УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ БЕЗБЕДНОСТИ

ЗАШТИТА КРИТИЧНИХ ИНФОРМАЦИОНО – КОМУНИКАЦИОНИХ ИНФРАСТРУКТУРА

– ЗАВРШНИ (СПЕЦИЈАЛИСТИЧКИ) РАД –

Ментор:
Проф. др Ненад Путник

Студент:
Александар Крсмановић
С36/21

Београд, 2022. година

САДРЖАЈ

1. Увод

Савремену друштвено-политичку ситуацију карактерише вишеструка криза. Последице здравствене COVID-19 кризе, мера изолације и прекида трговине капитала и услуга за време ванредног стања изражене су у виду економске кризе, што уз актуелну енергетску, еколошку кризу, рат у Украјини и миграције производи појачане тензије и даје повод за различите сукобе. У постојећим кризним условима безбедност информационих и комуникационих технологија (ИКТ) још више добија на важности, с обзиром да се актуелне тензије и сукоби могу лако ,,преселити" у сајбер простор (Лукнар, 2022).

Критичне инфраструктуре су физички или виртуелни системи и средства кључни за нормално функционисање државе. У околностима евентуалног делимичног или потпуног отказивања ових инфраструктура долази до угрожавања друштва, државе и националне безбедности (Мићовић, 2020). Због тога многе државе настоје да успоставе и развију мере заштите критичне инфраструктуре, које укључују идентификовање, израду мапа, размену информација, оспособљавање запослених у системима критичне инфраструктуре и увежбавање примене мера заштите или опоравка у случају потребе (Шкеро и Атељевић, 2015).

Брзи развој и унапређење информационих технологија стварају ново безбедносно окружење. Развој и примена информационих технологија је у пуној експанзији те се у данашње време рад бројних критичних инфраструктура заснива на информационо-комуникационим системима. У традиционалном приступу безбедности војне претње представљају највеће опасности по друштва и државе, док у савременом приступу безбедносни изазови и ризици леже у информатичкој сфери (Мићовић, 2020).

2. Дефинисање основних појмова

Појам кризе у модерно доба постао је синоним за појмове као што су побуна, конфликт или револуција. Током раног периода хладног рата, појам критичности је укључен у стратегију цивилне одбране Сједињених Америчких Држава, где је коришћен у сврху процене виталних делова државе, односно важне техничке инфраструктуре. То је почетак интензивније употребе предметног појма ради означавања и идентификације организација и институција које су на неки начин важне, релевантне или неопходне за континуитет снабдевања становништва и привреде добрима и услугама (Милосављевић и Вучинић, 2021).

„Појам ,'инфраструктура' потиче од латинских речи 'infra' (значење: под, испод, ниже) и 'struere' (значење: слагати, склапати) и представља темељ, подлогу; основу за привредни и друштвени развој коју чине: саобраћајна мрежа, водоводне инсталације, извори електричне и друге енергије, објекти намењени јавним потребама (осветљење, паркови, тргови, домови здравља, болнице, диспанзери, школе итд.)“ (Мићновић, 2020, стр.6).

2.1. Дефиниција појма критичне инфраструктуре

Данас је у оптицају више дефиниција критичне инфраструктуре и углавном се све односе на средства и имовину која је кључна за неометано функционисање економије и друштва:

У САД, критична инфраструктура се односи на „широк опсег различитих средстава и имовине који су неопходни за свакодневно функционисање друштвених, економских, политичких и културних система“ (Трбојевић, 2018, стр.102);

У Европској унији (ЕУ), критична инфраструктура представља „имовину, систем или његов део који се налази на територији земље чланице и који је неопходан за

одржавање кључних друштвених функција, здравства, безбедности, сигурности, економског или социјалног благостања, а чије би ометање или уништење имало значајан утицај на земљу чланицу“, односно у случају Европске критичне инфраструктуре на бар две земље чланице Европске уније (Шкеро и Атељевић, 2015, стр.193);

У Аустралији, критична инфраструктура представља „оне физичке објекте, ланце снабдевања, информационе технологије и комуникационе мреже, које би ако се униште или на дуже време онеспособе, могле да значајно утичу на друштвено или економско благостање нације, или на способност државе да одржи националну одбрану и обезбеди националну сигурност“ (Шкеро и Атељевић, 2015, стр.193).

Имајући у виду дефиниције појма критичне инфраструктуре, може се закључити да не постоји широко прихваћена дефиниција критичне инфраструктуре и да је то посебно питање сваке државе, односно да свака држава или организација мора да дефинише сопствену критичну инфраструктуру. Нејединство у дефинисању појма критичне инфраструктуре, последица је различитог посматрања безбедносних претњи и ризика, те разлика у географским, историјским и социополитичким факторима (Трбојевић, 2018).

Осим дефиниције, ни редослед приоритета у осигурању критичне инфраструктуре није јединствен. Високо развијене земље Европе и Северне Америке приоритет дају информационим системима и системима снабдевања енергијом, док су оне земље које се у свакодневном животу више сусрећу са егзистенцијалним питањима снабдевања храном и водом склоније да дају предност том сегменту (Јаковљевић, 2010).

3. Критична инфраструктура

Критична инфраструктура дуго је била непосредно повезана са потребама одбране државе ради означавања свега што је неопходно за функционисање војног система током војних сукоба, када су ресурси усмеравани на чување сопствених објеката, система и мрежа, али и њихово онеспособљавање на противничкој страни. Међутим, у савремено доба критична инфраструктура добија знатно шире одређење и значај за функционисање државе и друштва у целини. Појам критичне инфраструктуре обухвата објекте као што су зграде, путеви и транспортни, телекомуникациони, водоводни и енергетски системи, хитне службе, банкарске и финансијске институције и извори снабдевања, као и виртуелни (сајбер) простор. Уопштено, критичну инфраструктуру чине различити системи који су неопходни за несметано функционисање власти и друштва (Милосављевић и Вучинић, 2021).

Критичну инфраструктуру, и поред изражене сложености, можемо дефинисати набрајањем свих виталних инфраструктура, као у случају Америчке стратегије заштите критичне инфраструктуре из 2003. године, која представља један од првих докумената ове врсте. Други начин дефинисања, из научног угла посебно интересантан, заснива се на утврђивању специфичности карактеристика система и њихових односа релације у односу на друге системе или целине, као што је то случај са немачком националном стратегијом за заштиту критичне инфраструктуре, која одређује критичност као последицу поремећаја или неуспеха функције у вези са испоруком добара и услуга друштву. У овом случају утврђују се одређена релациона својства система, јер је дати систем критичан у односу на други систем, односно први је неопходан да би се наставило са радом другог система (Мићновић, 2020).

3.1.Заштита критичних инфраструктура

Променом међународних односа и порастом безбедносних изазова, ризика и претњи питање заштите критичних инфраструктура постало је једно од најзначајнијих безбедносних изазова. Термин заштита критичне инфраструктуре почиње да се интензивније користи након терористичких напада у Сједињеним Америчким Државама 2001. године. Промене у перцепцији претњи по критичну инфраструктуру и растућа међузависност различитих инфраструктурних елемената условиле су повећање значаја концепта заштите критичне инфраструктуре. Опасностима од природних катастрофа, технолошких несрећа и међународног тероризма, придодате су и нове информатичке претње, а заштита критичне инфраструктуре постала је изузетно комплексан сегмент савремене националне безбедности. Критична инфраструктура заштићена је на националном нивоу одговарајућим нормативним, организационим и безбедносно-техничким мерама (Милосављевић и Вучинић, 2021). Заштита критичне инфраструктуре подразумева и планирање опоравка, па је ефикасан опоравак од инцидената валидан показатељ успешне политике заштите критичне инфраструктуре (Трбојевић, 2018).

3.2. Класификација критичне инфраструктуре

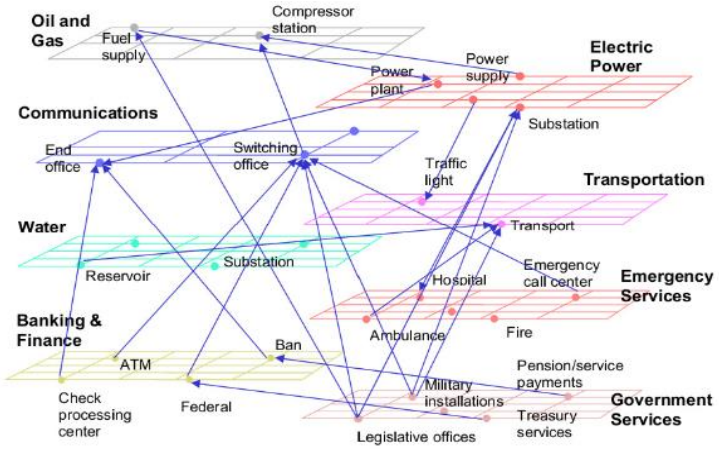
Критична инфраструктура може бити од интереса за: државе, регионе или свет, што значи да можемо говорити о националној, регионалној или светској критичној инфраструктури. С обзиром на време потребно за спровођење мера заштите, разликујемо: сталну, привремену или потенцијалну критичну инфраструктуру. Према критеријуму власништва, критична инфраструктура може бити у јавном, приватном или јавно-приватном поседу (Мићовић, 2020).

Велики број земаља настоји да идентификује и анализира критичне секторе, подсекторе, процесе и објекте коришћењем различитих методолошких приступа

како би формирали политике заштите критичне инфраструктуре, при чему највећи заједнички проблем представља изузетна комплексност инфраструктурних система. Велики је број инфраструктурних сектора који истовремено обухватају већи број подсектора, грана индустрије, служби, производних области и имају специфичну вертикалну структуру. Анализирајући различите приступе дефинисања и класификовања критичне инфраструктуре, може се закључити да она најчешће обухвата: храну, воду, пољопривреду, здравствене службе и службе хитне помоћи, енергију, саобраћај, информације и телекомуникације, банкарство и финансије, хемијска постројења, одбрамбену индустрију и поште и дистрибуцију роба (Мићовић, 2020).

3.3.Међузависности критичних инфраструктура

Велики значај критичних инфраструктура обавезује на стварање довољно добрих сигурносних мера које ће служити за умањење ризика од прекида рада. Критичне инфраструктуре су повезане на различитим нивоима и квар на елементу једне инфраструктуре може лако да се одрази на елементе друге и обратно, односно њихова међузависност је веома изражена (слика 1).



Слика 1. Међузависност критичних инфраструктура (Госпић, Мурић и Богојевић, 2012).

Како су информациони системи у великој мери међусобно повезани или повезани са јавним системима, чак и напади ниских размера на критичну ИКТ инфраструктуру представљају озбиљну претњу с обзиром да могу проузроковати штету на читавом низу међусобно повезаних инфраструктурних објеката.

Витални друштвени сектори су међусобно повезани и зависе једни од других, што доводи до стварања рањивости. Ометање функционисања једног сектора може да утиче и на друге секторе и обрнуто (међузависност). Врсте међузависности су:
− физичка (производ инфраструктуре неопходан је за функционисање друге),
− сајбер (стање једне инфраструктуре зависи од информација пренесених кроз информациону инфраструктуру),
− географска (одређени догађај ремети све физички блиске инфрастуктуре) и
− логичка (реципрочни ефекти јављају се на две или више инфраструктура без осталих међузависности, уз финансијске губитке). (Мићовић, 2020).

Међузависност критичних инфраструктура је од изузетне важности за конципирање мера заштите критичне инфраструктуре. Међузависност постоји између појединих мрежа, система, регија или држава. Критичне инфраструктуре су у све већој мери повезане са онима у другим државама, па је заштита могућа само заједничким деловањем, јер пропусти у једној држави могу довести до последица на ширем подручију (Јаковљевић, 2010).

