УДК: 004.056(4)
Biblid 1451-3188, 25 (2026)
Год XXV, бр. 93, стр. 145–162
Изворни научни рад
Рад примљен 07. 02. 2026. године
Рад одобрен 19. 02. 2026. године
DOI: https://doi.org/10.18485/iipe_ez.2026.25.93.8

ЕВРОПСКИ СТАНДАРДИ О САЈБЕР БЕЗБЕДНОСТИ

*Љубиша СТЕФАНОСКИ, Филип ВУЧЕН**

Апстракт: Јединствено дигитално тржиште (*Digital Single Market* – DSM) представља кључну компоненту стратегије Европске уније (ЕУ) за трансформацију једног од највећих светских економских простора у слободан и конкурентан дигитални простор. ЕУ је започела борбу за већи удео у дигиталном свету са усвајањем стратегије „Европа прилагођена дигиталном добу 2020 године". У циљу јачања стратешке аутономије и стварања јединственог дигиталног тржишта, ЕУ ће преко Комисије обезбедити практичне смернице и правну регулативу која ће у наредном периоду бити инкорпорирана у унутрашње правне системе држава чланица, и истовремено утицати на земље кандидате. Прилагођавање дигиталном добу значи да ће ЕУ до 2030. године чинити потребне напоре у ојачавању свог дигиталног суверенитета. У складу с тим, Савет европских националних регистара *(Council of European National Top Level Domain Registries* – CENTR*),* као удружење европских регистара националних домена највишег нивоа, има за циљ да својим члановима обезбеди форум за размену информација, притом поштујући културне и историјске разлике у локалним интернет заједницама. Због тога се у овом раду, у контексту деловања ове организације, разматра Директива (ЕУ) 2022/2555 познатија и као *NIS2 Директива.* Директива *(NIS2)*, која има

* Међународни Славјански Универзитет, Република Северна Македонија. E-mail: stefanoski_ljubisa@yahoo.com; ORCID iD: https://orcid.org/0009-0005-0331-152X; Јавна научна установа – Институт за интелектуалну својину Скопље, Република Северна Македонија. E-mail: filip.vucen@gmail.com; ORCID iD: https://orcid.org/0009-0003-8117-5856.

формални назив „Директива о мерама за високи заједнички ниво сајбер безбедности широм Уније“, представља акт који поставља једнаке, усклађене захтеве за сајбер безбедност у целој Унији. За земље кандидате, као што је Србија, *NIS 2* је релевантна у оквиру усаглашавања са ЕУ *acquis*-ом, као и за поглавља везана за информационо друштво, дигитализацију, безбедност и припреме критичне инфраструктуре за улазак у ЕУ. Следствено, овај рад пружа увид у утицај ове директиве на српско законодавство, будући да аутори сматрају да је она од посебне важности за дигиталну трансформацију српског друштва.

Кључне речи: Јединствено дигитално тржиште, Савет европских националних регистара, NIS2 Директива, Програм Дигитална Европа, ЕУ *acquis.*

1) УВОД

Недавни глобални шокови, попут пандемије COVID-19 и рата у Украјини, не само да су открили рањивости јединственог тржишта ЕУ, већ су истакли и његову централну улогу за конкурентност. Данас, јединствено дигитално тржиште ЕУ игра трансформативну улогу: оно повећава продуктивност и благостање потрошача путем електронске трговине и електронске управе, док правила ЕУ о подацима, платформама, вештачкој интелигенцији и сајбер безбедности подржавају поверење и отпорност. Кључни закони попут Закона о дигиталним услугама *(Digital Service Act* – DSA*)*, Закона о дигиталним тржиштима (*Digital Market Act* – DMA*)*, Електронске идентификације, аутентификације и услуге поверења 2.0 *(eIDAS 2.0)*, Закона о подацима *(Data Act* – DA*)*, Закона о вештачкој интелигенцији *(Artificial Intelegence Act* – AI Act*)* Директиве *NIS2*, Закона о сајбер отпорности *(Cyber Resilience Act* – CRA*),* по ступању на снагу били су постепено имплементирани.[1] Ово није случај и са Законом о дигиталним услугама

[1] “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC”, *OJ* L 257, 28. 8. 2014, pp. 73–114; “Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)”, *OJ* L, 2024/1689, 12. 7. 2024; “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)”, *OJ* L, 2024/2847, 20. 11. 2024.

(DSA) и Законом о дигиталном тржишту *(DMA),* који већ трансформишу европско тржиште кроз обавезе спровођења и усклађености.

