РЕГУЛАТОРНА КОМИСИЈА ЗА ЕНЕРГЕТИКА И ВОДНИ УСЛУГИ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Врз основа на член 30-а став (4) од Законот за енергетика („Службен весник на Република Македонија“ бр. 96/18 и „Службен весник на Република Северна Македонија“ бр. 96/19 и 236/22), Регулаторната комисија за енергетика и водни услуги на Република Северна Македонија, на седницата одржана на 08.06.2023 година, донесе

ПРАВИЛА ЗА САЈБЕР БЕЗБЕДНОСТ

Член 1
Предмет на уредување

Со овие Правила за сајбер безбедност се пропишуваат обврските за обезбедување сајбер безбедност и техничките и организациските услови за:

1) назначување службеник за сајбер безбедност и неговите овластувања и задачи;
2) определување на критичната инфраструктура во енергетскиот сектор за која Регулаторната комисија за енергетика и водни услуги на Република Северна Македонија (во натамошниот текст: Регулаторна комисија за енергетика) ќе утврди приоритет во обезбедувањето на сајбер безбедност;
3) доставувања на известувања за откриени сајбер безбедносни напади и инциденти доРегулаторната комисија за енергетика, до другите оператори и производители и до надлежното национално тело за одговор на сајбер инциденти;
4) изготвување и примена на методологијата за проценка на ризици од сајбер напади и инциденти и на оперативните планови за превенција и реакција на сајбер напади и инциденти;
5) воведување на меѓународните стандарди за безбедност на мрежите, информатичка безбедност и сајбер безбедност според кои се сертифицираат соодветните оператори и производители;
6) дефинирање на мерките и активностите за спречување и/или намалување на ризиците од сајбер напади и инциденти;
7) определување на начинот и постапката за проверка на безбедноста на применетите информациски системи;
8) дефинирање на барањата кои треба да ги исполнат новите и постојните уреди поврзани со интернет или кои се користат во мрежите и системите кои применуваат оперативни технологии;

9) изготвување и примена на програмата за спроведување обуки за вработените за сајбер безбедност;
10) препознавање на ризиците и изготвување на мерките и активностите за спречување и/или намалување на ризиците од сајбер напади и и инциденти предизвикани од домино ефектите во поврзаните мрежи, и
11) определување на роковите за исполнување на обврските пропишани со Правилата.

Член 2
Дефиниции

(1) Дефинициите за одделни изрази, содржани во Законот за енергетика, се применуваат и во овие Правила.

(2) Одделни изрази употребени во овие Правила го имаат следното значење:

1) **„Критична инфраструктура“** се објекти, системи и опрема кои, доколку се уништат, нарушат или на друг начин станат недостапни, би влијаеле на доверливоста или оперативноста на целиот енергетски систем;

2) **„Критична национална инфраструктура“** се средствата, системите и мрежите, кои може да бидат физички или виртуелни и кои се од суштинско значење за државата и нивното онеспособување или уништување ќе предизвика загрозување на општата безбедност, националната економска безбедност, јавното здравје или комбинација од било кои од наведените;

3) **„Сајбер напад“** е обид за инфилтрирање во информатичките системи, компјутерските мрежи или поединечни компјутери со намера да се украдат информации, да се предизвика штета или да се уништат одредени цели во системот;

4) **„Сајбер-безбедносен инцидент“** е настан што се случува на или е спроведен преку компјутерска мрежа што фактички или непосредно го загрозува интегритетот, доверливоста или достапноста на компјутерите, информациските или комуникациските системи или мрежи, физичката или виртуелната инфраструктура контролирана од компјутери или информациски системи, или информациите што се наоѓаат на нив. Сајбер-безбедносниот инцидент може да вклучува ранливост на информацискиот систем, како и на процедурите за безбедност на системот, внатрешните контроли или имплементацијата што може да биде искористена од изворот на закана;

5) **„Сајбер безбедност“** е способност да се заштити или одбрани сајбер-просторот од сајбер напади;

6) **„Модел за сајбер-безбедносна подготвеност (Cybersecurity Capability Maturity Model)“** е модел кој им помага на правните лица, независно на нивната големина, вид или дејноста која ја вршат да направат проценка, да определат приоритети и да ја подобрат сопствената сајбер безбедност.