Заштита критичних инфраструктура, међу којима посебно важно место заузима информационо-комуникациона инфраструктура, захтева конзистентно и кооперативно партнерство између јавног и приватног сектора – између власника и управљача инфраструктуре и влада држава. Данас је већина инфраструктурних сектора стекла транснационални карактер. После сектора информационих и комуникационих технологија који је одавно превазишао националне границе држава, такви су постали и сектори саобраћаја, хемијске, нуклеарне индустрије као и финансијски сектор. Међутим, у односу на остале секторе кртичне

инфраструктуре једне државе, информационо-комуникациони и електро-енергетски сектори се сматрају посебно осетљивим, будући да прожимају све остале секторе, те прекид у њиховом исправном функционисању доводи до дисфункционалности свих осталих инфраструктура. Изразита зависност система који омогућавају основне услуге од информационо-комуникационе инфраструктуре представља елемент ризика, с обзиром на то да информационо-комуникациона инфраструктура прожима све остале и намеће им сопствене рањивости, не само на националном већ и на регионалном и глобалном нивоу (Путник, Милошевић, и Цветковић, 2022).

Повећана међузависност критичних инфраструктура и већа операциона комплексност учиниле су критичне инфраструктуре посебно рањивим на природне катастрофе и природне хазарде, људске грешке и техничке проблеме, као и на нове облике сајбер криминала, тероризам и сајбер ратове. Сваки од ових догађаја може да доведе до озбиљних последица по критичну инфраструктуру. (Мићовић, 2020).

3.4. Критична телекомуникациона инфраструктура

Телекомуникационе мреже се сматрају неодвојивим делом друштвене интеракције. Комплетна електронска комуникациона инфраструктура која се састоји од комуникационих мрежа, дистрибуираних рачунарских система, софтвера и апликација игра кључну улогу у технолшком развоју и унапређењу укупног знања човека. Њеном могућношћу да окупи "критичну масу" људи, идеја и инвестиција, она на различите начине доприноси напретку на свим нивоима друштвеног и економског живота. Због тога, телекомуникациона инфраструктура представља веома важну имовину и средство које мора бити заштићено и које је неопходно препознати као део критичне инфраструктуре (Госпић, Мурић и Богојевић, 2012).

Телекомуникациона инфраструктура једне земље је комплексан скуп система који укључују велики број технологија и сервиса, а најчешће су у власништву више ентитета (држава, приватних компанија). Инфраструктура обухвата жичне, бежичне, кабловске и технологије за емитовање, језгрене мреже базиране на интернет протоколу као и интерне информационе системе. Многе телекомуникационе компаније (оператори) које управљају телекомуникационом инфраструктуром су током времена имплементирале мере заштите од природних катастрофа и незгода у оквиру својих инфраструктура уводећи редундантне чворове и системе, бизнис планове и стратегије за санацију након напада или природних непогода. Развојем технологија сектор телекомуникација и ИТ-а су постали практично нераздвојиви. Телекомуникациони сектор поред претходно наведених физичких елемената, укључује и сервисе као што су интернет саобраћај и рутирање, информационе сервисе и мреже кабловске телевизије. Самим тим, компоненте комуникационе инфраструктуре које су у власништву државе и приватних компанија су нераскидиво повезане у оквиру ових физичко-логичких структура. У дефинисању телекомуникационе инфраструктуре, уобичајено је да се за основу узима оно што је Међународна Унија за телекомуникације (ИТУ) дефинисала. Да бисмо дефинисали критичну телекомуникациону инфраструктуру, као основу можемо користили опште дефиниције критичне инфраструктуре. Она се може дефинисати као јавна или приватна мрежа која преноси информације релевантне за националну безбедност или информације велике материјалне вредности. У физичком смислу можемо је дефинисати као целокупну мрежу или део мреже преко које се преносе информације од велике важности (Госпић, Мурић и Богојевић,2012).

3.5.Управљање ризиком и јавно – приватно партнерство

Процес управљања ризиком представља једну од најважнијих активности у склопу управљања системима и организацијама. Свеобухватним управљањем ризиком можемо идентификовати системске хазарде и ризике на основу којих можемо сачинити одговарајуће планове, технике и мере намењене за елиминисање или минимализовање могућности њиховог настанка. У случају критичних инфраструктура, велики значај и рањивости које их карактеришу чине процес управљања ризиком јако сложеним процесом.

Оснивање јавно-приватног партнерства је неопходно како би јавни и приватни сектори постигли жељене бенефите, због тога што и јавни и приватни сектори поседују специфичности које уколико се комбинују унапређују оба сектора. Стварање јавно приватног партнерства у области критичне инфраструктуре захтева усклађивање менаџмента и надзорних структура и подструктура, укључујући и управљање безбедносним ризицима. У фази испитивања и уговарања могуће јавно–приватне сарадње спроводи се анализа могућих ризика од стране обе заинтересоване стране. По успостављеном партнерству анализа наставља да се развија и преиспитава од стране новооснованог менаџмент тима. Успостављање јавно-приватног партнерства може бити веома значајно за управљање ризиком, а посебно за фазу имплементације превентивниих мера и избора стратегија. У данашње време управљање ризиком није неопходно само због намере да се увећа продуктивност и профитабилност рада. Поред заштите пословних процеса циљ је и заштита запослених, спољних сарадника и животне средине. Методологија управљања ризиком и кризног менаџмента у критичној инфраструктури обухвата следећих 5 фаза:

1. **прелиминарно планирање**

Ова фаза ствара неопходне предуслове за успостављање система управљања ризиком који између осталог укључује: дефинисање позиције новог система

управљања ризиком у оквиру постојећег система инфраструктурног менаџмента; дефинисање улога, дужности и одговорности свих учесника у менаџменту и извршном организационом систему; дефинисање доступних ресурса и одређивање циљева система управљања ризиком и кризним менаџментом.

2. **Анализу ризика**

Као фаза започиње сегментацијом организације у процесе и подпроцесе. Што је већи број сегмената већи су напори и ресурси потребни за анализу, али добијене информације су детаљније и корисније.

3. **Специфицирање превентивних мера**

Сврха успостављања и спровођења превентивних мера и стратегија је смањење могућности остварења ризика и настанка кризе. Превентивне мере укључују:

1)Смањење ризика је примарни циљ менаџмента ризиком. Све активности које се спроводе при управљању ризиком, а које дефинишу хазарде и ризике и успостављају мере заштите, имају сврху неутрализовања идентификованих ризика или смањења вероватноће њиховог остварења и изазивања инцидената. Успостављањем јавно-приватног партенрства оснива се нови менаџмент тим који се састоји од експерата чији приоритет постаје минимизација ризика, што доприноси генералној стабилности у фунцкионисању критичних инфраструктура. Сваки приватни инвеститор има интерес да минимизује безбедносне ризике јер су инвестиције у превенцију финансијски знатно исплативије од инвестиција у опоравак од ефеката потенцијалних инцидената.

*2) Избегавање ризика***.** Како се не може постићи апсолутна безбедност тако је и веома тешко достићи апсолутну неутрализацију ризика, али он може бити смањен на минимум и околности које доводе до његове манифестације могу бити контролисане. Предузимање превентивних мера и контролисање интерних и екстерних фактора ризика и утицај на манифестацију ризика представљају основу избегавања ризика. Ово је сложен процес који захтева висок ниво свести о

опасностима и понашање које неће допринети факторима који утичу на остварење ризика. Овако сложен али неопходан процес је једноставније спровести у случају постојања јавно-приватног партнерства. Искуства приватног сектора уз асистеницију државе чине процес избегавања ризика ефикаснијим, кроз стручно праћење и управљање мерама избегавања ризика. Едукација и тренинг запослених у области безбедносних мера и метода избегавања ризика су свеобухватнији и могу се применити ефикасније у случају удруживања ресурса јавног и приватног сектора.

3)Трансфер ризика представља један од модела превентивне акције који подразумева пренос надлежности и задатака секцијама система или екстерним ентитетима који могу да управљају одређеним ризицима ефикасније у конкретним околностима. Анализа појединачног ризика представља процену вероватноће остварења ризика и последица које би исти могао да има, а саставни део ове процене је процес дефинисања угрожености или рањивости критичне инфраструктуре, препознавање постојећих безбедносних мера и могућност превазилажења недостатака и унапређења мера заштите. Трансфер ризика је стратегија која можда и најбоље осликава важност успостављања јавно приватног партнерства, јер њиме критична инфраструктура проширује свој систем новим организационим јединицама, објектима, радном снагом и материјалним ресурсима. У таквим околностима могућ је трансфер ризика са тачке у којој је остварење истог вероватније због недостатака превентивних мера и ресурса у друге подсистеме или организационе јединице које су у стању да контролишу и успешно управљају прихваћеним ризицима у датом тренутку.

4)Прихватање ризика је стратегија која се спроводи када су могућности свих претходно поменутих стратегија исцрпљне. Прихватање ризика је такође много једноставније у случају јавно-приватног партнерства, када управљање ризиком може да укључује различите ресурсе, искуства, и менаџмент тимове. Стратегија прихватања ризика може бити коначна стратегија или саставни део неке од

претходно поменутих стратегија. Успостављањем јавно-приватног партнерства обе стране показају жељу за прихватањем ризика. Држава у свом делу предаје делимично или потпуно управљање критичном инфраструктуром, ресурсима и системима виталним за функционисање друштва и институција , док привантни партнер улаже ресурсе, искуство и знање у те организације, које се често сусрећу са финанскијским губицима или не остварују очекиване приходе. У случајевима када ризик није преносив, када су предвиђене стратегије и мере избегавања или смањења ризика неефикасне ризик треба прихватити, што подразумева темељно и потпуно разумевање природе и карактера датог ризика, његовог извора, форме појављивања и изазивања штете.

4. увођење система управљања ризиком

Сврха увођења система управљања ризиком као и кризног менаџмента критичне инфраструктуре је одржавање највише могуће ефикасности система и опоравак критичних функција у најкраћем могућем року. План управљања ризиком као основ за успостављање и спровођење система управљања ризиком као и кризни менаџмент би требало да укључује и дефинише: сврху и циљеве плана, правни основ, организациону структуру управљања ризиком и кризног енаџмента, тим за кризни менаџмент и тим за одговор на кризу, дефинисање улога и одговорности чланова тима менаџмента, креирање специјалних процедура за управљање ризиком и кризни менаџмент, моделе кризне ескалације и де-ескалације, мере за опоравак и начине информисања.

5. Оцењивање

Као фаза укључује анализе и процене процеса дефинисања свих претходних фаза и њихове појединачне резултате као и коначни резултат целокупног процеса управљања ризиком. Сви планови и усвојене мере менаџмента су процењени на основу прикупљених података и резултата али и већ постојеће одлуке и активности су такође узете у обзир.

