|  |  |  |  |
| --- | --- | --- | --- |
| **ПРЕДСТАВИТЕЛИ НА МИНИСТРИТЕ** | CM документи | **CM(2022)10-окончателен** | 9 февруари 2022 г |

|  |
| --- |
|  |

|  |
| --- |
| **1424 -то заседание, 9 февруари 2022 г.**  2 Актуални политически въпроси    **2.4 Европейски комитет по демокрация и управление (ЕКДУ)**  б. Насоки на Комитета на министрите относно използването на информационни и комуникационни технологии (ИКТ) в изборните процеси в държавите-членки на Съвета на Европа |

**Насоки на Комитета на министрите относно използването на информационни и комуникационни технологии (ИКТ) в изборните процеси в държавите-членки на Съвета на Европа**

**Въведение**

Свободните и честни избори и референдуми са един от крайъгълните камъни на демокрацията. Почтеността на изборния процес е от основно значение за поддържането на общественото доверие в легитимността на демократичните институции.

Налице е актуална тенденция все повече да се разчита на информационни и комуникационни технологии (ИКТ) във всички сфери на живота, включително в изборната администрация. Тези насоки имат за цел да допринесат за гарантиране на почтеността на изборния процес и следователно за повишаване на доверието на гражданите в демокрацията. Насоките определят изискванията и предпазните мерки, които да бъдат въведени в законодателството на държавите-членки на Съвета на Европа, за да се обърне внимание на използването на ИКТ в различните етапи на изборния процес.

**Обхват на насоките**

Държавите могат да изберат да използват ИКТ решения за обработка на изборни данни и процеси като:

−     регистри и регистрация на избиратели, наблюдатели, медии и др.;

−     събиране на електронни подписи в подкрепа на въпроси (например инициативи или петиции), кандидати или партии;

−     онлайн публикуване на информация, свързана с избори;

−     електронното предаване на изборни данни между местните, регионалните и централните избирателни органи;

−     онлайн обучение на избoрния персонал и други заинтересовани страни или електронното акредитиране на наблюдатели;

−     определянето, обработването, предаването и публикуването на изборни резултати;

−     наблюдението на различни дейности, свързани с изборите и др.

Освен това бяха обсъдени ИКТ решения в контекста на пандемията от Covid-19, тъй като редовното провеждане на изборния процес беше засегнато.

Електронните данни и електронните процеси могат да подобрят упражняването на политически права, като предложат например по-добра достъпност, повече възможности за взаимодействие и повишена прозрачност. Може да има и предимства за изборната администрация по отношение на бързина, ефективност или точност. В същото време прилагането и използването на ИКТ също увеличава сложността и повишава излагането на заплахи и рискове, присъщи на използваните ИКТ решения или системи.

Тези насоки обхващат използването на ИКТ решения от или от името на съответните избирателни органи на всички етапи от изборния процес с изключение на електронното гласуване и електронното преброяване, които са обхванати от [CM/Rec(2017)5](https://search.coe.int/cm/Pages/result_details.aspx?Reference=CM/Rec(2017)5) относно стандартите за електронно гласуване и следователно са извън обхвата на тези насоки. Въпреки това хибридните форми на преброяване, които използват някои ИКТ, но не попадат в определението за електронно гласуване съгласно [CM/Rec(2017)5](https://search.coe.int/cm/Pages/result_details.aspx?Reference=CM/Rec(2017)5) , са обхванати от настоящите насоки. Използването на ИКТ от други лица в контекста на изборния процес, а именно дейности по провеждане на кампании като политически микротаргетинг от политически партии или информация, предоставена от медии, не се разглежда от тези насоки.

**Основни принципи на демократичните избори и референдуми**

Използването на ИКТ, подобно на използването на всяка друга технология в изборните процеси, трябва да е в съответствие с принципите на демократичните избори и референдуми и други съответни принципи и трябва да бъде балансирано спрямо други основни съображения като сигурност и достъпност за потребителите.