Јединствено дигитално тржиште *(Digital Single Market* – DSM*),* представља кључну компоненту стратегије ЕУ за трансформацију једног од највећих светских економских простора у слободан и конкурентан дигитални простор.[2] Основни циљ је елиминација националних баријера у дигиталној економији како би се омогућило несметано кретање дигиталних добара, услуга, података и капитала унутар ЕУ.[3] Директива DSM настоји да створи услове у којима грађани и фирме могу да користе дигиталне услуге, купују, продају и сарађују преко државних граница као да су на једном тржишту. *Директива* (ЕУ) 2022/2555 (у даљем тексту: NIS2 Директива), заправо је директива ЕУ која уређује заједнички висок ниво сајбер безбедности унутар Уније. То није само „правно поглавље" у смислу преговарачког ЕУ *acquis*-а, већ самосталан правни акт који припада сфери права ЕУ унутар политике дигиталног тржишта и сигурности мреже и информација.[4]

NIS2 Директива припада у области правила у вези са дигиталним јединим тржиштем и инфраструктуром дигиталне економије, конкретно у домету сајбер безбедности и сигурности мрежа и информација. С друге стране, NIS2 Директива не припада једном од „поглавља преговора" као што је Поглавље 10 – „Информациона технологија и наука", јер таква категоризација ЕУ *acquis-a* није директно формална у ЕУ праву. Уместо тога, акт спада у политике Договора о функционисању ЕУ или ТФЕУ[5] *(Treaty on the Functioning of the European Union)*, које одређују правно уређење дигиталног тржишта и заштиту инфраструктуре, укључујући и безбедносне захтеве.[6] Унутар *acquis-a,* а у смислу „поглавља ЕУ", NIS2

[2] „Јединствено дигитално тржиште", Хисоур. Интернет: https://sr.hisour.com/ko/подаци/јединствено_дигитално_тржиште/, 16. 1. 2026.

[3] Torsten Bettinger, Domain Name Law and Practice – An International Handbook, Oxford University Press, Oxford, 2005; Milton Mueller, *Ruling the Root*, The MIT Press, Cambridge, Massachusetts, London, 2004; Jacqueline Lipton, *Internet Domain Names, Trademarks and Free Speech*, Edward Elgar Cheltenham, Northampton, MA, 2010; WIPO Overview of on Selected UDRP Questions, Third Edition, WIPO Arbitration and Mediation Center, 2017.

[4] Правни оквир на основу којег се воде преговори о приступању Републике Србије у ЕУ.

[5] Љупчо Сотироски, „Право и политики на ЕУ – Предизвици и очекувања" Асоцијација за корпоративна безбедност, владеење на правото и човекови права, Скопје, 2021.

[6] "Consolidated version of the Treaty on the Functioning of the European Union2, *OJ* C 326, 26.10.2012, pp. 47–390.

Директива припада области дигиталног тржишта/сајбер безбедности, а не традиционалном називу по броју поглавља (нпр. поглавље 23, 24 итд.) који обично важи за преговоре са кандидатима. За земље кандидате (нпр. Србију) NIS2 је релевантна у оквиру усаглашавања са ЕУ *acquis-ом*, поглавља везаних за информационо друштво, дигитализацију и безбедност, припреме критичне инфраструктуре за улазак у ЕУ. Иако не постоји директна правна или институционална веза између NIS2 Директиве и CENTR-а, ипак је реч о успостављању јасне индиректне и функционалне повезаности. Национални регистри домена или ccTLD (*Country Code Top-Level Domains)*, као оператери критичне интернет инфраструктуре, у бројним државама чланицама класификовани су као критични ентитети (*essential* или *important entities*) у смислу NIS2 Директиве. Као такви, они подлежу обавезама које се односе на управљање ризицима сајбер безбедности, спровођење техничких и организационих мера, као и пријављивање значајних безбедносних инцидената надлежним органима.

Сви смо упознати са уобичајеним екстензијама имена домена: *.com , .net , .org , .gov* итд., али може се уочити да неке веб-странице користе краће, мање уобичајене екстензије, као што су: *.de, .rs, .eu* или *.ru*. Оне се називају ccTLD-ови или домени највишег нивоа са националним кодом. Према Европској комисији, Закон о дигиталним услугама (DSA) или Закон о дигиталним тржиштима (DMA) имају два главна циља. Први је стварање безбеднијег дигиталног простора у којем су заштићена основна права свих корисника дигиталних услуга, а други циљ је успостављање једнаких услова за подстицање иновација, раста и конкурентности, како на јединственом европском тржишту, тако и на глобалном нивоу.[7]

Политике ЕУ, као политика слободне конкуренције или општа регулатива заштите података, остају велики изазови како за саму ЕУ, тако и за Србију као земљу кандидата за пуноправно чланство у ЕУ. У смислу принципа супсидијарности ЕУ, и DSA и DMA ће бити циљеви наднационалног нивоа. Разлог за то је што су проблеми прекограничне природе и нису ограничени на поједине државе чланице. Дигитални сектор као такав, а посебно основне платформске услуге, су прекограничне природе. Као што показује обим прекограничне трговине скоро 24% укупне онлајн трговине у Европи је прекогранично.[8]

[7] "Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC", Brussels, 15. 12. 2020, COM/2020/825 final.