7) **„Тестирање преку пенетрација“** е симулирање, односно намерно предизвикување на сајбер напади користејќи стратегии и алатки дизајнирани за пристап или искористување на компјутерски системи, мрежи, веб-локации и апликации;

8) **„Отпорност“** е способност за претходно подготвување и приспособување на променливите услови и издржливост и брзо опоравување од прекини. Отпорноста вклучува способност за издржливост и опоравување во случај на намерни напади, несреќи или природни закани или инциденти;

9) **„Ризик“** е потенцијалот за несакан исход како резултат на инцидент, настан или појава, определен од веројатноста да настане и од предизвиканите последици;

10) **„Справување со ризици“** е процес на контрола на ризиците за организациските операции (вклучувајќи ги мисијата, функциите, имиџот, репутацијата) и средства, поединците, другите организации и државата, и вклучува: спроведување на проценка на ризикот, утврдување и спроведување на стратегија за намалување на ризикот и примена на технички мерки и процедури за континуирано следење на спроведените заштитни мерки.

Член 3
Примена на Правилата

Овие Правила ги применуваат операторите на електропреносниот и електродистрибутивниот систем (во натамошниот текст: оператори), и производителите на електрична енергија кои управуваат со електроцентрали со вкупна инсталирана моќност еднаква или поголема од 200 MW (во натамошниот текст: производители).

Член 4
Одговорно лице за сајбер безбедност

(1) Операторите и производителите се должни да назначат службеник за сајбер безбедност (во натамошниот текст: Одговорно лице за сајбер безбедност) и одлуката за негово назначување да ја достават до Регулаторната комисија за енергетика.

(2) За Одговорно лице за сајбер безбедност се назначува лице кое:

1) во моментот на определувањето со правосилна судска пресуда не му е изречена казна или прекршочна санкција забрана за вршење на професија, дејност или должност,
2) има завршено високо образование во областа на информатичките технологии, електротехниката или правото,
3) има познавања за дигиталните технологии и системите за прибирање и обработка на податоци и за контрола на процесите во енергетиката, и
4) има најмалку 3 години работно искусво во управувањето со соодветни информатички технологии (ИТ) или оперативни технологии (ОТ) и во нивната сајбер безбедност.

(3) Знаењата и вештините од ставот (2) точка 4) на овој член се докажуваат со сертификати или други докази за завршени обуки и за стекнато работно искуство.

(4) За Одговорно лице за сајбер безбедност може да биде назначено лицето кое е Лице за контакт во кризни и вонредни состојби („Liaison Officer“) или Одговорно лице за информатичка безбедност („Chief Information Security Officer“ – CISO), ако таквите лица ги исполнуваат условите од ставовите (2) и (3) од овој член.

(5) По потреба, одговорното лице за сајбер безбедност кај операторите и производителите ги извршува задачите од овие Правила со користење на услуги од надлежното национално тело за одговор на сајбер инциденти или други субјекти кои даваат услуги во областа на сајбер безбедноста.

(6) Задачите и овластувањата на Одговорното лице за сајбер безбедност вклучуваат, но не се ограничени на организација, координација и одговорност за извршување на следното:

1) спроведување и/или надзор на соодветната примена на одредбите содржани во овие Правила, други подзаконски акти и интерни акти,
2) следење и примена на меѓународни технички стандарди и правила, прописи и регулативи за сајбер безбедност;
3) изработка и спроведување на сајбер безбедносна програма која ќе опфати политики, процедури и мерки за заштита од сајбер напади и зголемување на сајбер отпорноста наИТ и ОТ,
4) откривање на структурни и системски слабости и ризици во информациско-комуникациските системи и мрежи, какои во физичката и виртуелната инфраструктура,
5) дефинирање на сценарија и процена на ризици по сајбер безбедноста во процесот на воспоставување на систем за управување со ризици,
6) редовно следење на ранливоста на системите, следење и проценка на актуелните опасности кон мрежните податоци и воведување мерки за ублажување на последиците од сајбер инциденти,
7) обезбедување на ажурирање на хардверските уреди и софтверските апликации,
8) координација во справувањето со потенцијалните сајбер напади и инциденти преку

учество во преземање мерки за заштита на системите,

9) комуникација со раководните лица и останатите единици, како и со други засегнати субјекти за прашања од сајбер безбедноста во енергетиката, и
10) редовна комуникација и координација со Регулаторната комисија за енергетика и надлежното национално тело за одговор на сајбер инциденти.