Демократичните избори и референдуми трябва да се провеждат в съответствие с определени принципи, които им дават демократичен статут. Кодексът на добрите практики по изборни въпроси на Европейската комисия за демокрация чрез право (Венецианската комисия), [1] приет през 2002 г., е референтният документ на Съвета на Европа в тази област. Той определя „европейското избирателно наследство“ от два аспекта: основните конституционни принципи на избирателното право и някои основни условия, необходими за тяхното прилагане.

В съответствие с Кодекса за добри практики по изборни въпроси от 2002 г. значението на основните избирателни принципи и условия може да се обобщи, както следва:

−              „всеобщо избирателно право“: всички хора имат право да гласуват и да бъдат избирани при определени условия, като възраст, националност или местожителство;

−              „равно избирателно право“: всеки избирател има еднакъв брой гласове; всеки глас има еднаква тежест и трябва да се осигурят равни възможности;

−              „свободно избирателно право“: избирателят има право да формира и изразява своето мнение по свободен начин, без принуда или неправомерно влияние;

−              „тайно избирателно право“: избирателят има право да гласува тайно като физическо лице, а държавата е длъжна да защитава това право;

−              „пряко избирателно право“: подадените от избирателите бюлетини пряко определят избраното(ите) лице(а);

−              „честота на изборите“: изборите трябва да се провеждат на редовни интервали;

−              „зачитане на основните права“: демократичните избори изискват зачитане на правата на човека, като свобода на изразяване, свобода на движение, свобода на събрания и свобода на сдружаване;

−              „регулаторни нива и стабилност на избирателното право“: правилата на избирателното право трябва да имат поне ранг на закон; правила по технически въпроси и подробности могат да бъдат включени в наредбите на изпълнителната власт. Основните елементи на изборния закон не трябва да подлежат на изменение по-малко от една година преди избори или трябва да бъдат записани в конституцията или на ниво, по-високо от обикновения закон;

−              „процедурни гаранции“: те включват процедурни гаранции, насочени към осигуряване на организирането на избори от безпристрастен орган, наблюдение на изборите от национални и международни наблюдатели и ефективна система за обжалване, наред с други неща;

Тези насоки са общи и са предназначени за всяко използване на ИКТ в предвидените етапи на изборния процес. В допълнение към основните избирателни принципи и зачитането на основните права, демократичните избори и референдумите следва да отговарят на всички други приложими правни принципи. Те включват съответните международни задължения, препоръки и стандарти, а именно относно изборите и ИКТ, като споменатите в преамбюла на Препоръка [CM/Rec(2017)5](https://search.coe.int/cm/Pages/result_details.aspx?Reference=CM/Rec(2017)5) относно стандартите за електронно гласуване. Освен това съответните правни принципи могат да бъдат намерени на национално и поднационално ниво.

Освен това сигурността (на данните и системата) трябва да се разглежда като един от водещите принципи, който информира за проектирането, разработването и внедряването на ИКТ решения на всички етапи от изборния процес, като по този начин се гарантира ориентиран към човека подход на изначално проектирана сигурност. Например, осигуряването на цялостност и автентичност, наличност и надеждност, секретност и поверителност, както и използваемост и достъпност предполага, че системата и информацията са защитени срещу потенциални рискове, които биха компрометирали тези цели. Следователно всяка оценка на риска трябва да бъде съобразена с фазата на изборния цикъл, за която се отнася. Провеждането на непрекъснато управление на риска въз основа на предварително определени критерии за приемане на риск и предварително определена методология е важна част от усилията за гарантиране на сигурност. Използваните ИКТ решения трябва да бъдат най-съвременни и да се основават на рецензирани алгоритми и концепции, които са широко одобрени от съответната научна общност. Това може да увеличи доверието в процеса.

Интердисциплинарността е силно препоръчителна при регулиране на използването на ИКТ решения в изборния процес, тъй като влияе положително върху качеството на регулирането. Освен това насоките се основават на поуките, извлечени от използването на електронно гласуване и електронно преброяване от държавите-членки, както и на добри практики.

**Общи насоки, приложими за всички разглеждани етапи от изборния процес**

В следващите насоки „държава-членка“ се отнася до органа, който отговаря за регулирането, провеждането или надзора на въпросния изборен процес. Обикновено, но не винаги, се отнася до органа за управление на изборите на местно, регионално или централно ниво. Може да се отнася и за други публични институции като парламента или правителството, според случая.

