УДК: 004.6:347.2(4-672EU)
Biblid 1451-3188, 17 (2018)
Год XVII, бр. 65, стр. 125–136
Изворни научни рад

БЕЗБЕДНОСТ МРЕЖЕ И ИНФОРМАТИЧКИ СИСТЕМИ У ПРАВУ ЕВРОПСКЕ УНИЈЕ

Озрен УЗЕЛАЦ[1]

Апстракт: Дигиталне технологије пружају велике могућности у области управних процедура, привредних активности и потреба друштва, при чему се свакодневно појављују нове врсте производа и услуга информатичке делатности које не познају границе националних држава. С друге стране, безбедносни инциденти у вези са дигиталном технологијом су све већих размера, а њихова учесталост представља озбиљну претњу функционисању мрежних и информатичких система. Предмет анализе представљају правни акти Европске уније који се односе на регулацију безбедности мреже и информатичких система.

Кључне речи: безбедност, мреже, технологије, дигиталне услуге, информатички системи, стратегија, ризици.

1) УВОД

Мрежни и информатички системи и услуге имају једну од важних улога у модерном друштву због чега су њихова поузданост и безбедност предуслов за трајно обављање привредне и друштвене активности и функционисање тржишта. С друге стране, безбедносни инциденти су све већих размера, а њихова учесталост и могућ утицај представљају озбиљну претњу функционисању мрежних и информатичких система. Штета или прекид рада мреже и информатичких система могу да угрозе обављање активности приватног и јавног сектора, наруши поверење корисника, проузрокује веће финансијске губитке и штету. С друге стране, дигиталне технологије пружају

[1] Универзитет у Новом Саду, Економски факултет у Суботици, E-mail: o3peh_y@yahoo.com.

велике могућности у бројним областима као што су на пример, управне процедуре, трговина, саобраћај и комуникације, при чему се свакодневно појављују нове врсте производа и услуга информатичке делатности које не познају границе националних држава. Један од циљева за уједначен и ефикасан приступ коришћењу предности дигиталних технологија, поред модернизације права интелектуалне својине због промењеног понашања потрошача, било је доношење прописа ради подстицања примене дигиталних технологија и услуга преко Интернета које би према Жану-Клоду Јункеру, председнику Европске комисије (даље у тексту: Комисија), требало да постану хоризонтална политика која обухвата јавни сектор и све секторе привреде.[2] Како је истакнуто у Стратегији јединственог дигиталног тржишта од 6. маја 2015. године, дигитална привреда може да допринесе ширењу тржишта, квалитетнијем пружању услуга по бољим ценама, већи избор и нове изворе запошљавања. Осим тога, јединствено дигитално тржиште може да створи нове пословне шансе новооснованим привредним друштвима, постојећим да омогући раст и коришћење предности тржишта од више од 500 милиона људи.[3] У последњих неколико година Комисија је донела низ прописа и предузела одређене мере ради подизања спремности у одбрани од информатичких инцидената свих заинтересованих субјеката на територији Европске уније (даље у тексту: ЕУ). У наставку излагања осврнућемо се на оне који су најважнији за постављену тему у овом раду.

2) МЕРЕ ЕУ

Један од првих корака на територији ЕУ у смеру информатичке безбедности било је оснивање Агенције ЕУ за мреже и информатичке системе (*European Union Agency for Network and Information Security* – ENISA) 2004. године,[4] чији је основни циљ обезбеђивање високог нивоа безбедности мрежа и информатичих система на територији ЕУ. Ова агенција: (а) прикупља и анализира податке о безбедносним инцидентима и новим ризицима, а посебно оне који на нивоу ЕУ

[2] Jean-Claude Juncker, "Political Guidelines for the next European Commission – A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change", Opening Statement in the European Parliament Plenary Session, Strasbourg, 15 July 2014, Priority n°2: A Connected Digital Single Market.

[3] *A Digital Single Market Strategy for Europe*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 6.5.2015 COM(2015) 192 final, p. 3.

[4] Уредба о оснивању Агенције ЕУ за мреже и информатичке системе (Regulation /EC/ No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, *Official Journal of the European Union*, L 77, 13.3.2004, p. 1-11).