[8] "24% of ecommerce in Europe is cross-border", Ecommerce News. Интернет: https://ecommercenews.eu/24-of-ecommerce-in-europe-is-cross-border/ 16. 1. 2026; "Proposal for a Regulation of the European Parliament and of the Council on

2) САВЕТ ЕВРОПСКИХ НАЦИОНАЛНИХ РЕГИСТАРА (CENTR)

NIS2 Директива којом се успоставља јединствен и високи ниво сајбер безбедности у целој ЕУ део је политике ЕУ и јединственог дигиталног тржишта у области сајбер безбедности и сигурности мрежа и информационих система. Њоме се замењује и знатно проширује ранија NIS1 Директива (2016/1148). Разлози за то су више него очекивани због драматичног раста сајбер напада – „рансомвер" (*ransomware*) и „фишинг" (phishing) напада на критичну инфраструктуру, неуједначене примена старије NIS1 Директиве у државама чланицама, дигитализације кључних услуга (енергија, здравство, финансије, транспорт) и потребе за отпорношћу дигиталног тржишта ЕУ. Основни циљ јесте обезбеђење функционисања, кључних и важних услуга чак и током сајбер инцидената. CENTR као удружење европских регистара националних домена највишег нивоа има за циљ да својим члановима обезбеди форум за размену информација. У том смеру, улоге и функције CENTR-а и NIS2 Директиве су узајамно повезани, јер NIS2 Директива поставља обавезе које директно утичу на ccTLD регистре и DNS провајдере, док, с друге стране, асоцијација CENTR прати, анализира и даје стручну подршку својим члановима у разумевању и примени тих правних обавеза. У сагласности са NIS2 Директивом, државе чланице имају обавезу да транспонују и примене ове захтеве у своје национално право и истовремено успоставе надзор над организацијама које спадају у садржај NIS2 Директивом (нпр. енергетика, здравство, дигиталне инфраструктуре итд.). С друге стране, Савет европских националних регистара окупља организације, правних субјеката или појединаца који управљају националним доменима, као што су национални регистар за *.rs u .срб* домене у Србији, национални регистар за *.rf u .рф* домене у Руској Федерацији, национални регистар за *.es* домене у Шпанији итд.[9] Заправо, реч је о пројекту из марта 1998. године који је незванично финансиран од стране учесника регистара, који ће касније у 1999. години прерасти у CENTR. Реч је о легално основаној непрофитној компанији у Великој Британији, која је касније у 2006. години регистрована као непрофитна организација са седиштем у Бриселу (Белгија).[10] Извор

contestable and fair markets in the digital sector (Digital Markets Act)", Brussels, 15. 12. 2020, COM(2020) 842 final.

[9] "CENTR Background and History". Интернет: https://www.centr.org/about/about-centr/item/background-and-history.html, 26. 1. 2026; https://www.rnids.rs, 20. 12. 2025.

[10] *Ibid.*

финансирања активности Савета европских организација који управљају националним доменима је чланарина од свих својих чланица. У питању су више од педесет земаља чланица између којих и неколико ваневропских земаља као Канада, Израел, Иран, Палестинска територија и други ентитети.[11] Примарни циљ и функција CENTR-а је да делује као канал комуникације између провајдера и других организација које се баве Интернетом, на тај начин што организује састанке и радионице на којима се расправља о правним питањима која утичу на рад националних регистара, а у циљу унапређивања услуга за кориснике интернета.[12] Према томе, улога и сврха CENTR-а је да промовише и развија високе стандарде рада регистара националних домена највишег нивоа, да координира њихов рад и јача међусобну сарадњу и обезбеди размену искустава, притом поштујући културне и историјске разлике у локалним интернет заједницама.

3) РЕЛЕВАНТНЕ ЕУ МЕРЕ САЈБЕР БЕЗБЕДНОСТИ КОЈЕ УТИЧУ НА ЈЕДИНСТВЕНОСТ ДИГИТАЛНОГ ТРЖИШТА

Доношењем Директиве (ЕУ) 2022/2555 о мерама за висок заједнички ниво сајбер безбедности широм Уније, укинута је Директива (ЕУ) 2016/1148 или (НИС1). Отуд, NIS2 Директива представља кључни правни акт ЕУ који треба да унапреди и усклади сајбер безбедносне стандарде у свим државама чланицама ЕУ. Ово је тренутно главна мера ЕУ која директно утиче на регистре имена домена и регулише, између осталог, и: *Обавезе у вези са сајбер безбедношћу*: Директива НИС2 третира регистре имена ТЛД-а и добављаче ДНС услуга као суштинске ентитете са обавезним дужностима управљања ризиком од сајбер безбедности и извештавања о инцидентима;[13] *Тачност података о регистрацији домена:* Сагласно, члану 28. NIS2 Директиве, од држава чланица захтева се да обезбеде да код земље-ТЛД регистри и провајдери услуга регистрације

[11] CENTR има 53 пуноправна члана, 10 придружених чланова и доделио је статус посматрача за 12 организација. Видети: "Members". Интернет: https://www.centr.org/about/members.html, 26. 1. 2026.

[12] David Lindsay, *International Domain Name Law: ICANN and the UDRP,* Hart Publishing, Oxford, 2007, p. 9.

