РЕПУБЛИКА СРБИЈА
Град Ваљево
Дом здравља Ваљево
Број: 13-01-3246
Датум 14 ОСТ 2022. год.
Ваљево, Железничка 12

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС”, број 6/2016 и 94/2017), чланова 2. и 3. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС”, број 94/16), Управни одбор Дома здравља Ваљево на седници одржаној дана 14.10.2022. године усвојио

ПРАВИЛНИК О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО-КОМУНИКАЦИОНОГ СИСТЕМА ДОМА ЗДРАВЉА ВАЉЕВО

I ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Правилником о безбедности информационо-комуникационог система (у даљем тексту: Акт о безбедности) Дома здравља Ваљево, у складу са Законом о информационој безбедности („Службени гласник РС”, број 6/2016 и 94/2017, у даљем тексту: Закон), ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система Дома здравља Ваљево (у даљем тексту: ИКТ систем).

Циљеви доношења Акта о безбедности су:

Члан 2.

1)одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;
2)спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност;
3)подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
4)прописивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;

Члан 3.

Корисници ИКТ система Дома здравља Ваљево (у даљем тексту: корисници) јесу запослени. Изузетно, корисници могу бити и трећа лица ангажована уговором за обављање послова у вези ИКТ система.
Корисници морају бити упознати са садржином Акта о безбедности и дужни су да поступају у складу са одредбама овог акта, као и других интерних процедура које регулишу информациону безбедност.
Директор установе је одговоран за праћење примене мера безбедности.

Члан 4.

Корисници су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних радних активности.

Непоштовање одредби Акта о безбедности, као и свако угрожавање или нарушавање информационе безбедности, повлачи дисциплинску одговорност запосленог.

Дисциплински поступак се покреће по пријави лица Рачунарског центра који представља службу овлашћену за праћење прикупљања, анализе и обраде статистичких података.

II МЕРЕ ЗАШТИТЕ

Члан 5.

Мерама заштите се обезбеђује превенција од настанка инцидената који угрожавају обављање делатности Дома здравља Ваљево, односно заштита података садржаних у ИКТ систему, од неовлашћеног приступа, модификације, коришћења и деструкције на начин да интегритет, тајност и расположивост података не смеју бити компромитовани.

Дом здравља Ваљево је у обавези да набави и одржава потребну софтверску и хардверску опрему помоћу које ће се омогућити примена мера заштите предвиђених Актом о безбедности.

Интерни акти који уређују обавезе и одговорности запослених у вези са управљањем информационом безбедношћу:

Члан 6.

•Правилник о унутрашњој организацији и систематизацији радних места;
•Уговори о раду;
•Процедура о управљању информацијама.

Удаљени приступ

Члан 7.

Дом здравља Ваљево дозвољава удаљени приступ и употребу мобилних уређаја од стране запослених лица, уколико је осигурана безбедност рада у случају обављања послова ван просторија послодавца, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења мобилних уређаја.

Удаљени приступ се омогућује помоћу заштићене VPN или IP Sec – заштићеним криптованим тунелом одговарајућег провајдера - конекције преко које се корисници повезују на ИКТ систем Дома здравља Ваљево.

Овај начин приступа се примењује и када се користе мобилне уређаји за повезивање на мрежу Дома здравља Ваљево.

Мобилни уређаји морају бити подешени тако да омогуће сигуран и безбедан приступ уз активан одговарајући софтвер за заштиту од вируса и другог злонамерног софтвера.

Удаљени приступ одобрава директор Дома здравља Ваљево на основу предлога одговорног лица Рачунарског центра Дома здравља Ваљево.

Члан 8.

Приликом коришћења мобилних уређаја потребно је осигурати пословне информације од могућег компромитовања.

Корисник мобилног уређаја преко којег је омогућен приступ мрежи Дома здравља Ваљево у обавези је да крађу или губитак мобилног уређаја пријави Рачунарском центру без одлагања, а у року од 72 сата да достави писану изјаву о околностима губитка или крађе мобилног уређаја.

Рачунарски центар је у обавези да, по пријави крађе или губитка мобилног уређаја, неодложно блокира несталом мобилном уређају приступ информационом систему и кориснику промени креденцијале за приступ.

У случају да се пронађе мобилни уређај чији је нестанак пријављен, Рачунарски центар ће извршити преглед уређаја и утврдити да ли он може бити поново коришћен за удаљени приступ.

Оспособљеност корисника

Члан 9.

Дома здравља Ваљево се стара да запослени који управљају ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности, као и свест о значају послова које обављају. Њихове одговорности су утврђене уговором о раду или ангажовању на привременим и повременим пословима.