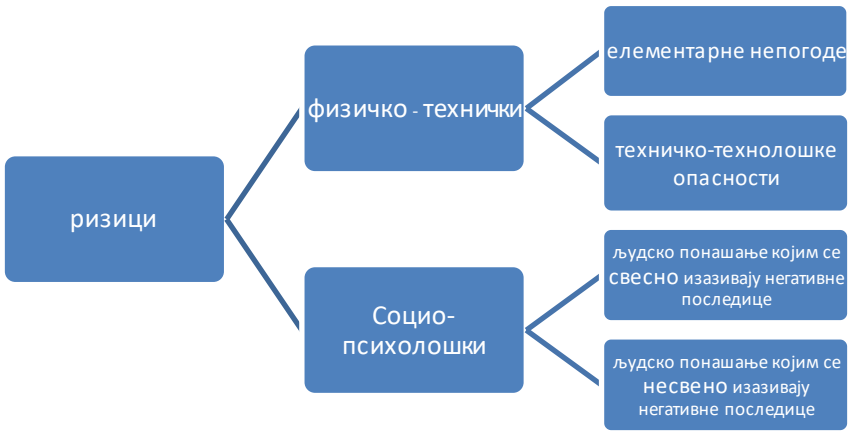
Сви претходно поменути инструменти и стратегије превенције ризика захтевају заједничку сарадњу управљачких структура у оквиру критичних инфрастурктура али и успостављање и одржавање сарадње са ентитетима изван система, пре свега са државним телима који имају заједничке интересе у стабилној и безбедној оперативности критичне инфраструктуре, како би несметано пружали сервисе и добра који су од велике важности за државу и друштво.

Омогућавање стабилног функционисања критичне инфраструктуре укључује примену све четири претходно описане стратегије, што чини само део комплетне методологије управљања ризиком. Тај задатак захтева посвећени експертски тим, континуирани рад, менаџмент људским ресурсима и припрему различитих интерних докумената који су у складу са нормативним актима државе у којој је јавно-приватно партнерство закључено. Оснивање јавно-приватног партнерства резултује у далеко више свеобухватних организационих активности у области превенције и одговора на ризике као и много веће могућности за њихово смањење, трансвер или прихватање. (Бошковић, Ивковић и Путник, 2013).

4. Начини угрожавања критичне ИКТ инфраструктуре

Инциденти, незгоде или намерно ометање нормалног функционисања инфраструктура могу да оставе озбиљне последице по економију и друштво односно да се одразе на велики број људских делатности. Критична инфраструктура мора бити добро заштићена из бројних разлога у које спадају: природне катастрофе, терористички напади, саботаже, али и информационо ратовање, у којем појединци или читаве државе могу из различитих разлога да нападају информационе системе других земаља и доведу до великих проблема, не само у функционисању информационе инфраструктуре, већ и других сектора, с обзиром на то да се многи ослањају на информационе системе. (Мићовић, 2020).

Извори угрожавања објеката критичне инфраструктуре могу се класификовати на више начина. Једна од најпрактичнијих класификација је категоризација заснована на подели безбедносних ризика на две основне групе - физичко-техничке и социо-психолошке, што је приказано на шематском приказу бр. 1. Група физичко-техничких ризика обухвата подгрупе елементарне непогоде и техничко-технолошке опасности, док група социо-психолошких ризика обухвата подгрупе људско понашање којим се несвесно изазивају негативне последице и људско понашање којим се свесно изазивају негативне последице (Ракић, 2015).



Шематски приказ бр.1 - подела ризика 1 (Ракић, 2015)

Безбедност у сајбер простору постала је тема од глобалног значаја техничко-технолошким напретком који је условио повећање зависности савременог човека од функционисања информационих технологија. Безбедносни ризици у сајбер свету су веома разнолики и крећу се од вршења кривичних дела на штету појединаца и правних лица преко или уз помоћ рачунарских система и мрежа до сајбер операција којима се угрожава безбедност држава и међународних организација кроз спровођење аката тероризма (Милошевић и Путник, 2017).

4.1. Сајбер тероризам

Поред појединаца, и основне државне структуре и индустрије све више своје функционисање ослањају на савремене информационе и комуникационе технологије, што доприноси расту глобалних претњи од различитих врсти сајбер малверзација и злоупотреба. Тиме сајбер безбедност постаје питање од прворазредног значаја. **Сајбер тероризам** представља значајну претњу којој треба посветити посебну пажњу. Он подразумева употребу компјутерских мрежа и интернет алата за ометање критичних националних инфраструктура или застрашивање влада једне земље и њених грађана (Лукнар, 2022). Сајбер простор представља идеално поље за прикривене организације пре свега због гаранције анонимности али и брзе размене информација и могућности достизања ширег медијског ефекта, што све светске терористичке организације користе у своју корист. Поред тога што сајбер простор злоупотребљавају као медиј ради ширења пропаганде и вођења психолошког рата, мобилисања нових чланова и њихове обуке, финансирања организације, комуникације и обавештајних активности, терористи сајбер простор користе за извођење техничких напада на критичне инфраструктуре непријатеља. Многе државе у данашње време у великој мери зависе од осетљивих рачунарских и телекомуникационих система, који су због тога могући терористички циљеви. Прикупљање почетних информација претходи било којој врсти терористичког напада, па напад чији је циљ сакупљање

одређених информација мора да предходи сајбер терористичком нападу. Методе социјалног инжењеринга су се у прошлости показале као јако ефикасне у ту сврху, па у данашње време представљају саставни део добро организованог напада. Сајбер терористички напад може да се изведе једноставним средствима и малобројним људством, а да притом нанесе екстремне последице држави, њеној привреди и становништву уколико успе да угрози неку њену критичну информациону инфраструктуру. (Мандић, Путник и Милошевић, 2017).

4.2. Сајбер ратовање

Настанак сајбер простора пружио је велике могућности за спровођење специјалних пропагандних дејстава али и извођење напада посредством рачунарских мрежа на противничке информационо-комуникационе системе. За такве сукобе данас користимо појам **сајбер ратовање**. (Путник, Милошевић и Бошковић, 2017).

Промене у начину вођења савремених ратова настале су већим делом као последица употребе нових технологија у војне сврхе. Неопходно је посветити посебну пажњу улози информационо-комуникационих технологија у савременом ратовању, које посебно утичу на исход конфликта. **Виртуелни (сајбер) простор** стекао је статус петог борбеног простора, поред копна, ваздуха, воде и космоса, и у будућим сукобима може постати место примарних борби. Сајбер простор је погодан амбијент за спровођење пропагандних активности, али и извођење напада поосредством рачунарских мрежа на противничке информационо-комуникационе системе који могу резултовати чак и нарушавањем суверенитета једне земље. Због тога је сајбер простор постао не само мета напада већ и моћно средство у арсеналу технолошких развијених армија (Путник,2022).

Сајбер ратовање представља спровођење напада на противничку информациону инфраструктуру употребом малвера и других сајбер алата и техника, као и спровођење пропагандних активности са циљем наношења штете противнку и слабљења његових одбрамбених капацитета у сајбер и физичком свету. Сајбер ратовање примењује специјалне информационе операције које обухватају широк спектар техника и инструмената за извршење напада на противничке ИКТ системе и манипулацију информацијама у офанзивне и дефанзивне сврхе. Његова главна обележја су да се одвија у сајбер простору (кога чине рачунари и рачунарске мреже) посредством софтверских алата, пропагандних и различитих техника за обмањивање противничких корисника информационо-комуникационих технологија са циљем наношења штете противнику, његовој критичној информационој инфраструктури, са њом умреженим критичним инфрастурктурама као и у њима садржаним подацима. Када је мета критична инфраструктура противника, сајбер ратовање може резултовати и конкретним материјалним и људским губицима, иако се одвија у виртуелном свету (Путник,2022).

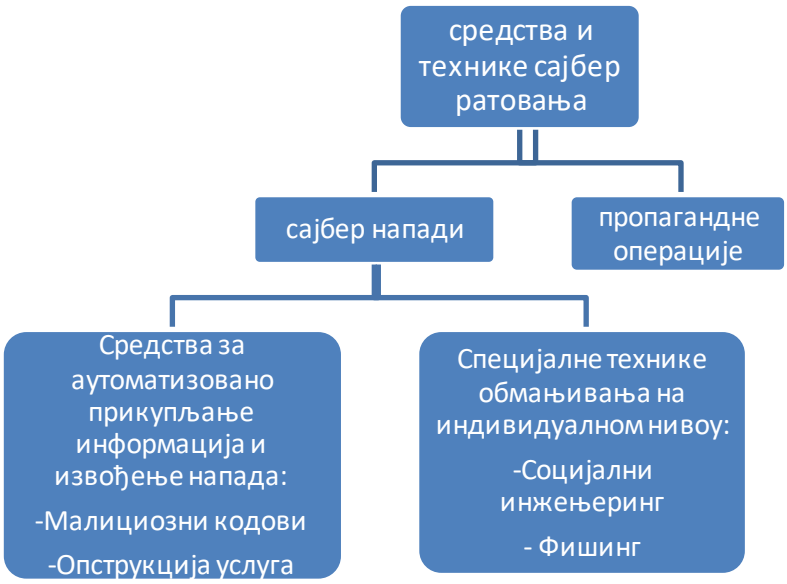
Сајбер ратовање може утицати и на доносиоце одлука у физичком свету, постићи да непријатељ прими информацију која га води лошој одлуци, обманути га у вези информација од значаја за стратегију и тактику, а у циљу доношења лоших процена при одлучивању. У сајбер свету физичка ограничења у односу на раздаљину и простор нису применљива, што доприноси претњи коју сајбер ратовање изазива (Путник, Милошевић и Бошковић, 2017).

Рачунарским нападима на системе аутоматизованог даљинског управљања и контроле индустријских процеса (ДЦС и СЦАДА системе) који су део критичне инфраструктуре претња сајбер ратом постала је стварна. Ови системи повезују реални и виртуелни свет, па би добро испланирани напад на њих могао да има озбиљне последице по безбедност државе и њених грађана, а уколико је мета

напада посебно осетљива критична инфраструктура попут нуклеарне електране, последице би могле бити регионалног или глобалног карактера. Одређени фактори допринели су повећању ризика по ове системе у које спадају усвајање стандардних и распрострањених технологија чије су рањивости широко познате, повезивање система на шире мреже које нису контролисане од стране управљача инфраструктуром, недовољна заштита удаљених терминалских јединица и широка јавна доступност осетљивих техничких информација о овим системима. Иако су до сада овакви напади успешно одбијани, пораст повезаности критичних инфраструктура унутар интернета и појава нових и ефикаснијих сајбер оружија доводе до повећања ризика од сукоба у којима би мета била критична инфраструктура противника (Путник,2022).

Напади на информационе системе представљају директне акције против мрежа или информационих система са циљем компромитовања поверљивости, интегритета и расположивости информација у систему. **Инструменти сајбер напада (сајбер оружје)** обухватају злонамерне информатичке програме чија је функција да заразе информациони систем противника ради стварања штете или крађе поверљивих и осетљивих информација, а постоје и напади који искоришћавају протоколе које користе системи и њихове рањивости и на тај начин успевају да приступе информационом систему. Приступ је често остварив и техникама социјалног инжењеринга, при чему су корисници система несвесно наведени да открију поверљиве информације нападачу. Сајбер оружије је ефикасно због његове доступности и економске приступачности као и ефекта на технолошки развијена друштва која се заснивају на исправном функционисању критичних информационих инфраструктура. У методе и средства сајбер ратовања, поред различитих сајбер напада сврставамо и покушаје злоупотребе сајбер простора као средства за масовну комуникацију, што укључује пласирање дезинформација и субверзивно–пропагандну активност (планска активност која има за циљ придобијање јавног мњења за одређену политику и циљеве).

Средства и технике сајбер ратовања (шема 2) можемо поделити на сајбер нападе и пропагандне операције, а сајбер нападе даље на средства за аутоматизовано прикупљање операција и извођење напада (малициозни програми и дистрибуирани напади усмерени на опструкције услуга) и специјалне технике обмањивања на индивидуалном нивоу (социјални инжењеринг и фишинг).