Член 5

Критична национална инфраструктура и критична инфраструктура

(1) Операторите и производителите до Регулаторната комисија за енергетика ги предлагаат објектите, опремата и средствата кои според нивна оцена претставуваат критична инфраструктура.

(2) Регулаторната комисија за енергетика, врз основа на претходно спроведена анализа и податоците за објектите, системите и опремата добиени од операторите и производителите, како и според критериумите од стратешките, планските и развојните документи во енергетскиот сектор, донесува одлука за определување на критична инфраструктура.

(3) Во постапката за утврдување на критична национална инфраструктура (во натамошниот текст: „КНИ“), Регулаторната комисија за енергетика доставува предлог за определување КНИ во енергетиката до надлежниот орган, согласно закон.

(4) Регулаторната комисија за енергетика до операторите и производителите ги доставува информациите за определената критичната инфраструктура, вклучително и за КНИ. Во критичната инфраструктура може да се смета, ако е потребно, и онаа на поврзаните друштва, како и друштвата кои се суштински во синџирот на снабдување.

(5) Оператори и производители ја категоризираат критичната инфраструктура и КНИ со градација во приоритетот и динамиката на примена на мерките за нејзина сајбер безбедност и сертифицирање според стандард.

(6) Оператори и производители кои имаат обврска за вршење на јавна услуга ги внесуваат соодветните трошоци за примена на мерките од став (5) на овој член во пресметката на тарифата или цената на енергијата или услугата, кои како предлог ги доставуваат до Регулаторната комисија за енергетика.

Член 6

Следење, известување и справување со сајбер напади и инциденти

(1) Операторите и производителите воспоставуваат мерки и активности за следење на сајбер

нападите кои се однесуваат на откривање на сајбер напади, утврдување на резултатите од нападот и проценка на каква било штета што резултирала или може да резултира од нападот.

(2) Операторите и производителите:
   1) ги внесуваат податоците за откриените сајбер инциденти на образец даден во Прилог 1 кој е составен дел на овие Правила, и
   2) врз основа на податоците од пополнетиот образец за сајбер инцидент, водат евиденција за сите откриени сајбер инциденти.

(3) Операторите и производителите доставуваат резиме на евиденцијата за сајбер инциденти до Регулаторната комисија за енергетика на квартална основа, најдоцна до петтиот ден од тековниот месец за претходните три месеци. Регулаторната комисија за енергетика ги доставува резимеата на евиденциите за сајбер инциденти до надлежното национално тело за одговор на сајбер инциденти.

(4) Ако операторот или производителот проценил дека сајбер нападот или инцидентот:

   1) резултирал со сериозна штета или предизвикал прекин на преносот, дистрибуцијата и/или снабдувањето со енергија, или
   2) може да предизвика сериозни последици по оперативното работење на други оператори или производители,

   ги пријавува деталите за сајбер нападот и предизвиканата штета до Регулаторната комисија за енергетика и до надлежното национално тело за одговор на сајбер инциденти во рок од 24 часа од настанувањето, односно откривањето и ги следи добиените упатства заради справување со сајбер нападите или отстранување на штетните последици.

(5) Регулаторната комисија за енергетика го координира споделувањето на информации за пријавените сајбер напади со останатите засегнати субјекти во енергетскиот сектор, како и со надлежното национално тело за одговор на сајбер инциденти.

Член 7

Деловен континуитет и отпорност

(1) Операторите и производителите воспоставуваат планови за деловен континуитет, односно отпорност со цел ублажување на штетата што може да резултира од сајбер нападите.

(2) Регулаторната комисија за енергетика, во соработка со надлежното национално тело за одговор на сајбер инциденти и со операторите и производителите, ќе изготви, усвои и објави референтен модел со методологија за оценување на сајбер отпорноста на системите и сајбер-безбедносната подготвеност на операторите и производителите.

(3) Врз основа на методологијата од став (2) на овој член, операторите и производителите вршат самооценување на сајбер-отпорноста на инфраструктурата и доставуваат годишни извештаи до Регулаторната комисија за енергетика.