Запослени и друга лица којима је на основу посебог уговора додељен приступ поверљивим информацијама, морају потписати споразум о поверљивости и заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Члан 10.

Запослени у Рачунарском центру Дома здравља Ваљево континуирано се обучавају у циљу унапређења техничког и технолошког знања. Ова лица су ауторизована за предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите.

Запослени у стручним службама Дома здравља Ваљево су у обавези да прођу одговарајућу обуку и редовно стичу нова и обнављају постојећа знања о процедурама које уређују безбедност информација, на начин који одговара њиховом пословном ангажовању и радном месту.

Заштита од ризика који настају при промени статуса корисника

Члан 11.

Запослени, као и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања, под претњом кривичне и материјалне одговорности.

Обавезе које остају важеће и после престанка запослења треба да буду садржане у тексту уговора о раду са запосленим и у условима заснивања радног односа.

Ова мера је ближе одређена Уговором о раду запосленог.

Члан 12.

Одељење за правне послове, кадровске и административне послове, у обавези је да Рачунарски центар обавести о престанку статуса запосленог, у року од три дана.

Након тога, Рачунарски центар предузима следеће активности:

•прегледа све налоге и приступе систему који су били доступни кориснику,
•проверава враћене мобилне уређаје и уређаје за преношење података,
•укида налог електронске поште и свих других права приступа ИКТ систему Дома здравља Ваљево кориснику коме је престао статус.

Ова активност извршиће се у року од три дана по пријему одговарајућег обавештења.

Идентификација информационих добара и њихова зашпита

Члан 13.

Дома здравља Ваљево врши идентификацију информационих добара и документује њихов значај. У информациона добра Дома здравља Ваљево спадају хардверске и софтверске компоненте ИКТ система, подаци који се чувају и обрађују као и подаци о корисничким налозима.Евиденцију о информационим добрима воде Рачунарски центар и Служба за материјално и финансијско пословање.

Члан 14.

Дома здравља Ваљево може да означи типове и локације података као поверљиве, интерне или јавне. Сврха ове класификације је:

•Јачања корисничке одговорности. како би корисници могли да уоче и препознају пословну вредност податка приликом чувања или слања и буду свесни одговорности за неовлашћено коришћење или преношење;
•Подизања свести о вредности информације или документа;
• Заштите садржаја;
•Интеграције са системима за архивирање.
Класификација документа мора да буде усклађена са правилима контроле приступа.

Члан 15.

Дома здравља Ваљево обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења информација и садржаја који се чувају на носачима података и имају посебан значај за функционисање ИКТ система.

Евиденцију носача података на којима су снимљени подаци од значаја за Дома здравља Ваљево води Рачунарски центар.

Члан 16.

Када престане потреба да неки медијум садржи податке који су од посебног значаја, безбедно уклањање података врши се применом форматирања медијума.
Медијуми код којих није могуће извршити форматирање морају се физички уништити.

Члан 17.

Када је потребно транспортовати носаче података који садрже информације од посебног значаја за Дома здравља Ваљево, за случај да је неопходно задржати њихов садржај, потребно је извршити њихову додатну физичку заштититу.

Одабрани начин транспорта мора да буде у складу са потребом заштите интегритета података.

Члан 18.

Подацима и средствима за обраду података може се ограничити приступ у складу са степеном поверљивости.

Приступ ресурсима ИКТ система одређен је врстом налога, односно додељеном улогом коју корисник има. Свака злоупотреба додељеног корисничког налога повлачи дисциплинску или кривичну одговорност корисника.
Дефинисани су кориснички нивоу и привилегије, такође и групе корисника.

Члан 19.

Дома здравља Ваљево управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора.

Управљање корисничким идентификаторима врши се поштујући следеће принципе:

•Кориснички идентификатори запослених су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности.
•Свааком кориснику у систему се додељују јединствени кориснички идентификатори.
•Запослени користе заједнички идентификатор који омогућава ограничени приступ ресурсима ИКТ система за потребе наставе, стручног усавршавања, тестирања апликација.
•Кориснику коме је престао статус запосленог укида се кориснички идентификатор.
Додељивање привилегованих (администраторских) права на приступ врши се на основу одлуке лица запосленом у Рачунарском центру.

Привилегована права на приступ додељују се посебно за сваки системски објекат уз дефинисан рок трајања тих права.
Привилегована права на приступ која треба доделити корисничком идентификатору другачија су од оних која се користе за редовне активности.

Редовне пословне активности не треба вршити из привилегованих корисничких идентификатора. Компетенције корисника са привилегованим правима на приступ се периодично преиспитују ради провере да ли су у складу са њиховим обавезама.
Забрањено је неовлашћено коришћење администраторских корисничких идентификатора.