[13] "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 (NIS 2 Directive)", *OJ* L, 333, 27. 12. 2022, pp. 80–152.

домена прикупљају, одржавају и верификују тачне и потпуне податке о регистрацији имена домена (име домена, датум регистрације, име регистранта, имејл и број телефона);[14] *Приступ и транспарентност*: Регистри морају учинити јавно доступним податке о доменима које нису лични, и одговорити на захтеве и образложити захтеве за приступ одређеним подацима о регистрацији у дефинисаним временским оквирима (на пр. 72 сата); *Сарадњу између регистара и регистрара:* Ова сарадња је неспорно неопходна, да би се избегло дуплирање прикупљања података и обезбедила усклађеност; *Статус имплементације:* NIS2 је ступио на снагу 2023. године, а од држава чланица се захтевало да га транспонују у национално законодавство закључно са 17. октобром 2024. године, и почну са применом од 18. октобра 2024. године.[15] Важност ове Директиве огледа се у хармонизацији заштите и она поставља јединствен стандард у ЕУ, што олакшава заштиту прекограничних услуга и инфраструктуре, обезбеђује ширу покривеност и безбедност и омогућава бољу координацију између држава чланица и институција ЕУ.[16] ЕУ је започела борбу за већи удео у дигиталном свету усвајањем стратегије „Европа прилагођена дигиталном добу 2020 године", којом на дугорочном периоду ЕУ планира да се одазове овом дигиталном изазову. Стратегија је понудила основу за јачање конкурентности ЕУ у тзв. „четвртој индустријској револуцији". У циљу јачања стратешке аутономије и стварања јединственог дигиталног тржишта, ЕУ ће преко Комисије обезбедити практичне смернице и правну регулативу која ће у наредном периоду бити инкорпорирана у унутрашње правне системе држава чланица. Прилагођавање дигиталном добу значи и да ће ЕУ до 2030. године чинити потребне напоре у ојачавању свог дигиталног суверенитета. Најновија регулатива ЕУ у дигиталној области обухваћена је Програмом политике дигиталне деценије 2030, од 14. децембра 2022. године.[17] Одлука (ЕУ) 2022/2481 којом се успоставља политичка агенда за дигиталну

[14] *Ibid.,* Art. 28; "Protect your Intellectual Property online with WIPO's ccTLD Services", WIPO. Интернет: https://www.wipo.int/amc/en/domains/cctld/index.html#1, 23. 12. 2025.

[15] "CENTR publishes comment on the proposed NIS 2 Directive", CENTR. Интернет: https://www.centr.org/news/news/centr-comment-nis-2.html, 23. 12. 2025.

[16] "Strengthening EU-wide cybersecurity and resilience – provisional agreement by the Council and the European Parliament", Council of the EU, Press release, 13. 5. 2022.

[17] "Digital Decade – Policy programme", European Commission. Интернет: https://digital-strategy.ec.europa.eu/en/policies/digital-decade-policy-programme, 23. 12. 2025.

деценију до 2030. године, представља важан правни извор који би требало да омогући подстицање дигиталне трансформације ЕУ.[18] Њоме се предвиђају општи и конкретни дигитални циљеви, механизми праћења и успостављања сарадње држава чланица и трећих држава, као и правни оквир за пројекте које би требало да омогуће реализацију Програма политике дигиталне деценије.[19] У приказаној табели налазе се и остали Правни акти ЕУ, који се односе или имају директан или индиректан ефекат на Савет европских националних регистара *(Council of European National Top Level Domain Registries,* CENTR*)*.

[18] "Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030", *OJ* L 323, 19. 12. 2022, pp. 4–26; Сања Јелисавац, „Програм политике дигиталне деценије Европске уније", Европско законодавство, 2023, бр. 81–82, стр. 217–228.

[19] „Програм Дигитална Европа", Министарство информисања и телекомуникација Републике Србије. Интернет: https://mit.gov.rs/tekst/ 18520/program-digitalna-evropa-.php, 23. 12. 2025.

Графички приказ 1.

Мера	**Директан утицај на ccTLD / чланове CENTR / Политика ЕУ**	**Тип мере**
Директива (ЕУ) 2022/2555NIS2 директива	Обавезе у вези са сајбер безбедношћу и тачношћу података о домену	Директива ЕУ
НИС Кооп – ГрупнеНИС смернице	Заштита личних података регистраната	Необавезујуће смернице ЕУ
Регулатива (ЕУ) 2019/517 о имплементацији и функционисању .eu домена[20]	Правни оквир за .eu ccTLD укључујући правила о доступности, управљању и његовој администрацији	Уредба ЕУ
Општа регулатива о заштити података Регулатива (ЕУ) 2016/679 (General Data Protection Regulation – GDPR)	Заштита личних података регистраната	Уредба ЕУ
Закон о дигиталним услугама (DSA)Regulation (ЕУ) 2022/2065[21]	Појашњења статуса одговорности и посредника	Уредба ЕУ
Предлози ЕУ за потрошаче/ интелектуалну својину	Потенцијалне обавезе регистра	Иницијативе и политике ЕУ
Политике у вези са интернетским управљањем и безбедношћу које развијају ЕУ институције[22]	Потенцијалне обавезе регистра	Иницијативе и политике ЕУ

ЕУ регулатива од значаја за рад Савета европских националних регистара (CENTR)Извор: www.centr.org

[20] "ICANN and the European Union General Data Protection Regulation", ICANN. Интернет: https://www.icann.org/resources/pages/icann-eu-gdpr-2022-12-22-en, 28. 12. 2025.

