УДК: 340.134:[007:004.056(4-672EU)
Biblid 1451-3188, 24 (2025)
Год XXIV, бр. 89, стр. 203–220
Изворни научни рад
Рад примљен 29. 01. 2025. године
Рад одобрен 12. 02. 2025. године
DOI: https://doi.org/10.18485/iipe_ez.2025.24.89.10

ПРАВНИ ОКВИР ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ ЕУ

*Марко НОВАКОВИЋ, Михајло ВУЧИЋ**

Апстракт: У савременом дигиталном добу, безбедност информационих система и мрежа представља основу за функционисање економских, друштвених и институционалних структура. Европска унија (ЕУ) препознала је значај ове области и развила свеобухватан правни оквир који обухвата низ директива и уредби с циљем јачања информационе безбедности и отпорности. Овај оквир укључује кључне акте попут NIS2 Директиве, која унапређује безбедносне стандарде и подстиче сарадњу између држава чланица, DORA Уредбе, која се бави управљањем дигиталним ризицима у финансијском сектору, CER Директиве за заштиту критичних инфраструктура, као и CSA и CRA Уредбе које дефинишу безбедносне стандарде за дигиталне производе и услуге. У раду се анализира постојећи правни оквир ЕУ, разматра се његова улога у јачању дигиталне отпорности и испитују се изазови у његовој примени. Посебна пажња посвећује се значају ових регулаторних мера за Републику Србију, која би као кандидат за чланство у ЕУ требало да усагласи своје прописе са европским стандардима. Имплементација поменутих директива и уредби представља не само регулаторни изазов, већ и прилику за унапређење националних капацитета у области информационе безбедности.

Кључне речи: EU, информациона безбедност, NIS2, DORA, CER, CSA, CRA.

---

* Институт за међународну политику и привреду, Београд. E-mails: marko@diplomacy.bg.ac.rs; mihajlo@diplomacy.bg.ac.rs. ORCID iD: https://orcid.org/0000-0002-7753-7506; ORCID iD: https://orcid.org/0000-0002-0064-4987.

Рад је настао у оквиру научноистраживачког пројекта: „Србија и изазови у међународним односима 2025", којег финансира Министарство науке, технолошког развоја и иновација Републике Србије, а реализује Институт за међународну политику и привреду током 2025 (евиденциони број: 200041).

1) УВОД

Убрзани развој дигиталних технологија и све већа зависност од информационих система и мрежа довели су до тога да информациона безбедност постане један од кључних приоритета, како за појединце тако и за институције и привредне субјекте.[1] У том контексту, ЕУ је током последњих деценија развила свеобухватан правни оквир који има за циљ јачање отпорности на информационе претње, унапређење безбедности критичних инфраструктура и заштиту дигиталних производа и услуга. Овај оквир обухвата низ директива и уредби попут NIS2 Директиве, која унапређује безбедносне стандарде и подстиче сарадњу између држава чланица, DORA Уредбе, која се бави управљањем дигиталним ризицима у финансијском сектору, CER Директиве за заштиту критичних инфраструктура, као и CSA и CRA Уредбе које дефинишу безбедносне стандарде за дигиталне производе и услуге и које постављају обавезне стандарде за државе чланице и индустрију, с циљем да се осигура висок ниво информационе безбедности у ЕУ.

2) NIS2 – ДИРЕКТИВА О МЕРАМА ЗА ОБЕЗБЕЂИВАЊЕ ВИСОКОГ НИВОА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ ЕУ

ЕУ Директива о мерама за високи заједнички ниво безбедности мрежних и информационих система широм ЕУ (*Directive on measures for a high common level of cybersecurity across the Union*, NIS2), представља важан корак у развоју европског законодавства у области информационе безбедности.[2] Усвојена је с циљем јачања безбедности критичних инфраструктура и услуга од суштинског значаја за економију и друштво. Директива стандардизује приступ информационој безбедности у државама чланицама и подиже ниво информационе отпорности унутар ЕУ. Прва NIS Директива из 2016. године донета је као одговор на растућу зависност од дигиталних технологија и мрежних система, али брз развој технологије и све већи број претњи по информациону безбедност створили су потребу за ревидирањем нормативног оквира. У децембру 2020. године Европска комисија предложила је ревидирани текст Директиве, познат као NIS2. Њени кључни циљеви су унапређење безбедности мрежних и информационих система,

[1] Stephen Quinn, Nahla Ivy, Matthew Barrett, Greg Witte, and R. K. Gardner, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*, NIST, US Department of Commerce, 2022. Интернет: https://doi.org/10.6028/NIST.IR.8286B.

[2] "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive) (Text with EEA relevance)Text with EEA relevance", *OJ* L 333, 27. 12. 2022, pp. 80–152.