***1. Държавите-членки следва да гарантират, че ИКТ решенията зачитат принципите на демократичните избори и референдуми и че се обръща достатъчно внимание на други съответни принципи.***

Трябва да се идентифицират общи правни принципи, които се прилагат към различните фази на изборния процес. Често не е възможно – дори и с базирани на хартия или на ръчна обработка решения – да се приложат всички принципи в еднаква степен. Това може да се дължи на две основни причини:

1.             може да има реален или предполагаем конфликт между принципите (например между поверителността и защитата на данните от една страна и прозрачността от друга), за които трябва да се определи балансирано ниво, което да бъде осигурено на всеки от тях.

2.             Решенията, независимо дали са на хартиен носител и на ръчна обработка или базирани на ИКТ, обикновено разчитат на допускания (като допускания за взаимодействието на потребителите помежду им или с ИКТ, или допускания за способността на потенциалните атаки). Само ако тези допускания са верни, принципите и производните изисквания могат да бъдат гарантирани. Ако допусканията не са реалистични, много е вероятно принципите да бъдат компрометирани и/или нарушени.

Следователно, освен идентифицирането на общите правни принципи, които се прилагат, е важно да се определи минималното ниво, до което те трябва да бъдат гарантирани. Освен това допусканията трябва да се анализират като част от редовната оценка на риска (вижте Насока 9) и трябва да се обърне достатъчно внимание на съображенията за сигурност.

Подробните правни и технически изисквания, които се прилагат към ИКТ решенията, трябва да бъдат извлечени от идентифицираните правни принципи. Трябва да се определят съответните минимални нива, до които те трябва да бъдат осигурени. Техническите изисквания трябва да включват функционални и нефункционални изисквания (например изисквания за поддръжка и оперативна съвместимост в допълнение към тези относно сигурността, използваемостта и достъпността), както и допускания. За техническите изисквания трябва да се посочи кои допускания са приемливи и кои не (обикновено, защото не са реалистични). Дефиницията на минималните нива трябва да включва списък с допускания. Техническите изисквания и допускания трябва да бъдат написани по технологично неутрален начин.

Процесът на разработване и вземане на решения за извеждане на технически изисквания, включително минимални нива и допускания, които биха могли да бъдат приемливи, трябва да бъде документиран, да включва информация за участващите хора (най-вероятно интердисциплинарен екип) и да бъде публично достъпен, като се гарантира прозрачен процес.

Регламентът следва да посочва какви жалби и механизми за разрешаване на спорове са налични във връзка с използването на ИКТ решения и следва да урежда как да се справят с евентуални искове за нередности.

***2. Държавите-членки следва да гарантират използваемостта и достъпността на ИКТ решенията, използвани в изборния процес, като прилагат подход, ориентиран към човека.***

Критериите за използваемост на ИКТ решенията са дефинирани например в стандарт ISO 9241. [2] Потребителските интерфейси, предназначени за по-широки групи от хора, особено гласоподаватели, трябва да бъдат проектирани, като се следват по-строги критерии от тези, предназначени за малки групи експертни потребители, като например длъжностни лица, свързани с изборния процес. Изискванията за достъпност трябва да вземат предвид нуждите на потребителите и да гарантират, че ИКТ решенията са достъпни за всички хора (независимо дали имат увреждане или не). Така използваемостта и достъпността се допълват взаимно. Правните и технически изисквания за използваемост и достъпност и минималното ниво, до което изискванията трябва да бъдат изпълнени, трябва да бъдат определени съгласно Насока 1. Тази втора насока се занимава с процеса на разработка.

При разработването на ИКТ решения за използване в изборния процес трябва да се възприеме подход, ориентиран към човека. Това означава, че от самото начало (бъдещите) потребители на ИКТ решението трябва да бъдат включени в целия процес на разработка и проектиране. Те могат да бъдат включени чрез полуструктурирани интервюта и фокус групи, чрез възможности за предоставяне на обратна връзка (на хартия) относно макети и процеси и чрез потребителски проучвания. Подходът, ориентиран към човека, също така включва провеждане на проучвания, след използване на ИКТ решението в изборния процес, за събиране на обратна връзка за допълнително подобряване на използваемостта и достъпността с течение на времето.