Шематски приказ бр.2 – средства и технике сајбер ратовања (Путник, 2022)

Безбедност савременог друштва постаје све комплекснија, због његове зависности од нових технологија, а безбедносне претње у сајбер свету су асиметричне. Могућност за извршење деструктивних акција све је приступачнија. Сајбер оружје могу развијати појединци или групе за шта су им потребни само знање и мотивација. Војна надмоћ не гарантује безбедност сајбер простора, већ је неопходно развијати нове стратегије одбране критичне информационе инфраструктуре. Околности отежава и природа сајбер простора у коме је лако сачувати анонимност нападача и у коме је мета доступна ма колико физички удаљено се налазила. Субјекти прећи у сајбер простору могу бити бројни: хакери, крекери хактивисти, инсајдери, криминалне групе, терористи, привредне

корпорације, националне армије и безбедносне службе, и притом сви субјекти имају своје специфичности у погледу мотивације, циљева и алата које користе.

Висок степен зависности великих сила од комуникационих линкова и информационих операција чини ово подручије погодном метом за потенцијалне нападе. Поред напада са циљем саботаже противничке информационо-комуникационе технологије који представљају реалну претњу за кључне комуникационе системе, сателити би могли представљати једну од првих мета у рату за стицање надмоћи, услед развоја наоружања које зависи од сателитских комуникација. Сателити представљају најбољи пример вишенаменских напредних ИКТ система који се могу користити и у војним акцијама. Свемирска материјална имовина истовремено је и нематеријална (информациона) јер сакупља, обрађује и преноси информације па чини ратовање у космосу и информационо ратовање повезанима (Путник,2022).

У савременим сукобима **информација** представља стратешки ресурс јер је победник углавном она страна која може брже да прикупља, експлоатише и манипулише информацијима. Информације, као и инфраструктура којом се преносе, постају све важније за националну безбедност, што посебно долази до изражаја у оружаним сукобима. Информација је постала стратегијски ресурс модерног доба. Овладавање информацијама, успостављање контроле над њима и могућност да се креира и јавном мњењу представи властита представа стварности промовисали су информацију у основни објект сајбер ратовања, а сајбер ратовање у примарни вид сукоба. Поред информација, целокупна критична инфрастурктура која је задужена за њихов пренос, обраду и складиштење је изложена безбедносним претњама сајбер ратовања.

Информационо ратовање обухвата технике које укључују прикупљање, пренос, заштиту, манипулацију, прекид и уништење информација, којима се одржава предност над противницима. Вођење информационог рата заснива се на три

принципа – сазнати, спречити другога да дође до сазнања и навести друге да дођу до неистинитог сазнања. Појам сајбер ратовања је ужи по обиму од информационог ратовања – он је део информационог ратовања који се изводи у сајбер свету - виртуелној реалности која се састоји од збира рачунара и рачунарских мрежа. У сајбер ратовању активност информационог ратовања одвија се посредством рачунарских мрежа (Путник, 2022).

Услед растуће зависности друштва од ИКТ и ниских трошкова приступа сајбер оружју, појавио се страх од рањивости у развијеним државама због тога што су непријатељи, који нису у стању да воде традиционални вид сукоба, добили могућност да нападну виталне тачке сајбер простора. Страх се показао оправданим јер се у последњих петнаестак година десио велики број сајбер напада на критичну инфраструктуру многих држава. И поред огромних издвајања у војне буџете великих сила, отворени ратни сукоб представља велики ризик чак и за најмоћније државе. Уместо класичних борбених дејстава у којима се губе бројни људски животи и који изискују велике финансијске издатке, много учинковитији биће сајбер напади и ратови. Сајбер простор је од есенцијалног оперативног значаја у модерном ратовању, где се слабости и снаге државе на овом пољу могу искористити у сврхе одвраћања или утицања на биланс моћи. Посебна предност је што сајбер нападе не морају изводити званичне државне институције већ недржавни ентитети, чиме се из правне перспективе избегава одговорност за напад (Путник, 2022).

Одбрана и заштита националног сајбер простора намеће се као приоритет савременог доба. Напади који погађају информациону инфраструктуру сматрају се веома опасним по безбедност нападнуте државе јер могу довести до нарушавања суверенитета државе. Процена безбедносних ризика је први корак у изради стратегијских докумената на пољу безбедности и одбране. Приликом израде стратегије сајбер одбране важно је узети у обзир специфичности сајбер

оружја и сајбер простора кога карактеришу несигурност и непредвидивост и који се веома раликује од физичког света. (Путник, 2022).

4.3. Друге сајбер претње

Сајбер претње представљају злонамерну употребу технологија у сајбер простору које се јављају од стране великог броја актера – криминалаца, терориста, организација и држава. Основне карактеристике **сајбер криминала** су угрожавање безбедности рачунарких података одређеног информационог система или његовог сегмента, противправност, захтев за посебним стручним знањима и практичним вештинама из области рачунарских технологија учиниоца, злоупотреба рачунара као средства за противправно остварење циља, намера учиниоца да прибави за себе или неко друго лице корист, или да причини штету неком другом физичком или правном лицу и непотребност физичког контакта починиоца са жртвом. Сајбер криминал не обухвата само нападе који се могу извести употребом телекомуникационих мрежа, већ и нападе на саме информационе системе и рачунаре, као што су: шпијунажа, откривање и пресретање тајних података и њихово неовлашћено копирање, ометање обраде података, крађа интелектуалне својине, ауторских права или патената, дистрибуција различитог садржаја, превара путем интернета и мејлова, мешање у онлајн финансијске услуге и бројне друге. Сајбер криминал се односи на било који облик криминала који се може извршавати посредством рачунарских система и мрежа, у рачунарским системима и мрежама или против рачунарских система и мрежа (Лукнар, 2022 б).

Рачунарско мрежна експлоатација је вид обавештајног рада, у који спадају прикупљање обавештајних података и друге операције које омогућавају да се дође до података супарничке стране кроз њен информациони систем. Операцијама се може постићи извлачење информација из противничких мрежа, али и убацивање

података и информација у противничке мреже чиме се остварује манипулација противничким информацијама. С друге стране, **Сајбер шпијунажа** представља тип обавештајног прикупљања података заснованог на пресретању електронске комуникације без знања и одобрења власника и држалаца информације, а ради стицања економске, војне или политичке предности. Она подразумева стицање илегалног приступа над противничким информационо–комуникационим системом, тачније његовим поверљивим и тајним информацијама, а ради остварења стратегијске предности. За разлику од сајбер ратовања, она представља само пресретање мрежног саобраћаја ради прикупљања обавештајних података, а не напад са циљем изазивања неоперативности противниче рачунарске мреже, као у случају сајбер ратовања (Путник, Милошевић и Бошковић, 2017).

Информационе и комуникационе технологије (ИКТ) стекле су виталан значај за функционисање земаља широм света. Развој савремених Информационих и комуникационих технологија може произвести како позитиван тако и **негативан ефекат** у зависности од начина и сврхе примене, јер поред тога што служе за функционисање и одржавање критичних државних инфраструктура, истовремено омогућавају повезивање и комуникацију актера унутар сложених криминалних система, као што су организовани криминал и тероризам.

Негативни ефекти развоја ИКТ описани су и у Стратегији националне безбедности Републике Србије („Сл. гласник РС“, бр. 94/2019) у којој је наведено да ће научно-технолошки развој наставити да буде подложан различитим врстама злоупотреба, што ће доводити до негативних безбедносних импликација. Поред тога, идентификовани су и облици угрожавања безбедности у сајбер простору, изазвани динамиком развоја информационих технологија, у виду сајбер шпијунаже, напада на критичну инфраструктуру, неовлашћене продоре у базе тајних података, као и ширења лажних вести и дезинформација путем друштвених мрежа.

5. Нормативна заштита критичне информационе инфраструктуре

У ери софистицираних техничких напада и убрзаног развоја сајбер оружја створена је потреба да се донесе национални закон који би регулисао материју информационе безбедности, нарочито информационих система који контролишу критичну инфраструктуру (Кривокапић, Петровски,Тасић и Кулунџија, 2019). Влада Републике Србије усвојила је различите стратегије, уредбе и акционе планове како би уредила област информационог друштва.

5.1. Закон о критичној инфраструктури

Законом о критичној инфраструктури („Сл. гласник РС“ , бр.87/2018), уређује се национална критична инфраструктура, идентификација и одређивање критичне инфраструктуре Републике Србије, заштита критичне инфраструктуре, надлежност и одговорност органа и организација у области критичне инфраструктуре и информације, извештавање, пружање подршке одлучивању, заштита података, управљање и надзор у области критичне инфраструктуре.

Закон дефинише појмове идентификације и заштите критичне инфраструктуре: „Идентификација критичне инфраструктуре је поступак утврђивања система, мрежа, објеката или њихових делова у одређеном сектору који се, у складу са утврђеним критеријумима, идентификују као критична инфраструктура.“; „Заштита критичне инфраструктуре представља скуп активности и мера које имају за циљ осигурање функционисања критичне инфраструктуре у случају ометања или уништења, односно заштиту у случају претњи и спречавање настанка последице ометања или уништења“ (чл. 2, ст. 2 и 4).

Критична инфраструктура дефинисана је у члану 4 закона:

„Критична инфраструктура су системи, мреже, објекти, или њихови делови, чији прекид функционисања или прекид испоруке роба односно услуга може имати

озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно угрозити функционисање Републике Србије".

Члан 6 одређује секторе у којима се врши идентификација и одређивање критичне инфраструктуре:

1) енергетика;
2) саобраћај;
3) снабдевање водом и храном;
4) здравство;
5) финансије;
6) телекомуникације и информационе технологије;
7) заштита животне средине;
8) функционисање државних органа.

Осим поменутих сектора, критична инфраструктура може се одредити и у другим секторима, на предлог министарства надлежног за одређену област.

Уредбом о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије („Сл. гласник РС",бр.69/2022), прописују се критеријуми за идентификацију критичне инфраструктуре и начин извештавања о критичној инфраструктури у Републици Србији.

Критеријуми према којима се врши идентификација критичне инфраструктуре ,према члану 2 уредбе, утврђују се на основу процене последица које могу да наступе услед ометања или уништења критичне инфраструктуре као и на основу последица које могу да наступе у случају претњи по критичну инфраструктуру.

За спровођење поступка идентификације критичне инфраструктуре у одређеном сектору, задужена су министарства за одређене области. Министарства имају

обавезу да континуирано планирају заштиту критичне инфраструктуре, која се заснива на сталном процесу алализе ризика по функционисање критичне инфраструкутуре и процене адекватности мера заштите. Такође, надлежна министарства су у обавези да достављају редовне и ванредне извештаје о критичној инфраструктури Министарству унутрашњих послова.

Наведена уредба уређује критеријуме за сваки сектор критичне инфраструктуре понаособ, а за нашу тему је значајан члан 10, који прописује критеријуме сектора телекомуникационе и информационе технологије. Под критичном инфраструктуром у сектору телекомуникационе и информационе технологије подразумевају се системи, мреже, објекти или њихови делови чији прекид рада проузрокује:

1) прекид пружања услуга оператора електронских комуникација са учешћем од најмање 10% корисника на одговарајућем тржишту на територији Р.Србије;
2) прекид пружања услуга оператора који управља емисионом инфраструктуром на територији Републике Србије;
3) прекид пружања сервиса електронске управе за грађане, привреду и институције Републике Србије у смислу критичне инфраструктуре која подразумева информационе системе у целини - од физичког нивоа Дата центара где су смештени системи, преко комуникационе и серверске инфраструктуре, до апликативног нивоа;
4) прекид обављања послова изградње, развоја, унапређења и управљања образовном и научноистраживачком рачунарском мрежом Републике Србије;
5) прекид пружања услуге размене интернет саобраћаја (енгл. "internet exchange point");
6) прекид обављања послова управљања регистром националног интернет домена и системом за именовање на мрежи (ДНС системи).