могу да утичу на отпорност и расположивост електронских комуникационих мрежа, као и на аутентичност, интегритет и поверљивост информација којима се преко њих приступа и врши слање и достављањем резултата тих анализа државама чланицама и Комисији; (б) даје савете и пружа помоћ, сходно својим циљевима, Европској скупштини, Комисији, европским и надлежним националним органима које су основале државе чланице; (ц) унапређује сарадњу различитих актера који послују у области мрежне и информатичке безбедности, поред осталог, редовним организовањем саветовања у индустрији, на универзитетима као и у другим секторима, успостављањем контаката са органима ЕУ, органима који врше јавна овлашћења држава чланица, приватним сектором и потрошачким организацијама; (д) обезбеђује сарадњу Комисије и држава чланица у утврђивању начина за спречавање, решавање и реаговање на мрежна и информатичка безбедносна питања; (е) доприноси подизању знања и расположивости за благовремено, објективно и детаљно информисање о мрежним и информатичким безбедносним питањима за све кориснике, поред осталог, промовисањем размене информација о најбољим поступцима, укључујући и методе за упозоравање корисника и тражењем синергије иницијатива приватног и јавног сектора; (ф) помаже Комисији и државама чланицама у дијалогу са индустријом ради решавања безбедносних проблема код хардвера и софтвера; (г) прати развој стандарда за производе и услуге о мрежној и информатичкој безбедности; (х) саветује Комисију о анализи области мрежне и информатичке безбедности, као и ефикасној примени технологије превенције ризика; (и) промовише активности оцене ризика, решења интероперативног управљања ризицима и анализира решења управљања превентивним мерама са организацијама јавног и приватног сектора; (ј) доприноси напорима ЕУ у сарадњи са трећим државама и међународним организацијама у промоцији заједничког глобалног решавања мрежних и информатичких питања, чиме доприноси развоју културе мрежне и информатичке безбедности; и (к) самостално изражава своје закључке, опредељења и даје савете о питањима из своје надлежности и постављених циљева.[5] Стратегијом ЕУ о информатичкој безбедности 2013. године планирано је остваривање пет следећих циљева: постизање информатичке отпорности, значајно смањење информатичког криминала, утврђивање политике капацитета и начина одбране од информатичких напада, развијање индустријских и технолошких ресурса за информатичку безбедност и утврђивање усклађене међународне политике о информатичком простору ЕУ и заштита суштинских вредности ЕУ.[6] Истовремено са овом стратегијом, Европска комисија је исте године упутила предлог Директиве о мерама за

[5] Ibidem, чл. 3.

[6] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, European Commission, JOIN(2013) 1 final, Brussels, 7.2.2013, pp. 4-5.

обезбеђење високог нивоа безбедности мрежа и информатичких система на територији Уније.[7] После доношења поменутих докумената, Комисија је појачала своју активност тиме што је информатичку безбедност ставила у сам врх својих приоритета. Тако је донесена Стратегија јединственог дигиталног тржишта 6. маја 2015. године која се заснива на следећа три стуба: (1) *боља расположивост* за потрошаче и правна лица дигиталним стварима и услугама на територији Европе;[8] (2) *окружење* које карактеришу повољни и равноправни услови за ширење дигиталне мреже и иновативних услуга;[9] и (3) максимално коришћење дигиталне економије за раст *економије и развој друштва*.[10] Комисија је наставила са активностима према претходно утврђеним плановима, те је као један од циљева Европске агенде о безбедности за период 2015–2020, која је усвојена 28. априла 2015. године, поставила борбу против тероризма, организованог криминала и информатичког криминала.[11] Овај документ утврђује конкретна средства и мере које ће се користити у заједничком деловању на обезбеђивању безбедности и најефикаснијем решавању ове три, како их ова агенда третира, највеће претње по Европу у наведеном периоду.[12]

---

[7] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, European Commission, Brussels, 7.2.2013, COM(2013) 48 final, 2013/0027 (COD).

[8] *A Digital Single Market Strategy for Europe*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 6.5.2015 COM(2015) 192 final, para. 2.

[9] Ibidem, para. 3

[10] Ibidem, para. 4.

[11] *The European Agenda on Security*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strasbourg, 28.4.2015 COM(2015) 185 final.