јачање сарадње између држава чланица и проширење обухвата на нове секторе и услуге. NIS2 проширује обухват на секторе као што су дигиталне услуге, здравствена индустрија и енергетика, класификујући субјекте у „кључне" и „важне", према критичности њихових услуга и величини организације.[3] Сви обухваћени субјекти обавезни су да обавесте надлежни орган о значајним инцидентима који би могли утицати на континуитет услуга или угрожавање података. Извештавање треба да буде брзо и ефикасно како би се омогућила благовремена реакција. Директива такође подстиче појачану сарадњу међу државама чланицама и развој механизама за размену информација и реаговање на информационе претње. Уводи захтеве за стварање и јачање националних регулаторних тела која ће пратити усклађеност и пружати подршку организацијама у спровођењу нових стандарда. Имплементација NIS2 Директиве у националне законодавне оквире може бити изазовна због сложености усклађивања између различитих сектора. Организације морају прилагодити своје безбедносне политике и процедуре, што укључује обезбеђивање адекватних људских ресурса и техничке инфраструктуре. Ово представља посебан терет за мала и средња предузећа, која често немају довољно капацитета. Упркос изазовима, NIS2 доприноси укупној отпорности и безбедности дигиталног простора у ЕУ, постављајући темеље за јачу и боље координисану информациону безбедност.

Однос NIS2 и DORA

Однос NIS2 са другим секторским прописима ЕУ, као што је Уредба о дигиталној оперативној отпорности за финансијски сектор (DORA), истиче њену специфичну улогу у интегрисаном правном оквиру информационе безбедности. Док NIS2 поставља опште стандарде и обавезе за управљање информационо-безбедносним ризицима, извештавањем и оперативном отпорношћу, DORA регулише специфичности финансијског сектора. DORA налаже финансијским институцијама да развију стратегије за управљање ИКТ ризицима, укључујући тестирање дигиталне отпорности и управљање ризицима трећих страна. Конкретно, DORA обавезује финансијске институције да поднесу три типа извештаја о инцидентима: почетни, посредни и коначни извештај, док NIS2 предвиђа општи оквир за пријављивање значајних инцидената са мањим степеном детаља. Такође, DORA се фокусира на развој тестирања попут *Threat-Led Penetration Testing* (TLPT), док NIS2 овај аспект не покрива у толиком обиму. Иако DORA регулише специфичности у финансијском сектору, NIS2 успоставља механизме за сарадњу између финансијског сектора и других актера у ширем

[3] *Ibid.*

оквиру информационе безбедности. Ово укључује радне групе за сарадњу, размену информација са CSIRT-овима и јединственим контактним тачкама. На овај начин, DORA осигурава дубинску специјализацију за финансијске субјекте, док NIS2 поставља шири оквир за информациону безбедност у различитим секторима. Интеграција оба прописа омогућава бољу координацију, ефикасније управљање ризицима и већу оперативну отпорност унутар јединственог дигиталног тржишта ЕУ.

3) DORA – УРЕДБА О ДИГИТАЛНОЈ ОПЕРАТИВНОЈ ОТПОРНОСТИ

Уредба о дигиталној оперативној отпорности за финансијски сектор (у даљем тексту и DORA), као одговор на овај изазов.[4] DORA је ступила на снагу 16. јануара 2023. године, са одложеном применом од 17. јануара 2025. године, с циљем да се унапреди отпорност финансијских услуга, као и других критичних инфраструктура које зависе од информационих технологија и мрежних система.[5] Основни циљеви DORA, као што јој само име каже, јесте побољшање оперативне отпорности у дигиталном окружењу, посебно у секторима који пружају финансијске услуге. Поред наведеног, фокус је на обезбеђивању јединственог регулаторног оквира који ће хармонизовати постојеће регулативе, а све у циљу унапређења заштите критичне инфраструктуре од потенцијалних ризика и напада, чиме се обезбеђује непрекидан рад економије и финансијског система.[6] DORA почива на пет стубова а то су: управљање ризицима, извештавање о инцидентима, тестирање дигиталне оперативне отпорности, управљање ризицима трећих страна и размена информација.

Управљање ризицима

DORA прописује бројне обавезе релевантне за остваривања циљева као што је, на пример, прописивање обавезе за све институције које пружају финансијске и друге критичне услуге да развију и примењују ефективне стратегије за управљање ризицима који произилазе из дигиталних инцидената, укључујући информационе нападе, природне катастрофе и технолошке неисправности. Ова управљачка стратегија треба да обухвати

[4] "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)", *OJ* L 333, 27.12.2022, pp. 1–79.

[5] "Digital Operational Resilience Act (DORA)", European Insurance and Occupational Pensions Authority. Интернет: https://www.eiopa.europa.eu/digital-operational-resilience-act-DORA_en

[6] *Ibid.*

све аспекте пословања, укључујући људске ресурсе, инфраструктуру и мреже и треба да омогући брзу детекцију и одговор на ризике. Управљање ИКТ ризицима уједно представља и један од пет стубова DORA.

Извештавање о инцидентима

DORA успоставља јединствен систем извештавања о информационим инцидентима, што омогућава бољу координацију и бржу реакцију на претње. Према DORA, све финансијске институције и треће стране које пружају услуге у финансијском сектору морају бити у стању да идентификују, пријаве и реагују на инциденте у ИКТ системима у складу са стандардизованим протоколима. Ово су све карактеристике и основе информационе безбедности као такве, те нису карактеристичне само за DORA већ и за све друге директиве и системе који за циљ имају побољшање информационе безбедности, па тако обавезе извештавања постоје и у оквиру NIS2 и CER. Како регулишу исту област, правила и захтеви ових Директива се некада поклапају па се поставља питање како институције треба да поступају у тим ситуацијама, односно правилима, и којим институцијама треба дати приоритет, а то би у овом случају била DORA.[7]