5.2.*Закон о информационој безбедности*

Закон о информационој безбедности („Сл. гласник РС“, бр. 6/2016,94/2017 и 77/2019) који је усвојен 2016.године, представља први кровни закон којим се регулишу мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања информационо - комуникационим системима и њиховог коришћења, те одређује надлежне органе за спровођење мера заштите.

Усвајањем подзаконских аката, односно прописа којима се ближе уређују одредбе закона, званично је заокружен предвиђени нормативни оквир за регулисање области информационе безбедности. То је омогућило да се одређени недостаци постојећег закона донекле превазиђу. У уредбе које се односе на ИКТ системе од посебног значаја спадају:

1. Уредба о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности ИКТ система од посебног значаја;
2. Уредба о ближем уређењу мера заштите ИКТ система од посебног значаја;
3. Уредба о утврђивању листе делатности у областима у којима се обављају делатности од општег интереса и у којима се користе ИКТ системи од посебног значаја; и
4. Уредба о поступку обавештавања о инцидентима у ИКТ системима од посебног значаја.

Једну од најважнијих законских новина чини оснивање Националног центра за превенцију безбедносних ризика (ЦЕРТ), тела задуженог за брзо реаговање у случају инцидената, као и за прикупљање и размену информација о ризицима за безбедност информационо-комуникационих система. (Размал, 2018).

Закон дефинише информационо-комуникациони систем (ИКТ систем) као технолошко-организациону целину која обухвата:

1) електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
2) уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;
3) податке који се воде, чувају, обрађују, претражују или преносе помоћу средстава из тачке 1 и 2, а у сврху њиховог рада, употребе, заштите или одржавања;
4) организациону структуру путем које се управља ИКТ системом;
5) све типове системског и апликативног софтвера и софтверске развојне алате.

5.3. ИКТ системи од посебног значаја

ИКТ системи од посебног значаја су информационо-комуникациони системи који су од велике важности за државу, јер у случају компромитовања таквих система, то може имати директан неповољан утицај на велики број грађана. (Кривокапић и сар., 2019). Прецизније, Закон о информационој безбедности дефинише три основне категорије ИКТ система од посебног значаја и то:

1) Системи који се користе у обављању послова у органима власти

У Органе власти спадају: државни органи, органи аутономне покрајине, органи јединице локалне самоуправе, организације и друго правно или физичко лице коме је поверено вршење јавних овлашћења.

2) Системи који се користе за обраду посебних врста података о личности Закон о заштити података о личности дефинише посебне врсте података о личности и то су подаци којима се открива: расно и етничко порекло, политичко мишљење, верско или филозофско уверење, чланство у синдикату, затим генетски подаци, биометријски подаци у циљу јединствене идентификације лица, подаци о здравственом стању, сексуалном животу и сексуалној орјентацији лица.

У случају обраде ових података, чиме се дубље задире у приватност грађана, мора се поступати у складу са Законом о заштити података о личности.
3) Системи који се користе у обављању делатности од општег интереса и другим делатностима

Закон дефинише области у којима се обављају делатности од општег интереса док су послови и делатности прецизније дефинисани *Уредбом о утврђивању листе делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја* („Сл. гласник РС“, бр. 94/2019). Наведене области су:

1) енергетика:

1 - производња, пренос и дистрибуција електричне енергије;

2 - производња и прерада угља;

3 - истраживање, производња, прерада, транспорт и дистрибуција нафте и промет нафте и нафтних деривата;

4 - истраживање, производња, прерада, транспорт и дистрибуција природног и течног гаса.

2) саобраћај:

1 - железнички,

2 - поштански,

3 - водни и

4 - ваздушни саобраћај.

3) здравство:

1 - здравствена заштита.

4) банкарство и финансијска тржишта:

1 - послови финансијских институција;

2 - послови вођења регистра података о обавезама физичких и правних лица према финансијским институцијама;

3 - послови управљања, односно обављања делатности у вези са функционисањем регулисаног тржишта.

5) дигитална инфраструктура:

1 - размена интернет саобраћаја;

2 - управљање регистром националног интернет домена и системом за именовање на мрежи (ДНС).

6) добра од општег интереса:

1 - коришћење, управљање заштита и унапређивање добара од општег интереса (воде, путеви, минералне сировине, шуме, пловне реке, језера,м обале, бање, дивљач, заштићена подручја).

7) услуге информационог друштва:

1 - услуге информационог друштва у смислу закона којим се уређује електронска трговина.

8) остале области:

1 - електронске комуникације;

2 - издавање службеног гласила Републике Србије;

3 - управљање нуклеарним објектима;

4 - производња, промет и превоз наоружања и војне опреме;

5 - управљање отпадом;

6 - комуналне делатности;

7 - производња и снабдевање хемикалијама.

Оператор ИКТ система је правно лице, орган власти или организациона јединица органа власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности. Његове обавезе су да:

1 - упише ИКТ систем од посебног значаја у евиденцију оператора;

2 - предузме мере заштите ИКТ Система од посебног значаја;

3 - донесе акт о безбедности ИКТ система;

4 - врши проверу усклађености примењених мера заштите ИКТ Система са актом о безбедности ИКТ система, и то најмање једном годишње;

5 - уреди однос са трећим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом;

6 - доставља обавештења о инцидентима који значајно угрожавају информациону безбедност ИКТ система;

7 - достави тачне статистичке податке о инцидентима у ИКТ систему.

5.4. Начела заштите ИКТ система

Приликом планирања и примене мера заштите ИКТ система треба се руководити следећим начелима:

1.Начело управљања ризиком - подразумева да се избор и ниво примене мера заснива на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се остварио, укључујући све врсте ванредних околности.

2) Начело свеобухватне заштите – подразумева да се мере заштите примењују на свим организационим, физичким и техничко-технолошким нивоима, као и током целокупног животног циклуса, односно у свим фазама и аспектима ИКТ система.

3) Начело стручности и добре праксе - подразумева да се мере примењују у складу са стручним и научним сазнањима и искуствима у области информационе безбедности. Комуникација са тачкама као што су ЦЕРТ-ови кључна је у превенцији напада, те у приступу бази знања и позитивних пракси.

4) Начело свести и оспособљености – Сва лица која су повезана са ИКТ системом од посебног значаја морају имати знање и свест о ризицима и инцидентима, што се постиже едукацијом коју спроводе експерти за информациону безбедност. (Кривокапић, и сар., 2019).

6. Врсте инцидената у ИКТ системима од посебног значаја у Републици Србији

Годишњи Извештај о статистичким подацима о свим инцидентима у ИКТ системима од посебног значаја у 2021. години (Национални ЦЕРТ Републике Србије, 2022) у нашој земљи представља свеобухватан преглед сајбер претњи у ИКТ системима од посебног значаја. Праћење ових података омогућава сагледавање трендова напада, што представља основ за креирање адекватних стратегија за одбрану од актуелних напада. У табели бр.1 приказан је број инцидената у прошлој години према групама инцидента.

Табела бр.1 – број инцидената према групама инцидената (Национални ЦЕРТ Републике Србије, 2022).

	Група инцидената	Број инцидената
1.	Неовлашћено прикупљање података	7,925,493
2.	Покушај упада у ИКТ систем	6,273,078
3.	Инсталирање злонамерног софтвера у оквиру ИКТ система	27,319
4.	Остали инциденти	17,813
5.	Превара	17,555
6.	Оперативни инциденти	9,679
7.	Недоступност или ограничена доступност ИКТ система	6,459
8.	Упад у ИКТ систем	1,487
9.	Инциденти физичко-техничке безбедности	112
10.	Угрожавање безбедности података	12
	УКУПНО	13,279,007

1.Неовлашћено прикупљање података подразумева скенирање портова, пресретање података између рачунара и сервера, социјални инжењеринг и компромитовање или цурење података, што је приказано на графикону бр. 1.

графикон бр. 1 – Неовлашћено прикупљање података
(Национални ЦЕРТ Републике Србије, 2022)

Најзаступљенија врста инцидената, скенирање портова је напад који служи за прикупљање информација и не наноси директну штету самој мети, већ се користи за прибављање корисних информација за следеће фазе напада. То је напад код којег се шаљу ИП пакети на изабране портове, а главни циљ је откривање који портови су отворени и који се сервиси користе како би се искористиле потенцијалне рањивости. Заступљеност је повећана и због аутоматизације ове врсте напада (Национални ЦЕРТ Републике Србије, 2022).

Социјални инжењеринг подразумева специфичну технику напада на штићени информационни систем, где нападач комуникацијом покушава да наведе корисника информационо-комуникационог система да прекрши безбедносне норме или процедуре и открије податке за приступ систему, а да притом ни не примети да је изманипулисана. У основи представља обману, манипулацију и уверавање друге особе у неистините чињенице злоупотребом вештине комуникације како би је навели да уради нешто што у нормалним околностима не би урадила, као што је откривање личних информација или отварање порука

електронске поште које садрже малициозни софтвер. Напад се може извршити на више начина, контактом - личним контактом, путем телефона или социјалних мрежа; без контакта - подметањем меморијског медијума, постављањем интернет адресе на форуму или помоћу малициозног софтвера; и комбиновано – комбинацијом два предходно поменута начина (Мандић, Путник и Милошевић, 2017).

2.Приликом **покушаја упада у ИКТ систем** нападачи најчешће користе технику ,,Brute Force" за откривање креденцијала или покушавају да искористе рањивости информационог система, што је приказано на графикону бр. 2.

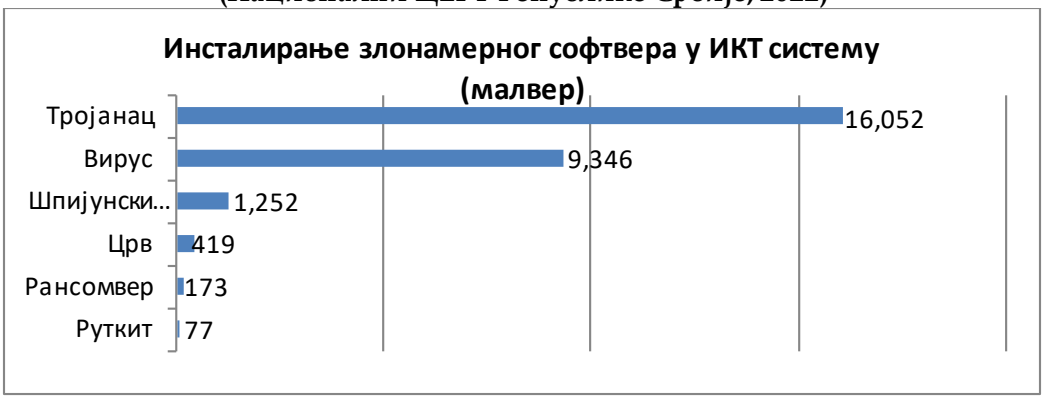
графикон бр. 2 – Покушај упада у ИКТ систем
(Национални ЦЕРТ Републике Србије, 2022)

Покушај откривања креденцијала је напад који подразумева покушај приступа систему жртве непрекидним испробавањем различитих комбинација слова, бројева и симбола са циљем идентификације корисничког имена и лозинке или коришћењем речника. Ови напади се ослањају на слабе лозинке корисника (Национални ЦЕРТ Републике Србије, 2022).