[12] Треба имати у виду да је у области борбе против информатичког криминала Европска скупштина донела неколико директива које доприносе остваривању постављених циљева из Европске агенде о безбедности. То су: (1) Директива о нападима на информатичке системе којом се ван снаге ставља Оквирна одлука Савета 2005/222/ЈХА (Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, *Official Journal of the European Union*, L 218, 14.8.2013, pp. 8-14) која је наложила државама чланицама да пооштре националне прописе и уведу строже казне за информатички криминал; (2) Директива о борби против сексуалног искоришћавања деце преко интернета и дечје порнографије (Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *Official Journal of the European Union*, L 335, 17.12.2011, pp. 1-14, и (3) Оквирна одлука Савета о борби против превара и фалсификовања новчаних безготовинских плаћања (Council

Ради спровођења зацртаних циљева из горе поменутих докумената, Европска комисија је 5. јула 2016. године потписала први уговор о јавно-приватном партнерству са индустријом о информатичкој безбедности, који би до 2020. године требало да допринесе инвестицијама у износу од 1,8 милијарди евра ради унапређења опреме Европе за заштиту од информатичких напада и повећању конкурентности сектора информатичке безбедности.[13] Усвајање Директиве о мерама за остваривање високог заједничког нивоа безбедности мрежа и информатичких система на територији Уније,[14] 6. јула 2016. године, представља још један важан корак ка безбеднијем информатичком окружењу. Поводом доношења Директиве о безбедности мрежа и информатичких система Андрус Ансип, потпредседник Европске комисије надлежан за јединствено дигитално тржиште, поздрављајући изгласавање ове Директиве, истакао је да ако становништво и правна лица желе да имају што веће користи од дигиталних услуга они морају да верују у њих, док је Гинтер Етингер, комесар ЕУ, истакао да ће усвајање првог прописа на нивоу ЕУ о информатичкој безбедности подржати и обезбедити стратешку сарадњу и размену информација између држава чланица.[15]

3) САДРЖАЈ

Директива има двадесет седам чланова који су подељени у седам поглавља. Прво поглавље од шест чланова (чл. 1–6) посвећено је предмету регулисања и области примене. Овом Директивом утврђују се правила с циљем постизања високог заједничког степена безбедности мрежних и информатичких система ЕУ како би се побољшало функционисање унутрашњег тржишта ЕУ. У ту сврху, овом Директивом: (а) утврђује се обавеза свих држава чланица да донесу националну стратегију за безбедност мрежних и информатичких система; (б) ствара се тим за сарадњу ради подршке и олакшавања стратешке сарадње и размене информација између држава чланица и развијања међусобног поверења и поузданости; (ц) ствара се мрежа тимова за одговор на рачунарске

Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, (2001/413/ЈНА), *Official Journal of the European Communities*, L 149, 2.6.2001, pp. 1-4), која дефинише преварна понашања која државе чланице ЕУ треба да пропишу као кривична дела.

[13] "Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats", European Commission – Press release, Brussels, 5 July 2016.

[14] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *Official Journal of the European Union*, 19.7.2016, L 194, p. 1-30.

[15] Statement by Vice-President Ansip and Commissioner Oettinger welcoming the adoption of the first EU-wide rules on cybersecurity, Statement/16/2424, Brussels, 6 July 2016.

безбедносне инциденте (даље у тексту: ТОРБИ) како би се допринело развоју поузданости и поверења међу државама чланицама и подстицала брза и ефикасна оперативна сарадња; (д) утврђују обавезе оператера кључних услуга и пружалаца дигиталних услуга[16] у вези са безбедношћу и обавештавањем; (е) утврђују се обавезе држава чланица да именују националне надлежне органе, јединствене тачке за контакт и ТОРБИ чији су задаци у вези са безбедношћу мрежних и информатичких система. Директивом се не доводе у питање прописи и мере које државе чланице доносе за заштиту својих основних државних функција, посебно за заштиту националне безбедности, укључујући и мере за заштиту информација за чије откривање државе чланице сматрају да би било супротно основним интересима њихове безбедности, те за одржавање закона и реда, посебно ради неометаног спровођења истрага, откривање и кажњавање кривичних дела. Обрада података о личности спроводи се у складу са релевантним прописима ЕУ за државе чланице и органе и институције ЕУ. Ради се о Директиви минималног усклађивања националних права држава чланица које су овлашћене да донесу или задрже прописе чији је циљ постизање вишег степена безбедности мрежних и информатичких система. У чл. 4 дају се дефиниције појмова који се користе у Директиви, од којих се осврћемо само на неке од њих. Тако, „безбедност мрежних и информатичких система" означава способност мрежних и информатичких система да одолевају, на одређеном нивоу поузданости, било којој радњи која угрожава доступност, аутентичност, целовитост или поверљивост смештених или пренесених или обрађених података или сродних услуга које ти мрежни и информатички системи нуде или којима омогућавају приступ. „Оператор кључне услуге" означава јавни или приватни субјект у појединим делатностима описаним у Анексу II Директиве који испуњава следеће критеријуме: (а) субјект пружа услугу која је важна за одржавање кључних друштвених и/или економских делатности; (б) пружање такве услуге зависи од мрежних и информатичких система; и (ц) инцидент би имао знатан негативан учинак на пружање те услуге. При утврђивању важности негативног учинка државе чланице узимају у обзир минимално следеће међусекторске елементе: (а) број корисника који користе услуге које тај субјект пружа; (б) зависност других сектора из Анекса II о услугама које тај субјект пружа; (ц) могући утицај инцидената, у погледу њихове тежине и трајања, на привредне и друштвене активности и на јавну безбедност; (д) тржишни удео тог субјекта; (е) територијалну распрострањеност могућег утицаја инцидента; (ф) важност субјекта за одржавање довољног нивоа услуге, узимајући у обзир расположивост алтернативних средстава за пружање те услуге. Како би се утврдило да ли би инцидент имао знатан негативан учинак државе чланице,