Када је DORA у питању, она захтева да финансијске институције поднесу три извештаја о инцидентима надлежном органу. Први је почетни извештај који садржи основне информације о инциденту како би орган могао да утврди његов значај и процени да ли постоји прекогранични утицај. Други је посредни извештај који укључује ажурирања о инциденту, као што су промене у статусу или нови доступни подаци, а подноси се када дође до значајне промене статуса, када су доступне нове информације, или када надлежни орган затражи додатне податке. Трећи је коначни извештај који укључује анализу коренског узрока инцидента.[8]

Тестирање дигиталне оперативне отпорности

Захтев за редовно тестирање оперативне отпорности у складу је са профилом ризика институције. Увођење редовних симулација и тестирања како би се установила оперативна спремност институција за суочавање са претњама по ИКТ системе. Јединствени систем извештавања не само што олакшава брзу и координисану реакцију, већ и пружа значајне могућности за побољшање капацитета анализа ризика и рањивости у финансијском сектору.

[7] D. Clausmeier, "Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)", *International Cybersecurity Law Review,* 4(1), 2023, pp. 79–90. Интернет: https://doi.org/10.1365/s43439-022-00076-5.

[8] Sara Elizabeth Boddy, *Case study: The decision-support framework and NIS2, CER, and DORA incident reporting obligations,* Jyväskylän Yliopisto Informaatioteknologian Tiedekunta, Master thesis, 2024.

Управљање ризицима трећих страна

Управљање ризицима трећих страна укључује постављање строгих услова за односе са ИКТ добављачима, укључујући праћење и процену ризика.

Размена информација и обавештајних података

Осим што подстиче институције на сарадњу у размени информација о претњама, што доприноси укупној отпорности система, или управо због тога размена информација представља један од основа информационе безбедности и у студијама старијим од десет година.[9]

Утицај на финансијске институције

Увођењем DORA финансијске институције у ЕУ суочавају се са потребом за значајним улагањима у инфраструктуру, процесе и обуку особља. Иако DORA Уредба не уводи револуционарне концепте, већ се фокусира на детаљнију и свеобухватнију имплементацију постојећих правила, њен ефекат је дубок. Хармонизација регулатива смањује административно оптерећење и омогућава бољу координацију међу државама чланицама, али истовремено повећава захтеве за усклађеност, посебно за мање финансијске институције. Мале и средње финансијске институције често немају довољно ресурса за имплементацију свих аспеката DORA, што може довести до потребе за коришћењем спољних консултаната и ИКТ добављача. За њих је посебан изазов управљање ризицима трећих страна и осигурање да њихови добављачи испуњавају услове које намеће Директива. Примена заједничког регулаторног оквира омогућава:

- Смањење ризика од напада на ИКТ системе кроз бољу координацију и стандардизацију безбедносних мера;
- Повећање транспарентности у односу са трећим странама, што смањује могућност злоупотреба и рањивости у ланцу снабдевања;
- Убрзавање реакције на инциденте захваљујући обавезном извештавању и размену информација.

Међутим, потребно је време да се у потпуности остваре ови бенефити, посебно у погледу развоја свести о значају дигиталне отпорности и изградње инфраструктуре која може одговорити на нове захтеве.

[9] Ulrik Franke, Joel Brynielsson, *Cybersituational awareness – A systematic review of the literature*, Swedish Defence Research Agency, SE-164 90 Stockholm, Sweden, 2014.

Изазови и могућности примене DORA у мањим финансијским институцијама

DORA ће имати изузетно широк утицај на компаније, који се неће ограничити само на ИТ сектор. На пример, DORA Уредба предвиђа детаљну ревизију постојеће документације и процеса, што ће ангажовати и правне и административне секторе. Такође, биће неопходно обезбедити да уговори са IT добављачима буду усклађени са новим захтевима, што подразумева успостављање нових процедура и способност праћења нових уговорних обавеза и намеће додатне обавезе правним службама компанија.[10] Ова ревизија укључује ажурирање клаузула које регулишу безбедност података, одговорност добављача и механизме управљања инцидентима. У контексту DORA, финансијске институције и друге обухваћене организације биће у обавези да унапређују своје капацитете за праћење ризика у ИТ сектору и обезбеде усклађеност са строгим стандардима оперативне отпорности, укључујући управљање ризицима и гаранције континуитета пословања. Осим правних тимова, у овај процес биће укључени и тимови за управљање ризиком, ИТ одељења и спољни партнери, како би се осигурало да сви аспекти пословања испуњавају нове регулаторне захтеве. DORA доноси значајне предности, али и изазове за финансијске институције, посебно за мање организације са ограниченим ресурсима и недовољном стручном подршком у области информационе безбедности. Ове институције су често приморане да се ослоне на спољне консултанте и добављаче ИКТ услуга, што може повећати оперативне трошкове и изазове у управљању ризицима. Недостатак интерних стручњака и механизама за праћење трећих страна додатно отежава усклађивање са захтевима Директиве. DORA препознаје ове специфичности, па предвиђа поједностављен оквир за управљање ИКТ ризицима, како за микро тако и за мала и средња предузећа.[11] Имплементација обавезних тестова, попут *Threat-Led Penetration Testing* (TLPT), захтева високу техничку експертизу и приступ напредним алатима, што је посебно изазовно за мање институције па DORA ову обавезу предвиђа пре свега за веће финансијске институције којима је наметнута обавеза да TLPT спроводе сваке три године.[12] Ипак, ова тестирања пружају драгоцене увиде за отклањање рањивости и побољшање безбедносних процедура, чиме се дугорочно јача дигитална отпорност. Увођењем виших безбедносних стандарда, институције могу побољшати поверење клијената и своју

[10] Antonio Giannino, Francesca Valenti, Federico Sertori, "Is DORA the dawn of a new era for cybersecurity compliance in the EU's financial sectop?", *Journal of Financial Compliance*, Volume 8 / Number 1 / Autumn/Fall 2024, pp. 32–42(11).