(4) Операторите и производителите кои биле погодени од сајбер напади го пријавуваат степенот на оперативност на објектите, системите и средствата и ефикасноста во обезбедувањето на услугите коишто се прекинати или се уште се во прекин, до Регулаторната комисија за енергетика и надлежното национално тело за одговор на сајбер инциденти, најмалку еднаш неделно сѐ додека оперативноста или обезбедувањето на услугата не се обнови во целост.

Член 8
Модел за сајбер безбедносна подготвеност

(1) Операторите и производителите воспоставуваат и применуваат модел за сајбер безбедносна подготвеност согласно овој член и насоките на Регулаторната комисија за енергетика.

(2) Операторите и производителите можат да користат модел за сајбер-безбедносна подготвеност кој е различен од моделот утврден од Регулаторната комисија за енергетика, под услов да изготват критериуми кои овозможуваат единствена примена и споредба на сајбер-безбедносната подготвеност на сите субјекти.

(3) Операторите и производителите воспоставуваат и применуваат мерки и активности неопходни за операционализација на моделот за сајбер-безбедносна подготвеност.

(4) Известувањето за моделот на сајбер-безбедносна подготвеност претставува составен дел од процесот на внатрешна ревизија согласно стандардот ISO 27001.

Член 9
Известување за извршена самоевалуација на сајбербезбедносна подготвеност

(1) Операторите и производителите вршат самоевалуација според моделот за сајбер-безбедносна подготвеност еднаш годишно.

(2) Операторите и производителите изработуваат извештаи со резултатите од самоевалуацијата според моделот за сајбер-безбедносна подготвеност.

(3) Врз основа на резултатите од самоевалуацијата, операторите и производителите изработуваат имплементациски план со предлог мерки за подобрување на сајбер-безбедносната

подготвеност и рокови за нивна реализација.

(4) Операторите и производителите ги доставуваат извештаите од ставот (2) и имплементациските планови од ставот (3) на овој член до Регулаторната комисија за енергетика, во рок од 15 дена од денот на нивното усвојување.

(5) Операторите и производителите, како и Регулаторната комисија за енергетика обезбедуваат соодветно ниво на заштита на извештаите од ставот (2) и имплементациските планови од ставот (3) на овој член.

(6) Ако со имплементациските планови од став (3) на овој член, операторите и производителите со обврска за обезбедување јавна услуга предвидуваат примена на мерки кои налагаат дополнителни инвестиции, Регулаторната комисија за енергетика ги зема предвид при определување на тарифите.

Член 10

Имплементација на стандардот ISO 27001

(1) Операторите и производителите се сертифицираат и го имплементираат стандардот ISO 27001 за управување со безбедноста на информациите.

(2) Во опфатот на стандардот ISO 27001, операторите и производителите треба да вклучат и составување и одржување на инвентар (попис, каталог) на средствата кои се дел од оперативните системи и/или информациските системи.

(3) Сертификацијата според стандардот ISO 27001 го врши надворешно акредитирано лице.

(4) Операторите и производителите ја обновуваат сертификацијата според стандардот ISO 27001 на секои три години.

Член 11

Имплементација на пристап за сајбер безбедност заснован на ризик

(1) Операторите и производителите воспоставуваат и применуваат повторлив процес на управување со сајбер безбедносни ризици.

(2) Операторите и производителите вршат проценка на сајбер безбедносниот ризик еднаш годишно, како и по секој успешно извршен сајбер напад или инцидент кој резултирал со сериозна штета или прекин во извршување на функциите.

Член 12
Регистар на ризици

(1) Секој оператор и производител води регистар на ризици за сајбер безбедноста на образец даден во Прилог 2 кој е составен дел од овие Правила.

(2) Ризиците се внесуваат во регистарот на ризици за сајбер безбедноста по претходно извршена проценка во која се идентификувани ризиците.

(3) Ризиците во регистарот на ризици за сајбер безбедноста се бодуваат врз основа на влијанието, веројатноста и последиците доколку ризикот се реализира и се приоретизираат според критериумите дадени во Прилог 3 кој е составен дел на овие Правила.

(4) Операторите и производителите ги ажурираат регистарите на ризици по секоја извршена проценка на сајбер безбедносниот ризик.

(5) Секој оператор и производител поднесува извештај до Регулаторната комисија за енергетика кој содржи резиме на регистарот на ризици за сајбер безбедноста по секоја извршена проценка на сајбер безбедносниот ризик.