[21] "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)", *OJ* L 277, 27. 10. 2022, pp. 1–102.

[22] "Call for experts – Internet Governance and Domain Name System (DNS)", European Commission. Интернет: https://digital-strategy.ec.europa.eu/en/news/call-experts-internet-governance-and-domain-name-system-dns

[23] "Connecting European dots", CENTR. Интернет: https://www.centr.org, 28. 12. 2025.

4) NIS2 ДИРЕКТИВА И САЈБЕР БЕЗБЕДНОСТ

Циљ NIS2 Директиве, јесте да унапреди ниво заштите од сајбер претњи и награди одговорност у важним секторима, с обзиром на брзу дигитализацију више сложених напада и било какву фрагментацију политика у ранијем систему.[24] У 2016. години ЕУ је усвојила прву Директиву о безбедности мрежа и информационих система, познату као NIS1 Директива ЕУ (2016/1148). Шест година касније, 14. децембра 2022, Европски парламент и Савет ЕУ усвајају Директиву (ЕУ) 2022/2555 (NIS2), као нову модернизовану верзију претходне Директиве, а ступила је на снагу 16. јануара 2023. године. Рок за имплементацију Директиве био је 17. октобар 2024. године, до када су државе чланице требале да транспонују Директиву у своје национално законодавство (тј. да усвоје законе који спроводе директиву). Од 18. октобра 2024. године Директива званично замењује претходну верзију Директиве. Према неким извештајима, више држава каснило је у транспозицији због чега је Комисија иницирала процедуре против њих за непоштовање рокова.[25] Главни циљ и значај NIS2 Директиве је да се подигне ниво сајбер безбедности у целој ЕУ, као и да се унификују правила између свих чланица. Тиме се повећава отпорност система на инциденте и нападе, преко пооштравања обавеза надзора и могућих казни са проширивањем броја сектора који морају да се придржавају правила, како би се унапредила сарадња између држава и институција.[26] Ови циљеви су одговор на све чешће сајбер нападе и потребу да се осигура стабилност кључних дигиталних и физичких инфраструктура у ЕУ. Директива NIS2 примењује се на секторе који су критично важни: енергија (енергетски системи); транспорт; здравство и фармација као инфраструктура; финансијски сектор (банке, тржишта

[24] "NIS 2 strengthens cybersecurity across the EU by setting higher standards for essential services", ENISA. Интернет: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2, 28. 12. 2025. "The NIS2 Directive: A high common level of cybersecurity in the EU", Think-Thank. Интернет: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI%282021%29689333, 27. 12. 2025.

[25] "Комисията призовава 19 държави членки да транспонират изцяло Директивата за МИС 2", Европейската комисия. Интернет: https://digital-strategy.ec.europa.eu/bg/news/commission-calls-19-member-states-fully-transpose-nis2-directive, 28. 12. 2025.

[26] "NIS2 Directive: securing network and information systems", European Commission. Интернет: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, 28. 12. 2025.

капитала); информационо-комуникационе технологије и дигитална инфраструктура; вода и управљање отпадом; поштанске и курирске услуге; јавна управа; производња критичних производа и други кључни сектори који утичу на економију и јавни живот. [27] Директива значајно проширује круг субјеката, тако да се NIS 2 односи на основне *(Essentials)* субјекте: енергетика (струја, гас, нафта), транспорт (авио, железница, луке), банкарство и финансијска тржишта, здравство, водоснабдевање, дигитална инфраструктура (DNS, cloud, data центри) и јавну управу, као и важне *(Important)* субјекте: поштанске и курирске услуге, управљање отпадом, производња кључне ИКТ опреме, дигитални сервиси (онлајн платформе, SaaS) и истраживачке организације. Кључне обавезе које NIS2 уводи су: управљање ризицима, обавеза пријаве инцидената, одговорност менаџмента и надзор и казне. У смислу управљања ризицима, организације морају да имају: мере заштите система, управљање инцидентима, резервне копије, безбедност ланца снабдевања, криптографију и контролу приступа. Око обавеза пријаве инцидената битна су: 24 сата – као прва пријава значајног инцидента, затим 72 сата – као детаљнија информација и коначни извештај након решавања инцидента. За одговорност менаџмента, само руководство је директно одговорно и оно мора да прође кроз обавезне обуке и за евентуално непрофесионално извршење службених дужности могуће су и личне санкције. У вези надзора и казни, предвиђене су високе новчане казне (до 10 милиона евра или 2% глобалног прихода), затим појачан надзор над „основним“ субјектима и веза са дигиталним тржиштем ЕУ. Заправо *NIS2* Директива штити поверење у дигиталне услуге, затим спречава поремећаје у прекограничном пословању, обезбеђује једнаке услове за све државе чланице, допуњује друге акте као што су: *Digital Operational Resilience Act (DORA),*[28] *Cyber Resilience Act (CRA*),[29] *General Data Protection Regulation (GDPR).*[30] Зато је она стуб сајбер безбедности јединственог дигиталног тржишта *ЕУ*. За земље кандидате (нпр. Србију), NIS2 је релевантна у оквиру: усаглашавања са *ЕУ acquis-ом*, као и за поглавља везана за информационо друштво, дигитализацију и безбедност, као и припреме критичне инфраструктуре за улазак у ЕУ.