[11] DORA, члан 14а.

[12] D. Clausmeier, *op. cit.*

конкурентност, док сарадња кроз размену информација доприноси лакшем усвајању најбољих пракси. Ове активности треба посматрати као део континуираног циклуса унапређења, а не као једнократне задатке. С друге стране, DORA поставља и значајне изазове за земље чланице ЕУ, које морају да прилагоде националне регулативе и обезбеде неопходне ресурсе за обуку особља и развој техничке инфраструктуре. У Србији, као земљи кандидату за чланство у ЕУ, имплементација DORA Директиве захтеваће унапређење капацитета за управљање ризицима и развој одговарајућих регулаторних механизама. Ово ће допринети безбедности и стабилности финансијског сектора, као и јачању дигиталне инфраструктуре у ширем смислу. Иако процес усклађивања са DORA захтевима подразумева значајне изазове, он представља прилику за трансформацију и јачање отпорности финансијских институција, што може донети дугорочне користи за националну економију и безбедност.

4) CER – ДИРЕКТИВА О ОТПОРНОСТИ КРИТИЧНИХ ЕНТИТЕТА

Директива о отпорности критичних ентитета ЕУ (у даљем тексту и CER), представља важан нормативни акт који има за циљ јачање безбедности и стабилности критичних инфраструктура и услуга у ЕУ.[13] Она је ступила на снагу 13. јануара 2023. године, уз обавезу држава да транспонују ову директиву у национално законодавство до 17. октобра 2024. године.[14] Поред тога, државе чланице су обавезне да до 17. јануара 2026. године усвоје Стратегију за унапређење отпорности критичких ентитета.[15] Пре свега, CER дефинише отпорност као способност критичног субјекта да спречи, заштити се од, одговори на, одупре се, ублажи, апсорбује, прилагоди и опорави се од инцидента.[16]

Директива обухвата 11 сектора: енергетику, транспорт, банкарство, инфраструктуру финансијских тржишта, здравство, пијаћу воду, отпадне воде, дигиталну инфраструктуру, јавну управу, свемир, и производњу, прераду и дистрибуцију хране.[17] Основни циљеви CER Директиве су

[13] "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)", *OJ* L 333, 27. 12. 2022, pp. 164–198.

[14] Члан 26. Директиве 2022/2557.

[15] Члан 4. Директиве 2022/2557.

[16] "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)", *op. cit.*

[17] Видети детаљније анекс Директиве 2022/2557 (Annex Sectors, Subsectors and Categories of Entities).

повећање отпорности критичних инфраструктура и услуга у ЕУ, како би се обезбедило континуирано пружање основних услуга грађанима и привреди у случају инцидената или катастрофа. Земље чланице су обавезне да идентификују и класификују критичне ентитете попут енергетских компанија, здравствених установа, транспортних система и технолошких инфраструктура, неопходних за функционисање кључних услуга. Директива прописује минималне безбедносне стандарде који обухватају физичку, информациону и технолошку безбедност, као и припрему и одговор на ванредне ситуације. Европска комисија усвојила је листу основних услуга које се односе на секторе обухваћене директивом, а на основу процене ризика идентификују се критични субјекти у свакој држави чланици. Ови субјекти су дужни да спроводе сопствене процене ризика, као и да предузимају техничке, безбедносне и организационе мере за унапређење отпорности и пријаву инцидената. Критични ентитети морају развијати стратегије за управљање ризицима и обезбедити планове за опоравак и континуитет пословања у случају прекида услуга, са посебним нагласком на прилагођавање планова специфичним врстама ризика. CER Директива такође наглашава значај међународне сарадње и координације међу земљама чланицама, с обзиром на прекограничну природу многих критичних инфраструктура и претњи попут напада на ИКТ системе. Брза размена информација и усаглашавање стандарда између држава кључни су за ефикасну заштиту. Национални органи за надзор имају обавезу да контролишу примену Директиве, спроводе инспекције и предузимају мере против организација које не испуњавају прописане стандарде. Овим приступом CER Директива настоји да осигура безбедност, стабилност и оперативну отпорност критичних инфраструктура у ЕУ. Иако CER Директива поставља јасне стандарде, њена имплементација представља велики изазов за земље чланице, али и за сам сектор критичних инфраструктура. Пре свега, CER омогућава значајну интерпретативну флексибилност државама чланицама приликом дефинисања кључних ентитета и мера безбедности. Ова флексибилност може довести до хетерогених ефеката, уводећи недоследности које ометају функционисање јединственог тржишта, а тиме и униформност отпорности широм ЕУ.[18] Идентификовање и класификација критичних ентитета може бити изазов, посебно у земљама које немају јасно дефинисане листе таквих ентитета. Такође, неке инфраструктуре могу бити тешко класификоване као критичне, али су важне за одржавање свакодневног живота грађана. Наравно, вечно питање ресурса погађа и ову реформу, јер је за имплементацију мера отпорности потребно значајно

[18] M. J. Alexopoulos, A. Niemi, B. Skobiej, F. Sill Torres, "Examination of the Critical Infrastructure Resilience Directive From the Maritime Point of View". *JCMS: Journal of Common Market Studies*, 2024. Интернет: https://doi.org/10.1111/jcms.13681.