(6) Врз основа на извештаите од став (5) на овој член, Регулаторната комисија за енергетика воспоставува и одржува единствен регистар на ризици за сајбер безбедноста во енергетиката, кој се ажурира по секој добиен извештај.

(7) Регулаторната комисија за енергетика овозможува пристап до податоците од единствениот регистар на ризици за сајбер безбедноста во енергетиката на надлежните национални и меѓународни тела за одговор на сајбер инциденти.

Член 13
Мерки за обезбедување сајбер безбедност

(1) Операторите и производителите определуваат и применуваат превентивни мерки за обезбедување сајбер безбедност, односно за заштита на едно или повеќе средства од сајбер напад.

(2) Операторите и производителите:

1) воспоставуваат постојана периметарска заштита од добро познати напади и напади со притаена автоматска активација и со „нула денови“ (zero - day) на потенцијална ранливост, кои одговорното лице за сајбер безбедност и другите стручни лица редовно ги следат и информираат со цел навремено откривање на потенцијални злонамерни активности на

критичната инфраструктура,
2) воспоставуваат и одржуваат активна заштита на индустриските контролни системи врз основа на SCADA системот,
3) вршат анализа на ранливоста и воспоставуваат соодветни системи за прилагодена сајбер заштита на оперативните системи со постара или аналогна технологија кои се во употреба и се надградени со елементи на дигитална технологија,
4) користат технологија за еднонасочен пренос на податоци за издвоени системи каде што таква технологија е применлива,
5) овозможуваат целосна видливост на мрежата, системите, крајните точки и индустриските контролни системи со цел детекција и превенција од потенцијални сајбер напади и соодветен одговор на истите преку имплементација на решение за следење и справување со злонамерни активности од надворешна мрежа (интернет) и внатрешна мрежа (интранет),
6) имплементираат централен систем за следење на отворени случаи од моментот на нивното отворање до моментот на нивното решавање и затворање, и
7) имплементираат централен систем за собирање на настани и активности од сите системи и мрежни елементи на централна локација (СИЕМ решение).

(3) Мерките за сајбер безбедност се избираат врз основа на извршената проценка на ризикот, потенцијалната последица и преостанатиот ризик по примената на мерката.

(4) Во регистарот на ризици за сајбер безбедноста се дава опис на секоја избрана и воведена мерка за сајбер безбедност, контрола и ублажување на ризикот и преостанатиот проценет ризик.

Член 14
Следење на мерките за сајбер безбедност

(1) Операторите и производителите воспоставуваат процедура за следење на ефикасноста на секоја имплементирана мерка за сајбер безбедност, од започнувањето на спроведување на мерката.

(2) Операторите и производителите водат евиденција за преземените мерки за обезбедување сајбер безбедност, како и за нивната надградба, замена или можно прекинување.

Член 15
Тестирање преку пенетрација

(1) Операторите и производителите вршат тестирање преку пенетрација заради утврдување на отпорноста од сајбер напади на системите, апликациите и мрежата, најмалку еднаш годишно и за добиените резултати од тестирањето ја известуваат Регулаторната комисија за енергетика.

(2) При тестирањето преку пенетрација се зема предвид инвентарот на средства дефинирани во опсегот на стандардот ISO 27001.

Член 16
Нови уреди и апликации

(1) Операторите и производителите воспоставуваат и применуваат процедури за утврдување на безбедноста на секој нов хардверски уред и софтверска апликација пред да го додадат во своите оперативни системи и информациски системи.

(2) За утврдување на безбедноста на нов хардверски уред и софтверска апликација се применуваат следните критериуми релевантни за предвиденото ниво на сајбер безбедност:

1) реномираноста (нивото на општата познатост) на производителот на уредот или апликацијата и достапноста на услугите за одржување и надградба,
2) стандардите за квалитет применети на уредот или апликацијата,
3) докажаните и познатите пропусти на уредот или апликацијата,
4) крајот на животниот век / застареноста на уредот или апликацијата,
5) транспарентното објавување на резултатите од тестирањето на уредот или апликацијата, и
6) вградените безбедносни карактеристики и актуелната верзија на уредот или апликацијата.

(3) Во оперативните системи и информациските системи на операторите и производителите можат да бидат додадени само хардверски уреди и софтверски апликации кои се соодветно проверени и чијашто сајбер безбедност е претходно утврдена.