Лозинке за администраторске корисничке налоге мењају се са променом администратора.

Дома здравља Ваљево једном годишње врши преиспитивање права корисника на приступ, као и након сваке промене (унапређење, разрешење и престанак статуса).

Члан 20.

Аутентификација корисника коме је одобрен приступ систему врши се путем његовог јединственог корисничког имена и лозинке.
Сви корисници су дужни да:

•Корисничко име и лозинку држе у тајности и не откривају их другим лицима, укључујући и надређене особе.
•Избегавају чување корисничког имена и лозинке у писаном облику.
•Промене лозинку увек када постоји било какав наговештај могућег компромитовања.
Лозинке морају да:
•садрже најмање 8 алфанумеричких знакова при чему у себи не смеју да садрже више од 3 узастопна идентична бројчана или словна знака,
•садрже комбинацију најмање три знака из следећих категорија: мало слово, велико слово, цифра и специјални знак.

Лозинке не смеју бити засноване на личним подацима особе, као што су име, телефонски број или датум рођења.
Корисници су дужни да привремене лозинке промене приликом првог пријављивања.

Физичко обезбеђење ИКТ система
Члан 21.

Дом здравља Ваљевоје дужан да предузме мере ради спречавања неовлашћеног физичког приступа просторијама у којима се налазе средства и документи ИКТ система, као и спречавање оштећења информатичке имовине.

Опрема за обраду информација се штити закључавањем просторија са двоја врата у којима се налази опрема и покривене су системом видео надзора и ПП сензорима. Просторије које садрже опрему за обраду информација заштићене су од спољних утицаја уз одржавање оптималне температуре у сервер соби Дома здравља Ваљево.

У радне просторије здравствених радника дозвољен је приступ свим запосленима.
У радне просторије Економско финансијске службе дозвољен је приступ само запосленима из поменуте службе. Такође у одређеним просторијама омогућен је рад са странкама – мисли се на благајне, људске ресурсе, правни послови и сл...

У серверску салу могу да уђу само овлашћена лица Дома здравља Ваљево.

Члан 22.

Запослени у Рачунарском центру редовно прати услове околине у серверској сали.
Опрема у серверској сали се штити од прекида напајања уградњом уређаја за непрекидно напајање који се редовно одржавају и проверавају у складу са спецификацијама произвођача.

У просторији је потребно обезбедити одговарајућу климатизацију простора. Радне температуре 25 степени.

Потребан је антистатик под, такође је потребно да се у просторију не одлажу други предмети – кутије и слично.

Одржавање опреме и заштита интегршпета информаиионих добара
Члан 23.

Рачунарска опрема се одржава како би се осигурале њена непрекидна расположивост и неповредивост. Уколико рачунарска опрема садржи осетљиве информације, а износи се ради сервисирања, онда се те информације уклањају пре сервисирања.

Опрема, информације или софтвер се измештају само уз одобрење Рачунарског центра, а током измештања се примењују следећа правила:
•Одредити запослене и спољне сараднике који имају овлашћење да врше измештање имовине.
•Поставити временска ограничења за измештање опреме и проверавање усклађености приликом повратка.
•Документовати идентитет и улогу лица која користе или поступају са имовином приликом премештања.
Приликом расходовања или поновног коришћења опреме која садржи медијуме за чување података, уклонити осетљиве податке и лиценцирани софтвер.
Корисници морају осигурати да опрема која је без надзора има одговарајућу заштиту, у циљу онемогућавања приступа заштићеним информацијама и подацима.

Члан 24.

Сва осетљива и поверљива документа и материјали морају да буду уклоњени са радне површине и одложени на одговарајуће место које се закључава, у периоду када запослени није присутан на свом радном месту или када се документа и материјали не користе.

Корисници ИКТ система Дома здравља Ваљево су уобавези да закључају радну станицу када је остављају без надзора.

Запослени у Рачунарском центру, у циљу обезбеђивања исправног и безбедног функционисања ИКТ система, обавезни су да поступају према радним процедурама за извршење следећих послова:

•Израда резервних копија база података.
•Процедуре за поновно покретање система и опоравак које се користе у случају отказа система.
•Надгледање активности на мрежи.
•Одржавање ажурног списка контаката за подршку (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа.

Резервне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја и треба их правити у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система.
За чување резервних копија користе се екстерни хард дискови и снимање на удаљеној локацији.