улагање у људске ресурсе, као и у развој инфраструктуре која ће бити отпорна на различите врсте напада и катастрофа. Такође, потребно је развијати стручност у управљању ризицима и кризним ситуацијама.

5) CSA – УРЕДБА О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

Уредба о Агенцији ЕУ за информациону безбедност и за информатичку сертификацију у области информационе и комуникационе технологије (у даљем тексту Уредба о информационој безбедности и CSA), нормативни је акт ЕУ који је ступио на снагу још 2019. године, као део шире стратегије ЕУ у области информационе безбедности.[19] CSA пре свега регулише успостављање и мандат ENISA-е, Агенције ЕУ за информациону безбедност и дефинише циљеве и задатке ENISA-е који укључују развој политика, јачање капацитета, оперативну сарадњу, унапређење тржишта и стандардизацију, ширење знања и информација, подизање свести, едукацију, истраживање, иновације и међународну сарадњу. Ова регулатива такође описује организациону структуру ENISA-е, која обухвата Управни одбор, Извршни одбор, Извршног директора, Саветодавну групу, Групу заинтересованих страна за безбедносну сертификацију и Мрежу националних официра за везу.[20] Оперативни аспекти ENISA-е укључују програмирање активности, транспарентност, поверљивост, приступ документима и управљање финансијама. Део регулативе односи се на оквир за безбедносну сертификацију, који обухвата успостављање шема сертификације, нивое осигурања, оцену усаглашености и националне органе за сертификацију информационе безбедности. Поред тога, регулишу се правне и административне одредбе као што су правни статус, одговорност, језичке одредбе, заштита података, сарадња са трећим државама и правила о безбедности. С циљем да испрати динамику развоја инормационог окружења у што већој мери, 2. децембра 2024. године Савет ЕУ је усвојио Акт о информационој солидарности, који је допуњен циљаним изменама Акта о информационој безбедности из 2019. године.[21] Нови Акт уводи систем за узбуњивање који успоставља паневропску инфраструктуру састављену од националних и прекограничних информационих центара, задужених за

[19] "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity CERtification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)", *OJ* L 151, 7. 6. 2019, pp. 15–69.

[20] *Ibid.*

[21] "Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)", *OJ* L, 2025/38, 15. 1. 2025.

размену информација, детекцију и реаговање на претње.[22] Такође, кроз амандмане уведен је механизам за ванредне ситуације у области информационе безбедности који подразумева спровођење припремних активности, као што је тестирање субјеката у критичним секторима попут здравства, транспорта и енергетике. Ове измене су осмишљене да побољшају постојећи нормативни оквир и обезбеде већу солидарност и ефикасније реаговање на претње унутар ЕУ.[23]

6) CRA – УРЕДБА О ИНФОРМАЦИОНОЈ ОТПОРНОСТИ

Уредба о хоризонталним захтевима у погледу информационе безбедности за производе са дигиталним елементима (У даљем тексту: Уредба о информационој отпорности или CRA), део је шире стратегије ЕУ да се подигне ниво информационе безбедности и отпорности и последњи нормативни акт ЕУ који ће бити анализиран у овом раду.[24] CRA је ступила на снагу 10. децембра 2024. године, али ће многи важни елементи ове Уредбе почети да се примењују тек од 11. децембра 2027, и поставља правни оквир који поставља захтеве у области информационе безбедности за хардверске и софтверске производе са дигиталним елементима који се пласирају на тржиште ЕУ. Овим актом се од произвођача захтева да озбиљно приступе безбедности током читавог животног циклуса производа. Интернет ствари (*internat of things* – IOT) представља еко-систем уређаја који су повезани, углавном преко интернета, и који тиме поседују такозвану „дигиталну интелигенцију". IOT уређаји обухватају свакодневне предмете попут телевизора, аутомобила и генерално уређаје за које се традиционално не сматра да би могли преко интернета да комуницирају без људског посредовања (зато се рецимо компјутери и паметни телефони не сматрају делом IOT). Са све већим бројем повезаних IOT уређаја, а очекује се да порасте са 14,6 милијарди у 2022. на 30,2 милијарде до 2030. године, потреба за обезбеђивањем њихове информационе безбедности прерасла је из информационе у физичку сферу безбедности.[25] Када је у питању IOT, због умреженог окружења, инцидент у једном производу може утицати на целу организацију или читав ланац снабдевања, често се ширећи преко

[22] *Ibid.*

[23] *Ibid.*

[24] "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)" , *OJ* L, 2024/2847, 20. 11. 2024.

[25] Ericsson, 'Ericsson Mobility Report' (June 2022) p. 13. Интернет: https://www.ericsson.com/49d3a0/assets/local/reports-papers/mobility-report/documents/2022/ericsson-mobility-report-june-2022.pdf, 12 March 2024.