***3. Когато държавите-членки изберат да осигурят електронно решение, което не е универсално достъпно, следва също да се предостави алтернативно, широко достъпно решение.***

Всеобщото избирателно право предполага, че всички участници в изборите могат да изпълняват всички задачи и да упражняват всички права, както е предвидено от закона. Наличието на паралелна, еквивалентна процедура, достъпна за повечето потребители, може да е необходима в случаите, когато ИКТ решението не е универсално достъпно. Трябва също така да се отбележи, че в някои случаи използването на ИКТ може да бъде по-достъпно за някои хора от традиционните решения на хартиен носител.

Като поддържат алтернативна процедура в допълнение към тази, използваща ИКТ, държавите-членки гарантират, че всички заинтересовани страни, които имат всеобщо избирателно право, имат достъп и по този начин избягват създаването или задълбочаването на цифровото разделение. Това означава, че потенциалните потребители са идентифицирани, достъпността е оценена, и алтернативно и широко достъпно решение е разработено и се поддържа. Обществото трябва да бъде информирано за алтернативното решение.

Регламентът следва да изясни правната стойност на резултатите, получени от съвместно съществуващи алтернативни решения, както и приложимите правила в случай, че се използват от едно и също лице. Освен това регламентът трябва да изясни справянето с конфликти и други възможни проблеми, произтичащи от използването на множество канали за един и същи процес.

***4. Държавите-членки следва да гарантират целостта и автентичността на информацията, предоставена от ИКТ решенията, използвани в изборния процес. Трябва да се въведат процедури за откриване и, ако е възможно, коригиране на всякакви грешки или неоторизирана намеса.***

ИКТ решенията трябва да прилагат механизми за удостоверяване, за да се избегнат неоторизирани промени в съответствие с допусканията, определени като част от Насока 1. ИКТ решенията в изборния процес трябва да работят без грешки или неоторизиран промени, като по този начин допринасят за целостта на изборите. Организацията на изборите трябва да осигури точни проверки и баланси през всички изборни фази. Такива проверки на целостта са съществени части от цялостните усилия за сигурност и киберсигурност за защита на изборите срещу атаки, от външни нападатели и/или неоторизиран вътрешен достъп, както и от усилията за справяне с потенциално неправилно боравене или грешки в софтуера или хардуера. Трябва да има протоколи за откриване и ефективно реагиране при такива случаи. Проверките следва да се извършват с подходяща степен на независимост.

В идеалния случай всички неоторизирани промени или грешки в електронния процес или електронните документи трябва да бъдат открити и коригирани. Ако това не е възможно, допусканията трябва да бъдат формулирани по съответния начин като част от Насока 1. Възможността за откриване и коригиране на грешки или манипулации е важна във всички фази на изборния процес, включително при работа с избирателните списъци, както и по отношение на преброяването и предаването на резултати от избирателните секции на регионален или централен орган, особено ако предаването се извършва по интернет.

За предпочитане е да има възможност някой да бъде привлечен към отговорност, ако възникнат неоторизирани промени или грешки. От съществено значение е да се осигури отчетна и прозрачна процедура относно това как да се взаимодейства с работеща система, да се коригират всякакви данни или да се промени или замени неизправна система. Взаимодействието с работеща система за такива цели трябва да бъде разгледано в анализите на риска (вижте Насоки 1 и 9).

Заинтересованите страни трябва да могат да проверят дали преброяването и предаването на резултатите са извършени правилно, включително, но не само, чрез използване на статистически тестове на числени изборни резултати, като одити за ограничаване на риска и различни видове наблюдения, информирани от специфичен за страната експертен опит.

***5. Държавите-членки следва да гарантират наличието и надеждността на ИКТ решенията, използвани в изборния процес.***

ИКТ решенията трябва да бъдат достъпни и надеждни. Едно ИКТ решение трябва да бъде функционално, в съответствие с изискванията и предположенията дори в случай на повреда на системата или грешки от потребители или други, или в случай на атаки. Освен това ИКТ решението трябва да бъде надеждно. То трябва да запази функционалността си, независимо от недостатъците в хардуера или софтуера в други части на изборния процес. Като алтернатива трябва да има мерки за предоставяне на информация за и към активиране на предварително установени резервни решения и канали, включително решения, които не разчитат на активни връзки.