---

[27] *Ibid.*

[28] “Digital Operational Resilience Act (DORA)”, EIOPA. Интернет: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en, 27. 12. 2025.

[29] “Cyber Resilience Act”, European Commission. Интернет: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act, 4. 1. 2026.

[30] “General Data Protection Regulation GDPR”, Intersoft Counsalting. Интернет: https://gdpr-info.eu/, 4. 1. 2026.

5) ДАТУМ СТУПАЊА НА СНАГУ

Директива (ЕУ) 2022/2555 Европског парламента и Савета од 14. децембра 2022. године о мерама за висок заједнички ниво сајбер безбедности широм Уније, којом се мења Уредба (ЕУ) бр. 910/2014 и Директива (ЕУ) 2018/1972 и ставља ван снаге Директива (ЕУ) 2016/1148 (Директива NIS 2), објављена је у Службеном листу ЕУ дана 27. 12. 2022. године, а ступила је на снагу двадесетог дана од објављивања, тј. 16. 1. 2023. године.

6) ИЗВОРИ

Bettinger, Torsten, *Domain Name Law and Practice – An International Handbook*, Oxford University Press, Oxford, 2005.

"Call for experts – Internet Governance and Domain Name System (DNS)", European Commission. Интернет: https://digital-strategy.ec.europa.eu/en/news/call-experts-internet-governance-and-domain-name-system-dns

"CENTR Background and History". Интернет: https://www.centr.org/ about /about-centr/item/background-and-history.html, 26. 1. 2026; https://www.rnids.rs, 20. 12. 2025.

"CENTR publishes comment on the proposed NIS 2 Directive", CENTR. Интернет: https://www.centr.org/news/news/centr-comment-nis-2.html, 23. 12. 2025.

"Connecting European dots", CENTR. Интернет: https://www.centr.org, 28. 12. 2025.

"Consolidated version of the Treaty on the Functioning of the European Union2, *OJ* C 326, 26. 10. 2012.

"Cyber Resilience Act", European Commission. Интернет: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act, 4. 1. 2026.

"Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030", *OJ* L 323, 19. 12. 2022.

"Digital Decade – Policy programme", European Commission. Интернет: https://digital-strategy.ec.europa.eu/en/policies/digital-decade-policy-programme, 23. 12. 2025.

"Digital Operational Resilience Act (DORA)", EIOPA. Интернет: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en, 27. 12. 2025.

"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 (NIS 2 Directive)", *OJ* L, 333, 27. 12. 2022.

"General Data Protection Regulation GDPR", Intersoft Counsalting. Интернет: https://gdpr-info.eu/, 4. 1. 2026.

"ICANN and the European Union General Data Protection Regulation", ICANN. Интернет: https://www.icann.org/resources/pages/icann-eu-gdpr-2022-12-22-en, 28. 12. 2025.

„Јединствено дигитално тржиште", Хисоур. Интернет: https://sr.hisour.com/ko/подаци/јединствено_дигитално_тржиште/, 16. 1. 2026.

"Комисията призовава 19 държави членки да транспонират изцяло Директивата за МИС 2", Европейската комисия. Интернет: https://digital-strategy.ec.europa.eu/bg/news/commission-calls-19-member-states-fully-transpose-nis2-directive, 28. 12. 2025.

Lipton, Jacqueline, *Internet Domain Names, Trademarks and Free Speech*, Edward Elgar Cheltenham, Northampton, MA, 2010.

Lindsay, David, *International Domain Name Law: ICANN and the UDRP,* Hart Publishing, Oxford, 2007.

"Members". Интернет: https://www.centr.org/about/members.html, 26. 1. 2026.

Mueller, Milton, *Ruling the Root*, The MIT Press, Cambridge, Massachusetts, London, 2004.

Национални ЦЕРТ Републике Србије – Регулаторно тело за електронске комуникације и поштанске услуге. Интернет: https://www.cert.rs/cesto-postavljana-pitanja.html, 10. 1. 2026.

"NIS 2 strengthens cybersecurity across the EU by setting higher standards for essential services", ENISA. Интернет: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2, 28. 12. 2025.