3. **Инсталирање злонамерног софтвера у оквиру ИКТ система** - У злонамерне програме (малвере) спадају: рачунарски вирус, рачунарски црв, рансомвер, рачунарски тројанац, шпијунски софтвер и руткит. Број напада сваким од њих у 2021. години приказан је у графикону бр. 3.

графикон бр. 3 – Инсталирање злонамерног софтвера у ИКТ систему

(Национални ЦЕРТ Републике Србије, 2022)



Тројанац је врста злонамерног софтвера која покушава да се представи корисницима као користан програм и на тај начин их превари да га покрену. Ови програми могу да преузму друге претње са интернета, убацују друге типове малвера на угрожене рачунаре, комуницирају са удаљеним нападачима, као и да бележе све што се куца на тастатури и шаљу нападачима (Национални ЦЕРТ Републике Србије, 2022). За разлику од вируса, тројанац не може да се самореплицира. Он се састоји од кода који извршава одређене функције и најчешће је убачен у неки други програм, као што је рачунарска игра, сервисни програм или апликација што отежава његову детекцију. Продор на кориснички рачунар који је мета напада се најчешће постиже прерушавањем или груписањем са црвима и вирусима. Посебну опасност представља инсталација килогера (Keystroke Logger) на рачунару мете, који снима сва куцања на тастатури, при чему бележи посећене сајтове, евидентира којим фајловима се приступало а може и да сними комплетан садржај на екрану у виду слике. Најчешће коришћени тројанци су они који омогућавају приступ са дистанце (remote accses) због тога што нападачу пружају комплетну контролу над нападнутим рачунаром (Мандић, Путник и Милошевић, 2017).

Вирус је врста малициозног програма који сам себе реплицира и убацује своје копије у легитимне програме где изводе нежељене операције које оштећују систем. Вирус представља део сложенијег кода који се шири унутар рачунара или

рачунарске мреже, копирајући се унутар других програма или у одређеном делу хард диска рачунара тако да се може активирати отварањем инфицираног фајла. и може проузроковати наменско брисање датотека са хард диска и сличну штету.

Шпијунски софтвер је софтвер који се користи за прикупљање информација из система на коме је инсталиран, са задатком да их пренесе примаоцу. Он, за разлику од вируса не може да се шири аутономно, већ захтева инсталацију корисника система. Овај софтвер представља претњу по приватност корисника, јер без дозволе сакупља и прослеђује личне информације и информације о активностима корисника система.

Црв је малициозни софтвер који има способност да сам себе умножава и да се шири системом. За разлику од црва он не мора да зарази ни једну датотеку већ може само служити даљем ширењу, сакупљањем сачуваних адреса електронске поште и слањем копије себе у виду прилога електронске поруке. Црв сам по себи не ствара значајну штету али често може бити преносилац скривене инсталације неког другог малициозног програма (Мандић, Путник и Милошевић, 2017).

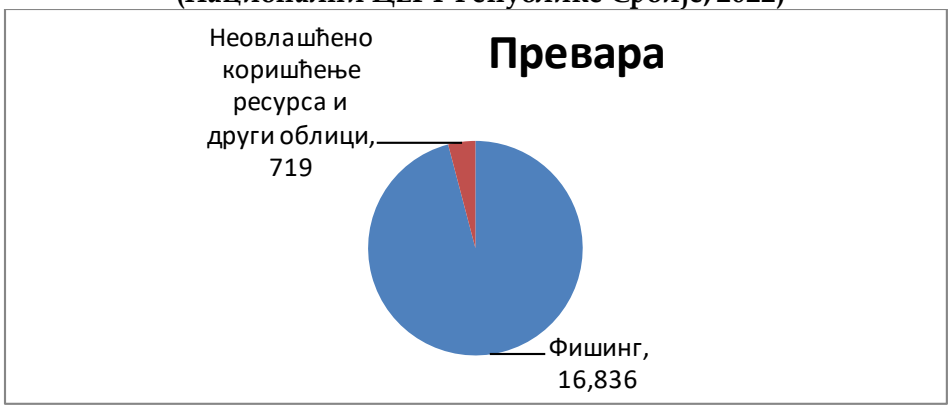
Рансомвер (енгл. *ransomware*) представља уцењивачки малициозни софтвер, који ауторизованом кориснику ограничава приступ рачунарском систему или у њему похрањеним подацима и захтева исплату откупнине како би му повратио право приступа над системом односно подацима. Неке врсте рансомвера могу да блокирају рачунар тако да се на екрану појави уцењивачка порука коју корисник не може да склони без плаћања откупнине, док неке друге врсте овог малвера могу да криптују датотеке у рачунару. Рансомвер се, такође, може проширити на друге рачунаре или уређаје за складиштење на мрежи или у интернет облаку ако је рачунар повезан са локалном мрежом. Напади овог типа могу циљати на ИКТ системе од посебног значаја, па представљају озбиљан изазов за доносиоце политичких одлука и креаторе националних безбедносних политика. Штета коју изазива рансомвер напад није ограничена само на цену откупа, већ обухвата и

трошкове који настају услед оштећења или губитка података, губитка продуктивности и опоравка система након напада. Повећање безбедносне културе код запослених и њихова циљана едукација за препознавање безбедносних претњи и одбрану од сајбер-напада представља најважнији корак у борби против рансомвер напада (Путник, Милошевић, и Цветковић, 2022).

4. У групу **осталих инцидената** спадају сви инциденти који нису наведени у претходним категоријама (Национални ЦЕРТ Републике Србије, 2022).

5.Под **преваром** се подразумевају фишинг напади, неовлашћено коришћење ресурса и други облици преваре. Њиход однос у приказан је у графикону бр.4.

графикон бр. 4 – Превара
(Национални ЦЕРТ Републике Србије, 2022)

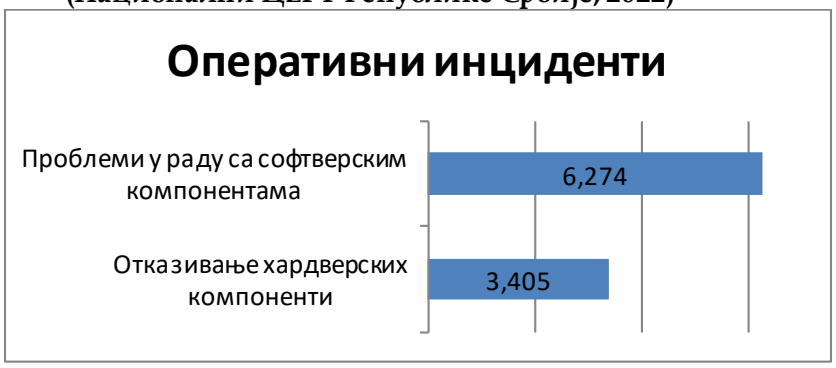


Фишинг је сајбер напад који се врши уз помоћ електронске поште, друшвених мрежа, телефонског позива или СМС-а, којим се захтева да се посети линк или отвори документ. Нападач користи социјални инжењеринг да би се представио као неко коме се може веровати и тако навео жртву да остави поверељиве податке или преузме злонамерни софтвер (Национални ЦЕРТ Републике Србије, 2022). Фишинг (phishing) представља једну од најзаступљенијих техника социјалног инжењеринга, и користи се да опише поступак илегалног прикупљања осетљивих информација, добијених обманом у сајбер простору. Често је у питању стварање лажних интернет страница које су визуелно идентичне оригиналима, али је њихова сврха преузимање поверљивих личних података (често ПИН кодова код

банкарских картица и сл.). Фишинг напад најчешће започиње тако што се жртва на различите начине - електронском поштом, друштвеним мрежама или форумима и сл. усмерава ка одређеној лажној веб страници која је готово идентична оригиналној. Жртва не сумњајући у аутентичност веб странице оставља властите податке које потом нападач прикупља и користи како би преузео њен идентитет и извршио незаконите трансакције. Последице су финансиски губитци или чак губитак електронског идентитета који може бити искоришћен за криминалне циљеве. Ови напади се у суштини заснивају на недостатку безбедносне културе корисника рачунарких система (Мандић, Путник и Милошевић, 2017).

6.Оперативни инциденти су сви они инциденти који доводе до отказивања хардверских компоненти или проблема у раду са софтверским компонентама. Приказани су графиконом бр. 5.

графикон бр. 5 – Оперативни инциденти
(Национални ЦЕРТ Републике Србије, 2022)



7.Нападима **недоступности или ограничене доступности ИКТ система** се оптерећује мрежни саобраћај, што доводи до кашњења операција или пада система (Национални ЦЕРТ Републике Србије, 2022). Доступност може бити угрожена и локалним радњама (уништење, прекид у дистрибуцији електричном енергијом и слично) или услед више силе, ненамерних или намерних људских грешака, што је приказано у графикону бр.6.

графикон бр. 6 – Недоступност или ограничена доступност ИКТ система

(Национални ЦЕРТ Републике Србије, 2022)

Дистрибуирано лишавање услуге („Distributed Denial of Service – DdoS“) су сајбер напади чији је циљ онемогућавање клијената или организације да користе услуге рачунарске мреже односно информационих ресурса, што се постиже нападом на системе који омогућавају те услуге. То је врста напада која циља пре свега на доступност информација. Последица ових напада је штета која се испољава у потребном времену за оспособљавање нападнутог система. Најчешће коришћени метод за спровођење напада је излагање рачунарских мрежа и сервера огромном броју захтева концентрисаних у кратком временском периоду. То је у данашње време аутоматизован процес, што га чини доступнијим и једноставнијим за извођење. Напад почиње тако што нападач присваја контролу над једним рачунаром који постаје „master“ напада, преко којег се хиљаде других рачунара инфицира црвом или бот-ом (малициозни програми чији је циљ да омогуће контролу са даљине) како би постали тзв. „Зомбији“. Зомби-рачунари могу да изврше сваку акцију која је предвиђена малициозним програмом а коју нападач позива командом са дистанце. Хиљаде инфицираних рачунара могу истовремено да покрену напад DDoS против мете коју је нападач одабрао (Мандић, Путник и Милошевић, 2017). Разлика у односу на нападе са циљем онемогућавања или ометања функционисања ИКТ система који нису дистрибуирани је то што

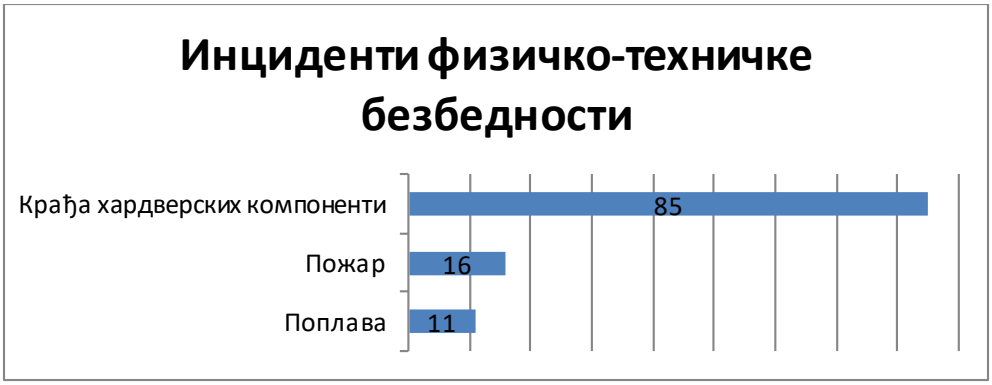
„DdoS“ напади постижу већу ефикасност користећи истовремено више компромитованих рачунарских система као изворе напада.

