/796 на Съвета ([12]), включително когато произхожда от Съюза;

4) „уязвимо място“ означава уязвимо място съгласно определението в член 3, точка 16 от Регламент (ЕС) 2022/2554;

5) „експлойт“ означава инструмент, техника или метод, използвани за откриване на едно или повече уязвими места с цел получаване на неразрешен достъп до системи, тяхното изменение или нарушаване или с цел по друг начин да възникнат риск или инциденти в областта на ИКТ;

6) „използване като оръжие“ означава подготовката или адаптирането на експлойти, които дават възможност за системно или мащабно възползване от уязвими места;

7) „критична или важна функция“ означава критична или важна функция съгласно определението в член 3, точка 22 от Регламент (ЕС) 2022/2554;

8) „модел на ИИ с общо предназначение“ означава модел на ИИ съгласно определението в член 3, точка 63 от Регламент (ЕС) 2024/1689;

9) „модел на ИИ с общо предназначение, пораждащ системен риск“ означава модел на ИИ с общо предназначение, класифициран като пораждащ системен риск, съгласно член 51, параграф 1 от Регламент (ЕС) 2024/1689;

10) „инцидент с ИКТ“ означава инцидент съгласно определението в член 3, точка 8 от Регламент (ЕС) 2022/2554;

([10]) Вж. научния труд „Системният киберриск“, ЕССР, февруари 2020 г., достъпен на уебсайта на ЕССР www.esrb.europa.eu.

([11]) Например червени екипи за етично хакерство въз основа на оперативни сведения за заплахи (TIBER), тестване за проникване (TLPT), усъвършенствани екипи за хакерство (ART) и стрес тестване на киберустойчивостта (CyRST).

([12]) Регламент (ЕС) 2019/796 на Съвета от 17 май 2019 г. относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки (ОВ L 129 I, 17.5.2019 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11) „риск в областта на ИКТ“ означава риск съгласно определението в член 3, точка 5 от Регламент (ЕС) 2022/2554;

12) „оперативна устойчивост“ означава оперативна устойчивост на цифровите технологии съгласно определението в член 3, точка 1 от Регламент (ЕС) 2022/2554.

Съставено във Франкфурт на Майн на 25 юни 2026 година.

Ръководител на секретариата на ЕССР,

от името на Генералния съвет на ЕССР,

Francesco MAZZAFERRO