"NIS2 Directive: securing network and information systems", European Commission. Интернет: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, 28. 12. 2025.

"Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)", Brussels, 15. 12. 2020, COM(2020) 842 final.

"Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC", Brussels, 15. 12. 2020, COM/2020/825 final.

"Protect your Intellectual Property online with WIPO's ccTLD Services", WIPO. Интернет: https://www.wipo.int/amc/en/domains/cctld/index.html#1, 23. 12. 2025.

"Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)", *OJ* L 277, 27. 10. 2022, pp. 1–102.

"Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)", *OJ* L, 2024/1689, 12. 7. 2024.

"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)", *OJ* L, 2024/2847, 20. 11. 2024.

„Програм Дигитална Европа", Министарство информисања и телекомуникација Републике Србије". Интернет: https://mit.gov.rs/tekst /18520/program-digitalna-evropa-.php, 23. 12. 2025.

"Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC", *OJ* L 257, 28. 8. 2014.

Сања Јелисавац, „Програм политике дигиталне деценије Европске уније", Европско законодавство, 2023, бр. 81–82.

Сотироски, Љупчо, „Право и политики на ЕУ – Предизвици и очекувања", Асоцијација за корпоративна безбедност, владеење на правото и човекови права, Скопје, 2021.

„Србија наставља да на дневном нивоу комуницира и сарађује са Европском комисијом", Политика. Интернет: https://www.politika.rs/ scc/clanak/721930/srbija-nastavlja-da-na-dnevnom-nivou-komunicira-i-saraduje-sa-evropskom-komisijom, 18. 1. 2026.

"Strengthening EU-wide cybersecurity and resilience – provisional agreement by the Council and the European.

"The Digital Europe Programme", European Commission. Интернет: https:// digital-strategy.ec.europa.eu/en/activities/digital-programme, 20. 1. 2026.

"The NIS2 Directive: A high common level of cybersecurity in the EU", Think-Thank. Интернет: https://www.europarl.europa.eu/thinktank/en/document /EPRS _BRI%282021%29689333, 27. 12. 2025.

"24% of ecommerce in Europe is cross-border", Ecommerce News. Интернет: https://ecommercenews.eu/24-of-ecommerce-in-europe-is-cross-border/ 16. 1. 2026.

WIPO Overview of on Selected UDRP Questions, Third Edition, WIPO Arbitration and Mediation Center, 2017.

„Закон о информационој безбедности", *Службени гласник Републике Србије* бр. 91/2025.

7) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Утицај NIS2 директиве – (ЕУ) 2022/2555 на српско законодавство је индиректан, али значајан. Србија није обавезна да транспонује Директиву као такву, али је кроз нови Закон о информационој безбедности (2025) и праксе у области сајбер безбедности усвојила широк спектар принципа и обавеза који су усклађени са NIS2 Директивом.[31] Зашто је Директива NIS 2 важна за Републику Србију? Иако Србија није чланица ЕУ, значај NIS 2 Директиве за Србију је вишеструк, и то ради:

Усклађивања са правом ЕУ (ЕУ *acquis*)

Србија је држава кандидат за чланство у ЕУ и има обавезу да постепено усклађује своје законодавство са правом ЕУ и то, посебно, у областима дигитализације и безбедности. Због тога, Директива NIS 2 индиректно је релевантна за Поглавље 10 (Информационо друштво и медији) и Поглавље 31 (Спољна, безбедносна и одбрамбена политика).

Утицаја на домаће законодавство

Република Србија усвојила је Закон о информационој безбедности, Национални CERT Републике Србије, успоставила је Регулаторно тело за електронске комуникације и поштанске услуге, национални CERT и секторске CERT-ове. [32] Међутим, NIS2 поставља више стандарде, затим захтева прецизнију класификацију субјеката и инсистира на управљању ризицима и одговорности менаџмента. Због свега овога у пракси, Србија ће

[31] „Закон о информационој безбедности", *Службени гласник Републике Србије* бр. 91/2025.

[32] *Ibid.;* Национални ЦЕРТ Републике Србије – Регулаторно тело за електронске комуникације и поштанске услуге. Интернет: https://www.cert.rs/cesto-postavljana-pitanja.html, 10. 1. 2026.

на путу ка ЕУ морати да измени или допуни постојеће законодавство и/или уведе строже обавезе за кључне дигиталне и инфраструктурне субјекте.

Утицаја на српске компаније које послују са ЕУ

Многе српске информационо-техничке компаније (ИТ), које пружају (ИТ) услуге клијентима у ЕУ и раде као cloud, hosting, DNS или софтверски провајдери, или су можда део су ланаца снабдевања у ЕУ, мораће иако нису у ЕУ индиректно да поштују NIS2 јер их њихови ЕУ партнери на то обавезују.