Трябва да бъдат въведени и редовно тествани планове за реакция при инциденти и планове за непрекъснатост на бизнеса. Мерките за сигурност за осигуряване на наличност и надеждност включват (този списък не е изчерпателен) управление на правата за достъп до системата, процедури за тестване на системата преди действителния изборен процес, процедури за извършване на актуализации по време на оперативната фаза, правила за сигурност за предаване на информация извън контролирани среди, изисквания за защита на данните, идентифициране на нередности от системата и комуникация в случай на проблеми. Това може да включва процедури, изисквани от стандартите на ISO, като серията ISO 27000.

***6. Държавите-членки следва да осигурят тайната и поверителността на информацията, съхранявана в рамките на ИКТ решението, както се изисква от изборните закони и законите за защита на данните.***

Изискванията за секретност и поверителност, произтичащи от съответните правни принципи, трябва да бъдат гарантирани, като се вземат предвид допусканията, които също трябва да бъдат дефинирани, както е посочено в Насока 1. Това включва съображения относно дългосрочната секретност, т.е. дали тайната трябва да бъде гарантирана във времето или не (например като се има предвид, че е възможно да се съхраняват криптирани данни днес и да се дешифрират по-късно, със съществуващи или нови решения, като например квантови компютри, които се очаква да станат широко достъпни).

Принципите за защита на данните като неприкосновеност на личния живот при проектирането или минимизиране на данните са минимални изисквания и трябва да се вземат предвид винаги, когато се използват ИКТ в изборния процес. Освен това, за всяко конкретно използвано ИКТ решение, държавите-членки следва да обмислят дали са необходими допълнителни, подходящи и специфични мерки, които надхвърлят мерките за защита на данните, за да се защитят основните права на субекта на данните, както се изисква например от член 6, параграф 1 от Конвенцията на Съвета на Европа за защита на лицата по отношение на обработката на лични данни (ETS № 108). Ако държавата-членка установи необходимост от такива специфични мерки, те трябва да станат част от изборните разпоредби.

Конфликтите между прозрачността, от една страна, и поверителността и секретността, от друга, трябва да бъдат внимателно обмислени (вж. също Насока 7).

***7. Държавите-членки следва да гарантират прозрачност на изборите и на използваните ИКТ решения.***

Осигуряването на прозрачност във всички аспекти на изборите е от ключово значение за провеждането на успешни и надеждни избори и за насърчаване на доверието в процеса, още повече, когато се използват ИКТ решения. Все по-често експертите, които не са ИТ, изпитват трудности при разбирането на ИКТ решенията. Следователно е необходимо да се увеличи капацитетът на всички заинтересовани страни за разбиране на ИКТ решенията.

Всички заинтересовани страни трябва да бъдат информирани за използването на ИКТ решения, включително въвеждането им в изборния процес, тяхната работа и следизборната оценка на използването на решението. Подробностите за неговото въвеждане трябва да включват:

1. разработване на общата стратегия;

2. публикуване на технически изисквания, предположения и информация за начина, по който трябва да бъдат изпълнени изискванията;

3. отстраняване на констатирани недостатъци от предишни избори;

4. комуникация относно процеса на разработване и вземане на решения, включително събраните входящи данни и участващия (интердисциплинарен) екип;

5. предоставяне на информация за целесъобразността на цялостното изпълнение;

6. предоставяне на информация относно придобиването на решението и неговата организация;

7. предоставяне на информация за изчерпателната оценка преди започване на използване на ИКТ решението, както и информация за резултатите от текущата оценка на риска;

8. предоставяне на информация за това как трябва да се подходи към противоречащи си или конкуриращи се принципи като неприкосновеност на личния живот и секретност срещу прозрачност;

9. публикуване на изходния код.

Прозрачността също така включва предоставяне на наблюдатели на достъп до документация и до процесите, в идеалния случай на познат за тях език.