[16] У смислу Анекса III ове Директиве дигиталне услуге су: 1. Интернет тржиште, 2. Интернет претраживач, и 3. Информатичке услуге у облаку.

према потреби, у обзир узимају и околности специфичне за поједини сектор. Друго поглавље садржи четири члана (чл. 7–10) који су посвећени националним оквирима за безбедност мрежних и информатичких система. У чл. 7 прописано је да свака држава чланица доноси националну стратегију за безбедност мрежних и информатичких система којом се одређују стратешки циљеви, адекватна политика и надзорне мере с циљем постизања и одржавања високог степена безбедности мрежних и информатичких система и одређују питања којима она треба да се бави. У чл. 8 Директива прописује обавезу држава чланица да именују једно или више националних органа који ће бити надлежни за безбедност мрежних и информатичких система који ће покривати секторе и услуге из Анекса II и III Директиве. Поменути органи надгледају примену ове Директиве на националном нивоу. Јединствена тачка контакта извршава функцију повезивања с циљем остваривања прекограничне сарадње органа државе чланице с релевантним органима у другим државама чланицама, са тимом за сарадњу и мрежом ТОРБИ. Државе чланице такође имају обавезу да обезбеде одговарајуће ресурсе за надлежне органе и јединствене тачке контакта ради делотворног извршавања својих задатака тако да могу да испуњавају циљеве ове Директиве. У чл. 9 обавезују се државе чланице да именују један или више ТОРБИ који су надлежни за решавање ризика и инцидената у складу с тачно прописаним поступком. Државе чланице именованим су дужне да тим тимовима обезбеде одговарајуће ресурсе за ефикасно извршавање задатака дефинисаних у Анексу I Директиве (1. праћење инцидената на националном нивоу; 2. пружање раних упозорења и најава, као и информисање релевантних лица о ризицима и инцидентима; 3. одговарање на инциденте; 4. пружање динамичке анализе ризика и инцидената и прегледа ситуације; 5. учествовање у мрежи тимова). Државе чланице су дужне да обезбеде да наведени тимови имају приступ прикладној, сигурној и отпорној инфраструктури за комуникацију и информисање на националном нивоу. Ако су одвојени надлежни орган, јединствена тачка контакта и ТОРБИ исте државе чланице међусобно сарађују у погледу испуњавања обавеза прописаних овом Директивом. Трећим поглављем са три члана (чл. 11–13) регулисана је сарадња у погледу питања мрежне и информатичке безбедности. Тим за сарадњу формиран је ради подстицања и олакшавања стратешке сарадње и размене информација између држава чланица, развијања поверења и поуздања с циљем постизања високог заједничког степена безбедности мрежних и информатичких система у ЕУ, док на националном нивоу ТОРБИ спроводе брзу и ефикасну сарадњу са надлежним органима других држава чланица и ЕУ. У четвртом поглављу са два члана (чл. 14 и 15) регулише се безбедност мрежних и информатичких система оператора кључних услуга. Тако су државе чланице обавезне да обезбеде да оператори кључних услуга предузимају одговарајуће и сразмерне техничке и организационе мере за управљање ризицима којима су изложени мрежни и