Националне и регионалне сајбер безбедности

Сајбер претње, нажалост, не познају границе и често имају регионални карактер. NIS2 подстиче сарадњу између држава и размену информација о инцидентима, кроз имплементацију заједничких стандарда. За Републику Србију то значи већу отпорност државних информационих система, бољу заштиту критичне инфраструктуре и јачање поверења међународних партнера. У овом правцу су и кључне обавезе (кроз усклађивање са EU *acquis*-ом) које ће бити релевантне и за Србију, кроз процену ризика и доношење безбедносних мера, обавезно пријављивање инцидената, усвајање планова континуитета пословања, преузимање одговорности руководства и спровођење санкција и мера надзора.

Закључак који се намеће јесте да NIS2 директива има велики значај за Републику Србију, иако није директно обавезујућа, јер утиче на реформу домаћег законодавства подстичући усаглашавање са стандардима ЕУ. Она погађа српске компаније које послују на ЕУ тржишту, или су повезане са њим, обезбеђујући правну и техничку предвидљивост. Директива јача националну сајбер безбедност кроз успостављање обавеза за критичне и важне инфраструктуре и представља корак ка пуном чланству Србије у Европској унији, јер показује спремност за усвајање европских регулаторних стандарда. Наиме, Република Србија је 30. јуна 2023. године званично постала пуноправна чланица Програма Дигитална Европа, потписивањем Споразума са Европском комисијом.[33] Овим споразумом Србија је добила могућност да активно учествује у пројектима, иницијативама и позивима за финансирање у оквиру Програма, под истим

[33] „Србија наставља да на дневном нивоу комуницира и сарађује са Европском комисијом“, Политика. Интернет: https://www.politika.rs/scc/clanak/721930/srbija-nastavlja-da-na-dnevnom-nivou-komunicira-i-saraduje-sa-evropskom-komisijom, 18. 1. 2026.

условима као и државе чланице ЕУ. Ово значи да правна и физичка лица из Србије, као на пример (ИТ) компаније, стартапи, истраживачке организације, образовне институције, државне установе и невладин сектор – могу да аплицирају за средства из Програма, самостално или у партнерству са субјектима из других европских земаља. Чланство у Програму Дигитална Европа представља значајну прекретницу у европским интеграцијама Србије, али и кључну подршку дигитализацији домаће привреде, науке и јавне управе.[34] Њоме се отварају могућности за привлачење инвестиција у (ИТ) сектор и иновациону инфраструктуру, успостављање сарадње са престижним европским партнерима, размену знања, искустава и добрих пракси, јачање капацитета државне управе за пружање ефикаснијих и дигитализованих услуга, едукацију и унапређење вештина стручњака, студената и шире јавности, бржи технолошки развој и подршку стартап екосистему. На основу потписаног споразума, правна и физичка лица са пребивалиштем у Републици Србији могу да аплицирају за финансирање пројеката, и у равноправном су положају са субјектима из земаља пуноправних чланица ЕУ када је реч о додели бесповратних средстава из европских фондова.[35]

[34] „Програм Дигитална Европа“, *op. cit.*

[35] "The Digital Europe Programme", European Commission. Интернет: https://digital-strategy.ec.europa.eu/en/activities/digital-programme, 20. 1. 2026.

EUROPEAN CYBERSECURITY STANDARDS

Ljubiša STEFANOSKI, Filip VUČEN*

Abstract: The Digital Single Market (DSM) is a key component of the European Union (EU) strategy to transform one of the world's largest economic areas into a free and competitive digital space. The EU has begun the fight for a greater share in the digital world with the adoption of the "Europe fit for the digital age 2020" strategy. To strengthen strategic autonomy and create a single digital market, the EU will provide, through the Commission, practical guidelines and legal regulations that will be incorporated into the internal legal systems of Member States in the coming period. At the same time, it influences the candidate countries. Adapting to the digital age means that by 2030, the EU will make the necessary efforts to strengthen its digital sovereignty. Accordingly, the Council of European National Top-Level Domain Registries (CENTR), as an association of European national top-level domain registries, aims to provide its members with a forum for information exchange while respecting the cultural and historical differences of local Internet communities. Therefore, in the context of the activities of this organisation, this paper discusses Directive (EU) 2022/2555, also known as the NIS2 Directive. The Directive (NIS2), which has the formal title "Directive on measures for a high common level of cybersecurity across the Union", is an act that sets equal, harmonised requirements for cybersecurity throughout the Union. For candidate countries, such as Serbia, NIS 2 is relevant in the framework of alignment with the EU acquis, as well as chapters related to information society, digitalisation, security, and preparation of critical infrastructure for EU accession. Consequently, this paper provides insight into the impact of this directive on Serbian legislation, as the authors believe it to be of particular importance for the digital transformation of Serbian society.

Keywords: Digital Single Market, Council of European National Registers, NIS2 Directive, Digital Europe Programme, EU *acquis.*

* International Slavic University, Republic of North Macedonia. E-mail: stefanoski_ljubisa@yahoo.com; ORCID iD: https://orcid.org/0009-0005-0331-152X; Public Scientific Institution – Institute for Intellectual Property Skopje, Republic of North Macedonia. E-mail: filip.vucen@gmail.com; ORCID iD: https://orcid.org/0009-0003-8117-5856.