граница унутрашњег тржишта за само неколико минута. Циљ CRA је успостављање и спровођење правила за унапређење информационе безбедности „производа са дигиталним елементима", укључујући IOT уређаје. CRA намеће обавезе произвођачима, добављачима и дистрибутерима како би се обезбедили основни захтеви за информациону безбедност пре него што уређаји буду доступни на тржишту. Иако CRA представља снажан оквир за побољшање информационе безбедности IOT уређаја, одређене нејасноће могу утицати на његов ефекат. На пример, терминологија попут „ограничити површину за нападе" или „без познатих рањивости које се могу искористити" захтева додатно разјашњење. Такође, CRA не пружа довољно детаљних смерница произвођачима за спровођење процене ризика у области информационе безбедности.[26] CRA се бави са два главна проблема: ниским нивоом информационе безбедности производа са дигиталним елементима, који се огледа у широко распрострањеним рањивостима и недовољном или недоследном обезбеђивању безбедносних ажурирања за њихово решавање. Недовољним разумевањем и недостатком информација код корисника, што их спречава да изаберу производе са адекватним безбедносним карактеристикама или да их користе на сигуран начин. Сви производи са дигиталним елементима, који су интегрисани у веће електронске информационе системе или повезани с њима, под одређеним условима могу послужити као вектор напада за злонамерне актере. Ови производи морају бити отпорни на нападе који могу угрозити њихову функционалност и безбедност података. У члану 2, CRA експлицитно наводи да се неће примењивати на неке производе попут моторних возила или медицинских средстава, *exempli gratia*.[27] CRA прописује произвођачима и добављачима да унапред припреме планове и процедуре за управљање информационим инцидентима и кризним ситуацијама. Ово укључује развој мера за откривање напада, брзо реаговање и минимизацију последица, као и обавезу да се пружи одговарајућа подршка корисницима у случају инцидента. Важност едукације, као једног од кључних елемената информационе безбедности, истакнута је и у CRA. Тако се у члану 10. предвиђају као обавезне: (а) развијање вештина у области информационе безбедности и стварање организационих и технолошких алата који ће обезбедити довољан број квалификованих стручњака за подршку раду органа за надзор тржишта и тела за оцењивање усаглашености; (б) јачање сарадње између приватног сектора, економских оператера, укључујући преквалификацију или додатну обуку запослених код произвођача, потрошача, пружалаца обука, као и јавне управе, чиме се

[26] Mohammed Raiz Shaffique, "Cyber Resilience Act 2022: A silver bullet for cybersecurity of IOT devices or a shot in the dark?", *Computer Law & Security Review*, Volume 54, September 2024, 106009.

[27] Уредба 2024/2847, Члан 2.

проширују могућности за младе да дођу до послова у сектору информационе безбедности.[28] Обавезе произвођача и добављача и дистрибутера су детаљно разрађене у одредбама CRA, која поставља јасне обавезе за произвођаче и добављаче дигиталних производа и услуга. Произвођачи производа са дигиталним елементима морају осигурати да су производи дизајнирани, развијени и произведени у складу са сушинским захтевима за информациону безбедност. Они су дужни да спроведу процену ризика која укључује могуће претње, начин коришћења производа и околности рада. Произвођачи морају документовати резултате и ажурирати процену током трајања подршке производу. Такође, неопходно је да припреме техничку документацију и изврше поступак оцењивања усаглашености, те обележе производ са CE знаком као доказ усклађености са прописима. Осим тога, произвођачи су дужни да пруже информације о подршци и безбедносним ажурирањима током најмање десет година или дуже, у зависности од трајања подршке производу.[29] Добављачи су дужни да на тржиште стављају само производе који су усклађени са захтевима ове регулативе. Пре стављања производа на тржиште, они морају да провере да ли је произвођач извршио одговарајућу оцену усаглашености, припремио техничку документацију и обезбедио SE знак. Уколико увозници утврде да производ није у складу са прописима или представља значајан ризик, дужни су да обавесте произвођача и надлежне органе, те да спрече даље стављање таквог производа на тржиште. Поред тога, увозници морају чувати документацију, укључујући ЕУ декларацију о усаглашености, најмање 10 година од датума стављања производа на тржиште.[30] И коначно, дистрибутери су дужни да, пре стављања производа на тржиште, провере да ли производ има CE знак и да ли су произвођач и добављач испунили своје обавезе. Уколико дистрибутер сумња да производ није у складу са прописима или представља значајан ризик, мора обавестити произвођача и надлежне органе. Они такође имају обавезу да, на захтев надлежних органа, доставе све потребне информације и документацију која доказује усаглашеност производа са прописима. У случају да произвођач прекине своје пословање, дистрибутери су дужни да обавесте кориснике и надлежне органе о овом питању.[31]

7) ЗАКЉУЧНА РАЗМАТРАЊА

Уредбе и директиве анализиране (укратко) у овом раду, и не само оне, имају специфичну сврху и обим, али заједно чине комплементарни оквир који промовише информациону отпорност у различитим секторима и производима

[28] Уредба 2024/2847, Члан 10.

[29] Уредба 2024/2847, Члан 13.

[30] Уредба 2024/2847, Члан 19.

[31] Уредба 2024/2847, Члан 20.