Освен това мерките за прозрачност следва също така да включват разпоредби за структурирани (машинночетими) данни за изборния процес (като местоположението на избирателните секции и тяхното работно време, списъци с кандидати и изборни резултати), включително като отворени данни.

Изискванията за прозрачност трябва да са насочени към осигуряване на обществен контрол. Трябва да има подходящи процеси за получаване, отговаряне или обсъждане на обратна връзка от обществеността и за обработка на заключенията. По този начин прозрачността може да допринесе за цялостната сигурност и доверие в изборния процес.

И накрая, прозрачността е междусекторна тема и като такава засяга и други насоки. Това изисква, наред с други неща, допускания за публикуване (Насока 1); предоставяне на информация относно процеса на разработване и вземане на решения за установяване на критерии за използваемост и достъпност (Насока 2); организиране на прозрачна процедура за взаимодействие с работеща система, коригиране на данни или промяна или замяна на неправилно работеща система (Насока 4); документиране на решения за наличност и надеждност, включително съответните изисквания (Насока 5); документиране на решения относно сигурността и поверителността, включително решения за тяхното съгласуване с изискванията за прозрачност (Насока 6); документиране на изискванията за оценка на системата (Насока 8); или документиране на процеса на управление на риска (Насока 9).

***8. Държавите-членки следва да организират оценка на ИКТ решенията, използвани в изборния процес, от независими експерти преди внедряването.***

Тази насока се занимава с процеса на оценка преди внедряването на ИКТ решение в изборния процес. Оценката трябва да обхваща, но да не се ограничава само до аспектите на сигурността, използваемостта и достъпността. Обхватът ѝ трябва да включва цялото ИКТ решение и неговата среда за използване.

Подходите за оценка трябва да бъдат дефинирани, включително нивото на гарантиране на оценката. В идеалния случай трябва да се даде предимство на стандартизиран подход за оценка. Като предварително условие целта на оценката трябва да бъде ясно дефинирана.

Оценката изисква няколко документа, които в случай на стандартизирана оценка трябва да бъдат ясно дефинирани. Трябва да се определи – на много ранен етап – дали оценката трябва да се извърши само от избрани експерти с достъп до ИКТ решението, изходния код и документацията и/или дали оценката (или части от нея) може да бъде извършена от всеки, защото ИКТ решението, изходният код и документацията са публично достъпни.

Трябва да се уточни и как се стига до независима оценка. Експертите трябва да бъдат възможно най-независими. Това може да бъде постигнато, ако участват два субекта: единият е упълномощен да извърши действителното оценяване, а другият, държавна организация, контролира оценяващия субект. Може да са необходими различни експерти за различни области на изискванията (като сигурност или използваемост/достъпност). И накрая, важно е да се вземе предвид времето, необходимо на независимите експерти за извършване на оценката.

Изискванията и подходът за оценка, както и резултатите от оценката и информацията за участващите субекти/лица (най-вероятно интердисциплинарен екип), трябва да бъдат публично достъпни.

***9. Държавите-членки следва да извършват непрекъснато управление на риска на ИКТ решенията, използвани в изборния процес.***

Процесите, които са важни за правилното провеждане на избори и предоставянето на точни резултати, може да са изправени пред рискове, подобни на електронното гласуване, особено ако основното решение е уеб базирано. Тези рискове трябва да се управляват. По-специално, когато се идентифицират рискове за сигурността, трябва да се разработят пропорционални отговори.

Рисковете трябва да бъдат изведени от изискванията и допусканията (Насока 1) и резултата от оценката (Насока 8). По този начин управлението на риска е уместно по време на процеса на разработка и при използване на ИКТ решението в изборния процес, както и при подготовката на бъдещи избори. Оценката на текущите рискове и вземането на решение дали оставащите рискове са все още приемливи е непрекъснат процес. Това е от особено значение, тъй като с времето се появяват нови видове атаки.

Важно е да има яснота за оставащите рискове. Освен това трябва да се реши дали и как да се управляват тези рискове. Подходите за управление на риска трябва да включват планове за действие в извънредни ситуации.