Рачунарски центар извршава следеће задатке:
•Процењује осетљиве и критичне податке за које је потребно правити резервне копије.
•Креира план прављења резервних копија.
•Верификује успешно прављење резервних копија.
•Води евиденцију урађених резервних копија.
•Одлаже копије на безбедно место.
•Периодично тестира исправност резервних копија и процедуре за прављење заштитних копија.
•Рестаурира податке са резервних копија.

За усвајање, измене и допуне радних процедура као и за заштиту од губитка података одговоран је Рачунарски центар.

Члан 25.

На опреми која је део ИКТ система Дома здравља Ваљево мора се инсталирати и одржавати софтверска заштита од злонамерног софтвера и софтверски алати за спречавање упада у ИКТ систем.

Заштита од злонамерног софтвера спроводи се у циљу заштите од вируса и друге врсте злонамерног софтвера који у рачунарску мрежу могу доспети путем интернета, елктронске поште, заражених преносних медијума, инсталацијом нелиценцираног софтвера и слично.

Забрањено је заустављање и искључивање антивирусног софтвера током скенирања радних станица или преносних медијума.
Преносиви медијуми, пре коришћења, морају бити проверени на присуство вируса. АКО се утврди да преносиви медијум садржи вирусе, уколико је то могуће, врши се чишћење медија антивирусним софтвером. Уколико чишћење није могуће, заражени медијум се не сме користити.

Ризик од евентуалног губитка података приликом чишћења медијума од вируса сноси доносилац медијума.

Корисницима ИКТ система је забрањено да самостално прикључују на систем уређаје који нису прошли проверу особља Рачунарског центра.

Недозвољена употреба интернета и рачунара обухвата:

•Коришћење и дистрибуцију нелиценцираног софтвера.
•Намерно ширење злонамерног софтвера.
•Преузимање огромне количине података којим се проузрокује загушење на мрежи.
•Неовлашћено преузимање материјала заштићених ауторским правима.
•Коришћење линкова који нису у вези са послом (гледање филмова, аудио и видеостреаминг и слично).
•Коришћење рачунара или компоненте ИКТ система Дома здравља Вљљево у приватне сврхе.

Корисницима ИКТ система, у случају доказане злоупотребе интернета, Рачунарски центар може укинути приступ.

У Дому здравља Ваљево 2019 године успостављен је Прокси сервер који води евиденцију о коришћењу и искоришћености интернет линка. Свака акција се чува у ЛОГ фајлу прокси сервера. Такође постављен је Микротик рутер са логом ин оут јавних адреса – и Доменски контролер тзв. „кец“ СРВ1

Члан 26.

Рачунарски центар чува и редовно преиспитује аутоматски генерисане записе о догађајима и бележи активности корисника, грешке и догађаје у вези са безбедношћу информација.

Систем за контролу и дојаву о грешкама и неовлашћеним активностима мора бити подешен тако да одмах обавештава администраторе ИКТ система о свим нерегуларним активностима корисника и о покушајима упада и упадима у систем.

Члан 27.

Дом здравља Ваљево спроводи поступке којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система.
Инсталацију и подешавање софтвера, на основу писменог захтева корисника, могу да врши само запослени у Рачунарском центру, односно корисник који има овлашћење за то добијено од стране Рачунарског центра.

Инсталацију и подешавање софтвера може да изврши и треће лице, у складу са Уговором о набавци, односно одржавању софтвера.
Приликом инсталације софтвера, лица која врше инсталацију морају да воде рачуна о могућности повратка на претходно стање.

Члан 28.

Дом здравља Ваљево врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима, и предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену мера заштите.
Запослени у Рачунарском центру благовремено прикупљају информације о техничким рањивостима информационих система који се користе, вреднују изложеност тим рањивостима и предузимају одговарајуће мере, узимањем у обзир припадајућих ризика.
Уколико се идентификују рањивости које могу да угрозе безбедност ИКТ система, запослени у Рачунарском центру су дужни да одмах изврше подешавања, односно инсталирају софтвер који ће отклонити уочене рањивости. Прво се узимају у разматрање системи са високим ризиком.
Забрањено је инсталирање софтвера који могу довести до изложености ИКТ система безбедносним слабостима.

Члан 29.

Приликом спровођења ревизије ИКТ система, Дом здравља Ваљево обезбеђује да ревизија има што мањи утицај на фукционисање система.
Ревизија ИКТ система врши се по потреби а при том се корисници о томе благовремено обавештавају. У правилу, ревизија се врши ван радног времена, осим када је у питању хитност потребе за њом.

Члан 30.