8.Упад у ИКТ систем подразумева успешно компромитовање система или апликација (сервиса) извршено са удаљене локације коришћењем нове или познате рањивости или неовлашћеним локалним приступом. Њихов однос је приказан графиконом бр.7.

графикон бр. 7 – Упад у ИКТ систем
(Национални ЦЕРТ Републике Србије, 2022)

9.**Инцидентима физичко-техничке безбедности** припадају крађа хардверских компоненти, пожар и поплава који су довели до угрожавања физичко-техничке безбедности ИКТ система, што је приказано на графикону бр.8.

графикон бр. 8 – Инциденти физичко – техничке безбедности
(Национални ЦЕРТ Републике Србије, 2022)



10.Угрожавање безбедности података -Поред злоупотребе података и система неовлашћеним приступом, односно неовлашћеном изменом или брисањем података, нарушавање безбедности података може бити и последица криптографског напада, као штоје приказано графиконом бр. 9.

графикон бр. 9 – Угрожавање безбедности података
(Национални ЦЕРТ Републике Србије, 2022)

Треба имати у виду да бројке представљају искључиво регистроване случајеве, и то само у Републици Србији за 2021. годину, што значи да број случајева одређеног инцидента не мора да буде сразмеран реалној претњи коју исти може да представља. Код појединх напада постоји велики број нерегистрованих случајева, а ни последице код свих инцидената нису идентичне. И поред тога извештај представља солидну основу за анализу инцидената.

7. Мере заштите ИКТ система од посебног значаја

Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система, којима се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената у ИКТ системима (Кривокапић и сар., 2019).

Мере заштите ИКТ система од посебног значаја су детаљно прописане и ближе уређене *Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја* ("Сл. гласник РС", бр. 94/2016). У наведене мере спадају:

1. Успостављање организационе структуре

Приступ ИКТ систему од посебног значаја треба да буде условљен радним задужењима и обавезама које свако од запослених има у опису свог радног места, са циљем да се смањи ризик од злоупотреба, неовлашћених приступа, нарушавања интегритета података у ИКТ систему и људске грешке.

2. Безбедан рад на даљину и безбедна употреба мобилних уређаја

Коришћење мобилних уређаја и приступ на даљину могу бити изазов у безбедности ИКТ система будући да користе јавне мреже како би комуницирали са централним ИКТ системом чиме се отвара могућност за МитМ (,,man in the middle") нападе у којима нападач користи недостатке везе како би приступио комуникацији и извршио крађу података. Безбедан начин за рад на даљину је повезивање путем виртуелне приватне мреже, стварањем издвојеног тунела између два рачунара на јавној мрежи, који се посебно кодира ради заштите.

3. Едукација о начину функционисања и одговорности запослених који користе ИКТ систем

Оператори ИКТ система од посебног значаја требало би да посвете пажњу константној едукацији запослених у области безбедности ИКТ система. Приликом започињања радног односа, новозапослени треба да се упозна са интерним актом о безбедности ИКТ система од посебног значаја, те да потпише

изјаву о томе као и изјаву о поверљивости информација до којих долази у току обављања послова, чиме преузима одговорност за прописно поступање са ИКТ системом. Потребно је организовати периодичне обуке за запослене који раде у оквиру ИКТ истема од посебног значаја. Суштина ових обука би требало да буде не само у објашњавању правних прописа, већ у анализи конкретних примера кршења закона и лоше праксе. Такође би требало организовати периодично тестирање запослених из области безбедности ИКТ система.

4. Заштита од ризика који настају при променама послова или кадровским променама

Оператор ИКТ система од посебног значаја има обавезу да уговором или другим интерним правним актом прецизније уреди дужности и обавезе запосленог или на други начин ангажованог лица које ради у ИКТ систему од посебног значаја, а које остају на снази при промени послова или након престанка радног односа или ангажовања, при чему исти нема право да открива поверљиве или друге информације које могу да утичу на безбедност ИКТ система од посебног значаја.

5. Идентификација и класификација информационих добара у оквиру ИКТ система

Оператор ИКТ система је дужан да формира базу информационих добара, опреме и софтвера који се користе за израду, обраду, чување, пренос, брисање и уношење података у оквиру ИКТ система од посебног значаја. У Бази би за свако информационо добро требала да буде назначена одговорна особа и да сваки унос у базу буде означен нивоом осетљивости и критичности.

6. Класификовање података

Оператор ИКТ система од посебног значаја, након извршене процене ризика, има обавезу да изради систем класификације података којим ће се одредити њихов ниво заштите у складу са осетљивости и важности података, те штете која може настати услед неовлашћеног откривања, измене, брисања или уништења

података, и у складу са прописима који регулишу тајне, односно осетљиве податке.

7. Заштита носача података

Носачи података су све врсте меморијских предмета и уређаја који се користе за складиштење и пренос података. Потребно је дефинисати који носачи могу да се користе у оквиру ИКТ система, а у зависности од оперативних потреба. Такође, треба прописати да запослена лица не могу да користе своје личне или уређаје и медије трећих лица како би складиштили или преносили податке унутар и изван ИКТ система од посебног значаја, како би спречили уношења малициозног софтвера у ИКТ системе од посебног значаја.

9. Енкрипција

Заштиту података у ИКТ систему од посебног значаја омогућава енкрипција, односно шифровање података тако да их је немогуће растумачити без шифре. Коришћење механизама (алгоритама) за енкрипцију мора да буде стандардизовано на нивоу оператора ИКТ система од посебног значаја. Оператор мора да пропише адекватне начине генерисања, чувања, дистрибуције, повлачења и брисања крипто кључева. Кључеви се морају чувати у енкриптованој бази са високо рестриктивним приступом.

10.Физичка заштита

Просторије оператора ИКТ система од посебног значаја треба да имају адекватну физичку заштиту у виду алармних система и система за контролу приступа (коришћењем идентификационих картица и сл). Просторије у којима се налазе опрема и документи који су саставни део ИКТ система од посебног значаја треба да буду безбедне зоне у оквиру објекта оператора. Сви сервери треба да буду смештени у посебној сервер сали, у којој се поштују одређене сигурносне мере. Приступ сали мора бити ограничен на службенике из ИКТ сектора који су

задужени за одржавање система, сервера, мреже и телекомуникација. Такође, сала се мора закључавати сигурносном бравом.

11. Исправно и безбедно функционисање ИКТ система од посебног значаја

Приступ ИКТ систему треба омогућити само лицима која одржавају систем као и лицима којима је приступ потребан због појединачног случаја. Кориснички приступ систему треба да буде на најнижем нивоу, односно да поседује минималне привилегије и то искључиво делу система који је кориснику потребан за рад. Такође, систем администатор треба да конфигурише систем тако да се након одређеног времена неактивна сесија прекине. Софтвер треба ажурирати благовремено и успоставити редовну шему прављења резервних копија.

12. Заштита од злонамерног софтвера

Пре свега, на нивоу хардвера треба блокирати све портове који нису потребни за оперативни рад на конкретним уређајима, те прописати правила о коришћењу уређаја који нису у власништву оператора ИКТ система од посебног значаја. Софтверска решења за заштиту од злонамерног софтвера су анти-вирус или анти-малвер софтвер на сваком уређају у оквиру ИКТ система, те софтверски зид („firewall") који филтрира саобраћај у оквиру мреже. Кад је у питању електронска комуникација, добра анти-спам и анти-малвер конфигурација смањује ризик да запослени из незнања унесу злонамеран софтвер у ИКТ систем.

13. Заштита од губитака података

Стварање резервне копије (бекап) је од кључног значаја када се јави потреба да се изгубљени подаци поврате. Понекад је на основу резервне копије могуће утврдити узрок пада система – реконструкцијом сигурносних пропуста или грешака у систему, и слично. Препоручено је и екстерно и интерно чување копија. Екстерни бекап се односи на чување датих копија података на посебним дисковима, док интерни бекап подразумева чување копија базе података у оквиру система, односно на серверу.

14. Логовање

Лог је регистар свих догађаја у оквиру једног система, односно свих активности корисника - од пријаве, преко уноса података до њихових промена, штампања, брисања и других поступака. Основни облик је приступни лог, и он садржи конкретне информације о кориснику који је приступио бази података, времену приступа, ИП адреси, о ресурсу коме је приступљено и врсту обраде података.

15. Интегритет софтвера

Систем администратор врши администрацију софтвера и води рачуна о свим сегментима ИКТ система. Његове активности подразумевају ажурирање софтвера, вођење рачуна о резервним копијама, униформно конфигурисање софтвера, успостављање механизама за повратак на преходно стање ИКТ система у случају грешке или безбедносног инцидента. Систем администратор треба да врши периодичне тестове безбедности ИКТ система како би идентификовао слабости у безбедносним процедурама. Ови тестови обухватају све сегменте ИКТ система, а пре свега приступ споља кроз ,,brute force" нападе или преко грешака у софтверском коду, а које омогућавају нападачима неприметан улаз у систем (,,backdors").

16. Заштита комуникационих канала

Приликом успостављања канала комуникације за пренос података најбоље је користити ,,енд то енд" енкрипцију, што би значило да се подаци енкриптују на извору, а декриптују на дестинацији, односно да они ни у једном тренутку нису јасно видљиви приликом преноса кроз јавне мреже. Оператор ИКТ система треба да изврши сегментацију мреже, односно да мрежу која се користи за пренос тајних и осетљивих података одвоји од мреже која има друге намене, тако да заштићеној мрежи могу приступити само овлашћена лица. Медији за пренос података и каблови за напајање електричном енергијом треба да буду адекватно

заштићени од електромагнетних зрачења и других физичких ризика који би могли да утичу на интегритет и безбедност података.

17. Животни циклус ИКТ система од посебног значаја

Стандарде информационе безбедности потребно је поставити у оквиру сваке фазе развоја ИКТ система од посебног значаја. Приликом пројектовања морају да се детаљно размотре сви ризици и потенцијалне слабости система. Значајно је кориговати процедуре на самом почетку примене, како би се убудуће избегле скупе и компликоване корекције система.

18. Уговор са пружаоцима услуга

Уколико постоји потреба да ИКТ систем од посебног значаја буде доступан пружаоцима услуга који ће користити одређени сегмент ИКТ система, као што су подаци или специфичне функције система, оператор ИКТ система од посебног значаја треба да одреди ниво и начин приступа у зависности од легитимних потреба пружалаца услуга. Обавезе пружалаца услуга регулишу се споразумом између оператора ИКТ система од посебног значаја и пружалаца услуга.

19. Превенција и реаговање на безбедносне инцидентне претње

Кад дође до ризика од инцидента, битно је да постоји процедура управљања инцидентима, како би систем постао функционалан што пре, те да би се разлог настанка инцидента брзо лоцирао. Оператор треба да развије протоколе који се састоје од правила и одговорних лица која ће знати шта тачно треба да раде кад примете да се десио, или да ће се десити инцидент.

20. Континуитет обављања посла у ванредним околностима

Од критичне важности је да након безбедносног инцидента систем буде враћен у функцију што пре. Оператор треба да има развијене процедуре које су функционално тестиране током редовног стања ИКТ система, како би њихова имплементација у ванредним околностима била јасна свим одговорним лицима (Кривокапић и сар., 2019).