информатички системи којима се служе у свом пословању и да, узимајући у обзир најновија достигнућа, тим мерама обезбеђују ниво безбедности мрежних и информатичких система примереним ризику којем су изложене. Државе чланице су у обавези да овласте надлежни орган и обезбеде му средства да од оператора кључних улога затражи доставу: (а) информација потребних за процену безбедности њихових мрежних и информатичких система, поред осталог, документоване процедуре безбедности; (б) доказа о ефикасном спровођењу безбедносних процедура, примера ради, резултата ревизије безбедности коју је обавио надлежни орган или квалификовани ревизор, као и да у случају да је обавља квалификовани ревизор надлежном органу достави те резултате заједно с доказима на којима се они заснивају. Приликом тражења таквих информација или доказа надлежни орган је дужан да наведе сврху захтева и одређује које су му информације потребне (чл. 15, ст. 2). Пето поглавље са три члана (чл. 16–18) регулише питања безбедности мрежних и информатичких система пружалаца дигиталних услуга. Тако су државе чланице дужне да обезбеде да пружаоци дигиталних услуга предузимају одговарајуће и сразмерне техничке и организационе мере за управљање ризицима којима су изложени мрежни и информатички системи којима се у ЕУ служе у оквиру пружања услуга. Узимајући у обзир најновија достигнућа, тим мерама се мора обезбедити степен безбедности мрежних и информатичких система примерен ризику којем су изложени и узимајући у обзир следеће елементе: (а) сигурност система и објеката; (б) решавање инцидената; (ц) управљање континуитетом пословања; (д) праћење, ревизија и тестирање; (е) усклађеност с међународним стандардима. За потребе примене ове Директиве сматра се да пружалац дигиталних услуга припада надлежности државе чланице у којој има пребивалиште, односно седиште. Пружалац дигиталних услуга који нема пребивалиште или седиште у ЕУ, али нуди услуге на њеној територији, дужан је да именује свог представника у ЕУ. Представник мора да има седиште у једној од држава чланица у којима пружалац продаје своје услуге. Сматра се да пружалац дигиталних услуга припада надлежности оне државе чланице у којој његов представник има пребивалиште. У шестом поглављу које има два члана (19–20) обавезују се државе чланице да с циљем подстицања конвергентног спровођења одредби о захтевима које оператори кључних услуга и пружаоци кључних услуга морају да испуне, да не намећу или дискриминишу одређене врсте технологија и да подстичу примену европских или међународно признатих норми и спецификација релевантних за сигурност мрежних и информатичких система. У том смислу Директива посебну улогу даје Агенцији ЕУ за мреже и информатичке системе да у сарадњи с државама чланицама израђује савете и смернице у погледу техничких области чије регулисање треба размотрити у односу на постојеће прописе. Субјекти који немају својство оператора кључних услуга или пружалаца дигиталних услуга могу на добровољној основи да

упућују обавештења о инцидентима који имају знатан учинак на континуитет услуга које та лица пружају. На крају овог дела истичемо да је Европски економски и социјални комитет поздравио доношење ове Директиве, али да је у свом Мишљењу о предлогу њеног текста био прилично критичан. Према његовој општој оцени, ова Директива је превише неодређена, недостаје јој довољно јасноће и њена примена зависи од прописа које буду донеле државе чланице.[17] Неодређеност се првенствено односи на непостојање јасних правила о томе како примењивати дефиниције из чл. 3, као и непостојање дефиниције инцидента који има „знатан учинак" што омогућава државама чланицама превише самосталног одлучивања о томе да ли ће неки инцидент пријавити.[18]

4) ДАТУМ СТУПАЊА НА СНАГУ И АНАЛИЗА ЊЕНЕ ПРИМЕНЕ

Европска скупштина усвојила је Директиву о безбедности мрежа и информационих система 6. јула 2016. године, која је ступила на снагу двадесетог дана после објављивања у Службеном листу Европске уније. Државе чланице су дужне да до 9. маја 2018. донесу и објаве законе и друге прописе који су потребни за усклађивање с овом Директивом. Оне су дужне да о томе одмах обавесте Комисију и да те прописе почну да примењују од 10. маја 2018. године. Када државе чланице донесу поменуте прописе, они морају да садрже позивање на ову Директиву или да на њу упућују приликом њихове објаве у националном службеном листу. Начине тог упућивања одређују државе чланице. Државе чланице Комисији достављају текст главних одредаба националног права које донесу у области на које се односи ова Директива. Европска комисија има обавезу да Европској скупштини и Савету до 9. маја 2019. године поднесе извештај са проценом доследности у приступу држава чланица при идентификацији оператора кључних услуга. Комисија има обавезу да периодично анализира функционисање те Директиве и Европској скупштини и Савету о томе подноси извештај. У ту сврху, као и с циљем даљег унапређивања стратешке и оперативне сарадње, Комисија ће узимати у обзир извештаје тима за сарадњу и мреже тимова за реаговање на безбедносне рачунарске инциденте о искуству стеченом на стратешким и оперативним нивоима. Први извештај Комисија је дужна да достави до 9. маја 2021. године.