у Европи. Нормативни оквир ЕУ у области информационе безбедности представља свеобухватан систем закона, директива, и регулатива усмерених на заштиту дигиталног простора, критичне инфраструктуре, и осетљивих података од све већих претњи информационе безбедности. Овај оквир је изграђен на принципима транспарентности, солидарности и заједничке одговорности држава чланица у унапређењу отпорности на информационе ризике. Један од централних докумената у овој области је Директива о мрежној и информационој безбедности (NIS Директива), усвојена 2016. године. Она је први правно обавезујући акт који се директно односи на информациону безбедност у ЕУ. NIS Директива има за циљ успостављање високог заједничког нивоа безбедности у мрежним и информационим системима кроз читаву Унију. Она обавезује државе чланице да идентификују операторе основних услуга и пружаоце дигиталних услуга, као што су финансијске институције, здравствене установе, енергетска предузећа и провајдери клауд услуга, те да обезбеде да ови субјекти примењују мере за управљање ризицима и пријављују инциденте који утичу на континуитет њиховог рада. У новембру 2022. године усвојена је ревидирана верзија ове Директиве, позната као NIS2 Директива, како би се додатно ојачали механизми информационе безбедности у светлу нових технолошких изазова. NIS2 проширује обухват сектора и ентитета на које се односи и уводи строже обавезе у погледу управљања ризицима и пријављивања инцидената. Такође, унапређује сарадњу међу државама чланицама кроз успостављање Европске мреже тимова за брзо реаговање на инциденте (CSIRT мреже) и креирање оперативних центара за информациону безбедност. Поред NIS Директива, важну улогу има и CSA која поред оснивања Европске агенције за информациону безбедност (ENISA) и уводи Европски оквир за сертификацију информационе безбедности, који обезбеђује стандарде и сертификације за дигиталне производе, услуге и процесе. Као део нормативног оквира, анализиране су DORA – уредба о дигиталној отпорности, CER – Уредба о отпорности критичких ентитета, CRA – Уредба о информационој отпорности. Додатно, Општа уредба о заштити података (GDPR) има значајну улогу у заштити личних података и обезбеђивању безбедности информационих система. Уредба захтева од организација да примењују техничке и организационе мере како би спречиле неовлашћен приступ, губитак или компромитацију података али за разлику од нормативних аката анализираних у овом раду, иако ГДПР прописује да се лични подаци морају обрадити безбедно, користећи адекватне техничке и организационе механизме, она не прописује које су конкретне мере у питању.[32] Са растом

[32] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", *OJ* L 119, 4. 5. 2016, pp. 1–88.

претњи као што су информациони криминал, хакерски напади и информациона шпијунажа, ЕУ је такође усвојила Стратегију информационе безбедности 2020–2025. године. Ова стратегија тежи унапређењу заштите критичних инфраструктура, побољшању капацитета за превенцију и реаговање на инциденте, као и јачању сарадње са трећим земљама и међународним организацијама. Кроз ове мере, нормативни оквир ЕУ настоји да осигура безбедан и отпоран дигитални екосистем, прилагођавајући се брзом развоју технологија и еволуцији претњи.

8) ИЗВОРИ

- „Анализа ефеката Закона о изменама и допунама закона о информационој безбедности“. Интернет: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rsjp.gov.rs/upload/Analiza%20efekata%20propisa%20-ZOIB.pdf.
- Alexopoulos, M. J., Niemi, A., Skobiej, B., Sill Torres, F., “Examination of the Critical Infrastructure Resilience Directive From the Maritime Point of View”. *JCMS: Journal of Common Market Studies*, 2024. Интернет: https://doi.org/10.1111/jcms.13681.
- Boddy, Sara Elizabeth, *Case study: The decision-support framework and NIS2, CER, and DORA incident reporting obligations,* Jyväskylän Yliopisto Informaatioteknologian Tiedekunta, Master thesis, 2024.
- Clausmeier, D., “Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)”, *International Cybersecurity Law Review,* 4(1), 2023, pp. 79–90. Интернет: https://doi.org/10.1365/s43439-022-00076-5.
- “Digital Operational Resilience Act (DORA)”, European Insurance and Occupational Pensions Authority. Интернет: https://www.eiopa.europa.eu/digital-operational-resilience-act-DORA_en.
- “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive) (Text with EEA relevance)Text with EEA relevance”, *OJ* L 333, 27. 12. 2022.
- “Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)”, *OJ* L 333, 27. 12. 2022.
- Ericsson, ‘Ericsson Mobility Report’ (June 2022). Интернет: https://www.ericsson.com/49d3a0/assets/local/reports-papers/mobility-report/documents/2022/ericsson-mobility-report-june-2022.pdf, 12 March 2024.

- Franke, Ulrik, Brynielsson, Joel, *Cybersituational awareness – A systematic review of the literature*, Swedish Defence Research Agency, SE-164 90 Stockholm, Sweden, 2014.
- Giannino, Antonio, Valenti, Francesca, Sertori, Federico, "Is DORA the dawn of a new era for cybersecurity compliance in the EU's financial sectop?", *Journal of Financial Compliance*, Volume 8 / Number 1 / Autumn/Fall 2024.
- Novakovic, Marko, A review of the efficiency of justice and other elements of the 2022–2025 CEPEJ action plan: "Digitalisation for a better justice, in: Digitalization in Penal Law and Judiciary, ed. Matic Boskovic, Marina and Kostic, Jelena, Institut za uporedno pravo; Institut za kriminološka i sociološka istraživanja, 2022.
- "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", *OJ* L 119, 4.5.2016.
- "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity CERtification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)", *OJ* L 151, 7. 6. 2019.
- "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)", *OJ* L 333, 27. 12. 2022.
- "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)", *OJ* L, 2024/2847, 20. 11. 2024.
- "Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)", *OJ* L, 2025/38, 15. 1. 2025.
- Shaffique, Mohammed Raiz, "Cyber Resilience Act 2022: A silver bullet for cybersecurity of IOT devices or a shot in the dark?", *Computer Law & Security Review*, Volume 54, September 2024.