8. Улога националног ЦЕРТ-а у заштити критичне информационе инфраструктуре

Усвајање закона који се односи на заштиту критичне инфраструктуре и регулисање сарадње између јавног и приватног сектора представља основу за формирање система заштите критичне инфраструктуре. Ради успостављања ефикасног система раног упозорења створена је потреба за формирањем тима за ванредне ситуације у области информационих и комуникационих технологија који би радио на превенцији али и превазилажењу постојећих криза и заштити државног интернет окружења од потенцијалних сајбер напада. Многе развијене земље препознале су ту потребу, те су формирани тимови који свакодневно уско сарађују и изграђују заједничку базу података која садржи све релевантне информације о потенцијалним и стварним претњама критичној инфраструктури, као и податке о позитивним и негативним искуствима одређених држава у вези решавања проблема повезаних са заштитом критичне инфраструктуре. Такође, оформљени су Центри за анализу и размену података чија је улога да обезбеде информације о претњама, рањивостима и инцидентима који би могли да угрозе критичнун инфрастуру (Кешетовић, Путник и Ракић, 2013).

Можда и најважнији нормативни ослонац сајбер безбедности представљају законске одредбе којима се успоставља систем ране детекције и успешне превенције сајбер напада, уз додељивање јасних овлашћења и обавеза надлежним субјектима. Ове одредбе се налазе у Закону о информационој безбедности (2016) у којем је члановима 14 и 15 прописано успостављање Националног ЦЕРТ-а и одређене су његове надлежности, док су у члановима од 16 до 19 прописани надзор над ЦЕРТ-ом, посебни центри за превенцију безбедносних ризика у ИКТ системима, Центар за безбедност ИКТ система у органима власти, као и ЦЕРТ самосталног оператора ИКТ система. (Милошевић и Путник, 2017).

Национални ЦЕРТ – Центар за превенцију безбедносних ризика у ИКТ системима („Computer Emergency Response Team“) према закону о

информационоој безбедности представља тело које обавља послове координације, превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији на националном нивоу. За послове Националног ЦЕРТ-а надлежна је Регулаторна агенција за електронске комуникације и поштанске услуге (РАТЕЛ).

Овакво тело постоји у већини земаља света. Надлежности националних ЦЕРТ-ова се, у зависности од специфичности инфраструктуре, разликују од државе до државе, али то је увек експертска организација чија је главна надлежност координација и комуникација на националном и међународном нивоу, ради превенције и управљања ризицима у овој области.

Национални ЦЕРТ је надлежан да прати инциденте на националном нивоу, да пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инцидентима, да реагује по пријављеним или на други начин откривеним инцидентима, тако што пружа савете на основу расположивих информација лицима која су погођена инцидентом и предузима друге потребне мере из своје надлежности на основу добијених сазнања.

Ово тело такође прати пријављене инциденте на националном нивоу и на основу прикупљених података континуирано израђује анализе ризика и инцидената, подиже свест код грађана, привредних субјеката и органа јавне власти о значају информационе безбедности, води евиденцију посебних ЦЕРТ-ова, те извештава надлежно министарство као надлежни орган на кварталном нивоу о предузетим активностима.

Посебан ЦЕРТ (Посебан центар за превенцију ризика у ИКТ системима) је правно лице или организациона јединица у оквиру правног лица, уписана у евиденцију посебних ЦЕРТ-ова коју води Национални ЦЕРТ. Посебан ЦЕРТ такође обавља послове превенције и заштите од безбедносних ризика у ИКТ системима, али у оквиру одређеног правног лица, групе правних лица, области пословања и слично. За разлику од Националног ЦЕРТ-а који подиже свест о

могућим безбедносним ризицима, пружа упозорења, прати инциденте на националном нивоу и координише информације које добија, посебни ЦЕРТ-ови имају оперативнију улогу да конкретно бране ИКТ системе на које су фокусирани, односно у оквиру којих су формирани. На тај начин, посебни ЦЕРТ-ови се специјализују за одређену област или групу, те прате стање и реагују у случају инцидената само за ту област или групу. На овај начин посебни ЦЕРТ-ови стичу посебна знања и искуства за одређене области и спремнији су да пруже специјализовану помоћ.

ЦЕРТ органа власти (Центар за безбедност ИКТ система у органима власти) обавља послове који се односе на заштиту од инцидената у ИКТ системима органа власти, осим ИКТ система самосталних оператора. Послове ЦЕРТ-а органа власти обавља орган надлежан за пројектовање, развој, изградњу, одржавање и унапређење рачунарске мреже републичких органа, односно Канцеларија за информационе технологије и електронску управу. ЦЕРТ органа власти је задужен за заштиту јединствене информационо-комуникационе мреже електронске управе и координацију и сарадњу са операторима ИКТ система које повезује ова мрежа у циљу превенције инцидената, откривања и прикупљања информација о инцидентима и отклањању њихових последица, као и давање стручних препорука за заштиту ИКТ система органа власти, осим када су у питању ИКТ системи за рад са тајним подацима.

Самостални оператори ИКТ система су Министарство одбране, Министарство унутрашњих послова, Министарство спољних послова и службе безбедности. Наведена министарства и службе су у обавези да формирају сопствене центре за безбедност ИКТ система ради управљања инцидентима у својим системима, који могу размењивати информације о инцидентима, као и са Националним ЦЕРТ-ом, са ЦЕРТ-ом органа власти, а по потреби и са другим организацијама. (Кривокапић и сар. , 2019).

У циљу остваривања сарадње и усклађеног обављања послова у функцији унапређења информационе безбедности, као и иницирања и праћења превентивних и других активности у области информационе безбедности Влада је основала Тело за координацију послова информационе безбедности, у чији састав улазе представници министарстава надлежних за послове информационе безбедности, одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата владе, Народне банке Србије, Центра за безбедност ИКТ система у органима власти и Националног центра за превенцију безбедносних ризика у ИКТ системима (Кривокапић и сар. , 2019). Иако закон дефинише Тело за координацију углавном као саветодавно, оно представља прилику за свеобухватнији приступ информационој безбедности, тако што ће се препознати могућност формирања стручних радних група у којима ће учествовати и представници других институција, приватног сектора, академске заједнице и цивилног друштва. (Размал, 2018).

9. Закључак

Информационе и комуникационе технологије су постале окосница функционисања савремених критичних инфраструктурних система. Оне су омогућиле повезивање, односно умрежавање различитих инфраструктурних елемената.

Критична информациона и комуникациона инфраструктура пружа функционалну подршку која је потребна за рад критичног инфраструктурног система. Информационе технологије и електронске комуникације повезују све остале секторе критичне инфраструктуре па је њихона доступност од изузетног значаја за функционисање целокупног система. Нефункционисање критичне информационе и комуникационе инфраструктуре може да узрокује прекид и озбиљно угрози функционисање комплетне критичне инфраструктуре (Лукнар, 2022).

Због тога је неопходно имати у виду актуелне претње по ИКТ системе, спроводити постојеће мере заштите критичне ИКТ инфраструктуре, које је потребно константно преиспитивати и усавршавати, с обрзиром да је област информационих и комуникацијоних технологија веома склона појави нових облика угрожавања и претњи.

Литература

Бошковић, М., Ивковић, В. и Путник, Н. (2013). *Risk Management in Public-Private Partnership over Critical Infrastructures.* U: Dimitrijević, I. (editor), National Critical Infrastructure Protection – Regional Perspective. (pp. 231-243). Београд: Универзитет у Београду - Факултет безбедности и Институт за корпоративну безбедност – Љубљана;

Госпић, Н., Мурић, Г. и Богојевић, Д.(2012). *Дефинисање критичне телекомуникационе инфраструктуре у Србији*. Београд: XXX Симпозијум о новим технологијама у поштанском и телекомуникационом саобраћају – ПосТел 2012;

Закон о информационој безбедности („Сл. гласник РС“, бр. 6/2016,94/2017 и 77/2019);

Закон о критичној инфраструктури („Сл. гласник РС“, бр.87/2018);

Јаковљевић, В. (2010). *Ресурси критичне инфраструктуре и њихов значај за управљање ванредним ситуацијама.* Годишњак Факултета безбедности, 63-81;

Кешетовић, Ж., Путник, Н. и Ракић, М. (2013). *Possibilities of Improving Critical Infrastructure Protection in Countries in Transition.* U: Dimitrijević, I. (editor), *National Critical Infrastructure Protection – Regional Perspective*. (pp. 131-142). Београд: Универзитет у Београду - Факултет безбедности и Институт за корпоративну безбедност – Љубљана;

Кривокапић, Д., Петровски, А., Тасић, Д. и Кулунџија, С. (2019). *Водич за ИКТ системе од посебног значаја: Информациона безбедност*. „Share“ фондација;

Лукнар, И. (2022). *Злоупотреба информационих и комуникационих технологија: појам и уређење у Републици Србији.* Политика националне безбедности, 22(1/2022), 171-188;

Лукнар, И. (2022б). *Сајбер тероризам - Мере за сузбијање и превенција,* Београд: Институт за политичке студије;

Мандић, Г., Путник, Н., Милошевић, М. (2017). *Заштита података и социјални инжењеринг - правни, организациони и безбедносни аспекти*. Београд: Универзитет у Београду - Факултет безбедности, 512 стр;

Милосављевић, Б. и Вучинић, Д. (2021). *Однос према критичној инфраструктури у Републици Србији*. Београд: Војно дело, 4/2021, 42-145;

Милошевић,М. & Путник,Н.(2017). *Сајбер безбедност и заштита од високотехнолошког кр иминала у Републици Србији - стратешки и правни оквир*, Култура полиса, год. XIV, бр. 33, стр. 177-191;

Мићовић, Д.М. (2020). *Специфичности критичне инфраструктуре у Републици Србији*. Београд:Криминалистичко – полицијски универзитет;

Национални ЦЕРТ Републике Србије (2022). Извештај о статистичким подацима о свим инцидентима у ИКТ системима од посебног значаја у 2021. години;

Путник, Н. (2022). *Сајбер рат и сајбер мир*. Научна монографија, стр. 198. Београд: Универзитет у Београду – Иновациони центар Факултета безбедности и Академска мисао;

Путник, Н., Милошевић, М. и Бошковић, М. (2017). *Стратешко планирање сајбер одбране – ка адекватнијем правном оквиру и новој концепцији процене ризика, изазова и претњи*, Војно дело, vol. 69, бр. 7, стр. 174-185;

Путник, Н., Милошевић, М., и Цветковић, В. (2022). *Рансомвер као претња безбедности - друштвени и кривичноправни аспекти*. Социолошки преглед, 56(1), 328-353;

Размал, И. (2018). *Водич кроз информациону безбедност у Републици Србији 2.0.* Београд: Мисија ОЕБС-а у Србији, Уником Телеком, ИБМ, Јунипер;

Ракић, М.М. (2015). *Кризни менаџмент у функцији заштите критичних инфраструктура у земљама у транзицији*. Докторска дисертација. Београд: Факултет безбедности;

Стратегија националне безбедности Републике Србије („Сл. гласник РС“, бр. 94/2019);

Трбојевић, М. (2018). *Заштита критичних инфраструктура – искуства транзиционих земаља*. Политичка ревија, 56(2/2018), 99-118;

Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја ("Сл. гласник РС", бр. 94/2016);

Уредба о утврђивању листе делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја („Сл. гласник РС“, бр. 94/2019);

Уредбао критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије („Сл. гласник РС“,бр.69/2022);

Шкеро, М. и Атељевић, В. (2015). *Заштита критичне инфраструктуре и основни елементи усклађивања са директивом савета европе 2008/114/ЕС*. Београд:Војно дело, 3/2015, 192-207.

ИЗЈАВА О АКАДЕМСКОЈ ЧЕСТИТОСТИ

Изјављујем да сам у приложеном раду поштовао/ла сва правила о академској честитости.

Овај писани рад резултат је искључиво мог личног рада, темељи се на мојим истражиањима и ослања се на наведену литературу.

У Београду, дана _____ године.

Потпис студента:

_____