Член 17
Обука и комуникација

(1) Операторите и производителите изготвуваат и спроведуваат програма за континуирана обука на вработените во сајбер безбедноста со цел унапредување на сајбер безбедноста во оперативното работење.

(2) Програмата особено содржи:

1) основите на сајбер безбедноста – за сите вработени
2) основите на сајбер безбедноста - за раководните лица,
3) основни начини и мерки за обезбедување на сајбер безбедност од секое вработено лице,
4) сајбербезбедност на критичната инфраструктура,
5) основи на стандардот ISO 27001,
6) напредни аспекти на стандардот ISO 27001 – наменета за лицата за информатичка

безбедност, и
7) проценка на ризици.

(3) Операторите и производителите воспоставуваат и применуваат процедури за редовно информирање на своите вработени за прашања од сајбер безбедноста.

Член 18

Континуирано ревидирање

(1) Операторите и производителите воспоставуваат и применуваат процедури за континуирано ревидирање на постоечките мерки за сајбер безбедност со цел нивно постојано подобрување.

(2) Операторите и производителите водат евиденција на иницијативите за континуирано ревидирање и подготвуваат годишен план за сајбер безбедност кој го доставуваат до Регулаторната комисија за енергетика најдоцна до 31 март.

Член 19

Преодни одредби

(1) Регулаторната комисија за енергетика го усвојува и објавува референтниот модел со методологија за оценување на сајбер отпорноста на системите и сајбер-безбедносната подготвеност на субјектите во енергетиката во рок од шест месеци од денот на влегувањето на сила на овие Правила.

(2) Регулаторната комисија ги пропишува насоките за моделот за сајбер-безбедносна подготвеност во рок шест месеци од денот на влегувањето на сила на овие Правила.

(3) Операторите и производителите назначуваат одговорно лице за сајбер безбедност во рок од 60 дена од денот на влегувањето во сила на овие Правила.

(4) Операторите и производителите ги носат програмите и плановите и ги воспоставуваат регистрите и евиденциите пропишани со овие Правила во рок од девет месеци од денот на влегувањето во сила на овие Правила.

(5) Операторите и производителите се сертифицираат според стандардот ISO 27001 во рок од 18 месеци од денот на влегувањето во сила на овие Правила.

Член 20
Завршна одредба

Овие правила влегуваат во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Претседател на Регулаторна комисија за енергетика
и водни услуги
на Република Северна Македонија

Марко Бислимоски

Бр. 01-1324/1
08 јуни 2023 година
Скопје

ПРИЛОГ 1

Образец за пријавување на сајбер инцидент		
Инцидент #:	Организација:	Датум:
Титула:		
Име на лицето за контакт:	Адреса за е-пошта:	Телефон:
Локација:		
Опис:		
Време на почеток на инцидентот:		
Времетраење на нарушувањето:		
Начин на кој е откриен инцидентот:		
Време за откривање на настанот:		
Време за утврдување на нарушувањето:		
Време за регулирање на нарушувањето:		
Време за опоравување од нарушувањето:		
Вкупен број на засегнати корисници:		
Географска распространетост:		
Обемот на нарушувањето:		
Степен на влијание врз економските и општествените активности:		
Напаѓач:		
Штета:		
Влијание:		
Цел:		
Жртва:		
Ранливост:		
Докази:		
Реакција:		
Исход:		

ПРИЛОГ 2

РЕГИСТАР НА РИЗИЦИ

Ризик	Причина (Ранливост)	Влијание	Веројатност	Исход	Ниво на ризик	Трошок	Ублажување

ПРИЛОГ 3

КРИТЕРИУМИ ЗА ОПРЕДЕЛУВАЊЕ НА НИВОТО НА РИЗИК

НИВО НА РИЗИК	ОПИС
КРИТИЧНО	Проблеми со висок степен на сериозност кои можат да бидат злоупотребени изолирано без потребни дополнителни чекори и кои можат да предизвикуваат целосно компромитирање насистемот
НИСКО	Безбедносни прашања кои имаат ограничено или тривијално влијание врз околината
СРЕДНО	Умерени безбедносни прашањакои бараат одреден напор за успешно влијание врз околината
ВИСОКО	Сериозни проблеми кои лесно може да се искористат за веднаш да влијаат на околината