- Quinn, Stephen, Ivy, Nahla, Barrett, Matthew, Witte, Greg, Gardner, R. K., *Prioritizing Cybersecurity Risk for Enterprise Risk Management*, NIST, US Department of Commerce, 2022. Интернет: https://doi.org/10.6028/NIST.IR.8286B.
- Закон о информационој безбедности, *Сл. гласник РС*, бр. 6/2016, 94/2017 и 77/2019. Интернет: https://www.paragraf.rs/dnevne-vesti/080724/080724-vest10.html.

9) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Усвајање ових европских стандарда и најбољих пракси може донети вишеструке користи за Србију, под условом да се ти стандарди усвоје на одговарајући начин и имплементирају тако да дају највише ефекта.[33] Имајући у виду динамичност дигиталног окружења и значај координације, а све у контексту ЕУ аспирација Републике Србије, од изузетног значаја (као и у великој већини случајева када су ЕУ нормативни акти у питању) је да Србија усклади свој нормативни оквир у великој мери. У овом случају то ће ојачати националну информациону безбедност и отпорност на претње, а само усклађивање са европским стандардима може олакшати економску и технолошку сарадњу са земљама ЕУ, отварајући нове могућности за привредни развој и иновације, али и унапредити систем у Србији. Иако имплементација ових стандарда представља изазов, она такође пружа прилику за унапређење националних капацитета у области информационе безбедности. То укључује развој нових законских и регулаторних оквира, јачање институционалних капацитета, као и едукацију и обуку стручњака из области информационе безбедност. Тренутно је у Србији на снази Закон о информационој безбедности, који је по својој природи застарео и у току је израда новог закона.[34] Разлози за доношење измена и допуна Закона о информационој безбедности засновани су на потреби потпуног усклађивања са НИС Директивом ЕУ, која предвиђа мере за висок ниво безбедности мрежних и информационих система. Закон је иницијално усвојен пре доношења ове Директиве, али је потребно да се у потпуности усклади како би се осигурала адекватна заштита и реаговање у случајевима инцидената у информационо-комуникационим системима. Циљ измена јесте унапређење постојећег правног оквира ради ефикасније примене у пракси. Ово укључује

[33] Marko Novakovic, A review of the efficiency of justice and other elements of the 2022–2025 CEPEJ action plan: "Digitalisation for a better justice, in: Digitalization in Penal Law and Judiciary, ed. Matic Boskovic, Marina and Kostic, Jelena, Institut za uporedno pravo; Institut za kriminološka i sociološka istraživanja, 2022, pp. 201–212.

[34] Закон о информационој безбедности, *Сл. гласник РС*, бр. 6/2016, 94/2017 и 77/2019. Интернет: https://www.paragraf.rs/dnevne-vesti/080724/080724-vest10.html.

јачање капацитета Националног ЦЕРТ-а, успостављање јединственог система за пријаву инцидената, бољу сарадњу између ЦЕРТ-ова у Републици Србији и укључивање нових сектора у домен информационе безбедности. Предвиђене измене треба да обезбеде већу повезаност релевантних актера, унапређење превенције и ефикасније решавање инцидената који угрожавају информациону безбедност.[35]

EU INFORMATION SECURITY LEGAL FRAMEWORK

Marko NOVAKOVIĆ, Mihajlo VUČIĆ*

Abstract: In the modern digital age, the security of information systems and networks is the basis for the functioning of economic, social, and institutional structures. The European Union (EU) has recognised the importance of this area and developed a comprehensive legal framework that includes a number of directives and regulations with the aim of strengthening information security and resilience. This framework encompasses key acts such as the NIS2 Directive, which improves security standards and encourages cooperation between member states; the DORA Regulation, which deals with the management of digital risks in the financial sector; the CER Directive for the protection of critical infrastructures; as well as the CSA and CRA Regulations that define security standards for digital products and services. The paper analyses the existing EU legal framework, discusses its role in strengthening digital resilience, and examines the challenges in its implementation. Special attention is paid to the importance of these regulatory measures for the Republic of Serbia, which, as a candidate for EU membership, should harmonise its regulations with European standards. The implementation of the aforementioned directives and regulations represents not only a regulatory challenge but also an opportunity to improve national capacities in the field of information security.

Keywords: EU, information security, NIS2, DORA, CER, CSA, CRA.

[35] „Анализа ефеката Закона о изменама и допунама закона о информационој безбедности". Интернет: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rsjp.gov.rs/upload/Analiza%20efekata%20propisa%20-ZOIB.pdf.

* Institute of International Politics and Economics, Belgrade. E-mails: marko@diplomacy.bg.ac.rs; mihajlo@diplomacy.bg.ac.rs. ORCID iD: https://orcid.org/0000-0002-7753-7506; ORCID iD: https://orcid.org/0000-0002-0064-4987.