Комуникациони каблови и каблови за напајање морају бити постављени у зиду или каналицама, тако да се онемогући неовлашћен приступ, односно спречи могуће оштећење.
Активна мрежна опрема се мора налазити у закључаном орману.
Запослени у Рачунарском центру су у обавези да контролишу мрежну опрему и благовремено предузимају мере у циљу отклањања евентуалних неправилности.
Бежична мрежа коју могу да користе запослени,пацијенти и кориснициДома здравља Ваљево и друга лица мора бити одвојена од интерне мреже коју користе запослени и кроз коју се врши размена службених података.

Члан 31.

Коришћење рачунарске мреже Дома здравља Ваљево, система електронске поште и интернета врши се у складу са Правилником о општим правилима приступа и коришћења услуга провајдера „Телеком Србија".

Електронска пошта се може користити искључиво за пословне потребе. Није дозвољено корисничке налоге додељене за приступ ИКТ систему користити за регистровање на друштвеним мрежама и другим порталима (изузев портала којима се приступа због потреба посла).

Електронском поштом не смеју се слати подаци чија компромитација може да угрози безбедност ИКТ система Дома здравља Ваљево.

Сарадња са трећим лицима

Члан 32.

Споразуми о поверљивости или неоткривању штите информације Дома здравља Ваљево и обавезују потписнике да информације штите, користе и објављују их на одговоран и ауторизован начин.

Да би се идентификовали захтеви за споразуме о поверљивости или неоткривању, треба узети у обзир следеће елементе:

•Дефиницију информација које треба заштитити.

•Очекивано трајање споразума, укључујући случајеве у којима је потребно да се поверљивост сачува неограничено.

•Поступања које се захтевају по истеку споразума, попут повраћаја или уништавања информација.

•Право на проверу и праћење активности које укључују поверљиве информације.

•Радње које треба предузети у случају кршења овог споразума.

Члан 33.

Рачунарски центар је задужен за технички надзор над реализацијом уговорених обавеза од стране трећих лица.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система, запослени у Рачунарском центру воде документацију.

Документација из претходног става мора да садржи описе свих процедура а посебно процедура које се односе на безбедност ИКТ система.

Члан 34.

У захтеве за нове информационе системе или за побољшање постојећих информационих система морају бити укључени захтеви који се односе на безбедност информација и они су саставни део уговора о набавци, модификацији и одржавању информационог система.

Захтеви за безбедност информација укључују:

•Проверу идентитета корисника.

•Доступност, поверљивост, непорецивост и интегритет података и имовине.

•Надгледање пословних процеса.

•Омогућавање приступа за кориснике са различитим нивоима привилегије.

У уговору са набављачем за купљене производе дефинишу се захтеви безбедности, тестирања и имплементације.

Поступање у случају безбедносних инцидената

Члан 35.

У сврху опоравка ИКТ система од последица инцидената који угрожавају безбедност ИКТ система, запослени у Рачунарском центру су у обавези да:

•направе и воде ажурно документацију за сервисе, апликације и базе података;

•чувају резервне копије конфигурационих фајлова сервера. апликација и база података;

•чувају резервне копије података на најмање три локације (од којих бар једна мора бити на удаљеној локацији);

•воде податке о тиму који ће бити ангажован на отклањању последица нежељених догађаја.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, корисник је дужан да одмах обавести Рачунарски центар.

У случају погрешног функционисања или других аномалијских понашања система врши се исто извештавање као и у случају догађаја у вези са безбедношћу информација.

Корисник који сматра да је дошло до напада или злоупотребе података мора одмах припремити опис проблема и путем електронске поште или телефона обавестити Рачунарски центар.

Рачунарски центар врши проверу пријављеног инцидента и извршава активности на успостављању нормалног функционисања ИКТ система.

Рачунарски центар води евиденцију о свим инцидентима, као и пријавама инцидената, на основу којих се против одговорног лица могу водити дисциплински, прекршајни или кривични поступци.

II.ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 36.

Обавеза Дома здравља Ваљевоје да најмање једном годишње изврши проверу ИКТ система и изврши евентуалне измене Акта о безбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему Дома здравља Ваљево.

Ступањем на снагу Акта о безбедности, сваки неовлашћен рад на ИКТ опреми Рачунарски Центар је дужан да води евиденцију и користи прописане процедуре, такође сваки квар на опреми настао несавесним радом запосленог

Дом здравља Ваљево може покренути поступак за утврђивање одговорности на захтев одговорног лица, односно директора.

Члан 37.

Правилник о безбедности информационо-комуникационог система Дома здравља Ваљево ступа на снагу даном доношења, а примењиваће се осмог дана од дана објављивања на огласној табли и сајту Дома здравља Ваљево.

Објављено на огласној табли
17 ОСТ 2022

Председник Управног одбора
Борко Алексић