[17] Opinion of the European Economic and Social Committee on the 'Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union', *COM(2013) 48 final – 2013/0027 (COD)*, *Official Journal of the European Union*, (2013/C 271/25), 19.9.2013, p. 133-137, чл. 4.1.

[18] Ibidem, чл. 4.6.

5) ИЗВОРИ

A Digital Single Market Strategy for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 6.5.2015 COM(2015) 192 final.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *Official Journal of the European Union*, 19.7.2016, L 194.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, *Official Journal of the European Union*, L 218, 14.8.2013.

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *Official Journal of the European Union*, L 335, 17.12.2011.

Juncker, Jean-Claude (15 July 2014). "Political Guidelines for the next European Commission – A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change", Opening Statement in the European Parliament Plenary Session, Strasbourg.

Opinion of the European Economic and Social Committee on the 'Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union', COM(2013) 48 final – 2013/0027 (COD), *Official Journal of the European Union*, 2013/C 271/25, 19.9.2013, pp. 133-137.

Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, European Commission, Brussels, 7.2.2013, COM(2013) 48 final, 2013/0027 (COD).

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, *Official Journal of the European Union*, L 77, 13.3.2004, pp. 1-11.

Statement by Vice-President Ansip and Commissioner Oettinger welcoming the adoption of the first EU-wide rules on cybersecurity, Statement/16/2424, Brussels, 6 July 2016.

The European Agenda on Security, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strasbourg, 28.4.2015 COM(2015) 185 final.

"Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats", European Commission – Press release, Brussels, 5 July 2016.

Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, (2001/413/JHA), *Official Journal of the European Communities*, L 149, 2.6.2001, pp. 1-4.

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, European Commission, JOIN(2013) 1 final, Brussels, 7.2.2013.

6) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Штета или прекид рада мреже и информатичких система могу да угрозе обављање активности приватног и јавног сектора у области управних процедура, трговине, саобраћаја и комуникација, наруши поверење корисника, проузрокује веће финансијске губитке и штету. С обзиром и на све учесталије вршење кривичних дела коришћењем Интернета и електронских комуникационих средстава било је неопходно да се на нивоу Европске уније установе минимални стандарди за безбедност мрежа и информатичких система и оквири сарадње на спречавању информатичких инцидената. Како извршилац неког дела против безбедности мрежа и информатичких система, као и дела тероризма, прања новца, дечје порнографије итд., може да се налази у једној држави а да штетне последице произведе на мрежи и рачунарским системима у другој држави на истом или другом континенту, поменути ризици имају глобалну природу и захтевају удружено деловање надлежних органа већег броја држава. Због тога законодавац Републике Србије треба да прати законодавне промене у праву Европске уније и да их правовремено спроводи у складу са, из овде разматране Директиве, обавезом примењивања најновијих општеприхваћених стандарда о безбедности мрежа и информатичких система. Република Србија, њени грађани и привреда треба да у највећој могућој мери искористе предности дигиталне привреде која може да допринесе ширењу тржишта, квалитетнијем пружању услуга по бољим ценама, већем избору и новим изворима запошљавања. Услед неодређености неких дефиниција и делова Директиве, за очекивати је да ће државе чланице у својим прописима детаљније регулисати све или неке од недостајућих елемената неопходних за установљавање јасних овлашћења и начина поступања. А то ће, као и у случају минималног усклађивања права држава чланица у другим областима, довести до разлика у националним прописима.

NETWORK SECURITY AND INFORMATION SYSTEMS IN THE LAW OF THE EUROPEAN UNION

Abstract: Digital technologies provide great opportunities in the area of administrative procedures, economic activities and the needs of society, where new types of products and services of informatics which do not recognize the borders of national states appear on a daily basis. On the other hand, the number of security incidents related to digital technology is increasing, and their frequency is a serious threat to the functioning of the network and information systems. The subject of the analysis is the legal acts of the European Union related to the regulation of the security of the network and information systems.

Key words: Security, networks, technologies, digital services, information systems, strategy, risks.