В светлината на управлението на риска следва да се реши каква информация трябва да бъде публично достъпна и каква не, като се има предвид, че сигурността чрез неизвестност обикновено се счита за контрапродуктивна.

Подходът за управление на риска трябва да се преразглежда редовно, поне след всеки проведен вид избори. Всички необичайни случаи, проблеми или оплаквания трябва да бъдат взети под внимание.

Подходът за управление на риска, както и информацията за участващите субекти/лица (най-вероятно интердисциплинарен екип), трябва да бъдат публично достъпни.

***10. Държавите-членки следва да изградят и поддържат необходимия капацитет за оценка, въвеждане и управление на използването на ИКТ решения в изборния процес.***

При въвеждането на ИКТ в която и да е част от изборния цикъл е от съществено значение държавите-членки да разполагат с необходимия административен и технически капацитет и свързаните с това ресурси, включително финансови ресурси, за да планират, прилагат и управляват технологията успешно и по устойчив начин.

Държавите-членки следва да обмислят, наред с други неща, степента на автоматизация на целия изборен процес и потенциалните синергии между новото решение и съществуващите нискотехнологични или високотехнологични решения. В идеалния случай те трябва да разполагат с по-широка стратегия за инвестиции, свързани с ИКТ.

Административният и технически капацитет по същество изисква квалифицирана работна ръка, която трябва да бъде непрекъснато обучавана, оборудвана с необходимите инструменти и ресурси и, най-важното, да ѝ се дава достатъчно време, за да се съсредоточи върху задачите си.

Крайната цел на притежаването на необходимия капацитет е да се избегне възлагането на основни задачи по администриране на избори на трети страни с печалба и по този начин да се даде възможност на съответните органи да наблюдават ефективно изборите в съответствие със законовите изисквания, без да са зависими от частни лица.

***11. Държавите-членки следва да носят крайната отговорност, също и когато са включени частни заинтересовани страни.***

При организирането на избори държавата-членка носи крайната отговорност за правилното изпълнение и провеждане на изборния процес. Такъв е и случаят, когато трети страни (включително частни лица) подпомагат държавата-членка при провеждането на изборния процес или когато части от изборния процес са възложени на външни изпълнители и/или са възложени на трети страни. Третите страни трябва да зачитат и изпълняват същите стандарти и очаквания като държавите-членки. Съответните разпоредби трябва да бъдат включени в договорните споразумения.

***12. Държавите-членки следва проактивно да се занимават с възможното използване на ИКТ решения в ситуации, при които „непреодолима сила“ засяга редовното провеждане на избори.***

Неотдавнашният опит в адаптирането на изборните процедури към новите ограничения, свързани със здравето, наложени от пандемията Covid-19, подчерта въпроса за въвеждането на ИКТ решения, които да помогнат за справянето с такива изключителни обстоятелства. Въпреки това, както е показано в тези насоки, използването на ИКТ решения не може да се счита за краткосрочно средство за защита при извънредни ситуации. Вместо това, то трябва да бъде част от по-дългосрочното планиране на изборния процес и от по-широк подход за справяне с извънредни събития.

Държавите-членки следва проактивно да се справят с бъдещи смущения, включително пандемии. Ако държавите-членки възнамеряват да използват ИКТ решения при такива извънредни обстоятелства, те се съветват да се подготвят предварително за такъв случай, в съответствие с гореспоменатите насоки.

**Речник на някои термини, използвани в насоките**

* **Достъпност:** достъпността е свързана с проектиране на продукти и системи, които са достъпни за всеки, независимо дали човек има увреждане или не. В същото време достъпността може конкретно да адресира дискриминационни аспекти, свързани с еквивалентни потребителски изживявания, като се фокусира върху хората с увреждания, за да гарантира приобщаване. [3]
* **Допускане**: Допусканията описват условията, на които работната среда, в която се използва ИКТ решението, трябва да отговаря, ако иска да осигури цялата си функционалност за сигурност. „Ако целта на оценката (англ. Target of evaluation или TOE) [ИКТ решението] е поставена в работна среда, която не отговаря на тези допускания, TOE може вече да не е в състояние да предоставя цялата си функционалност за сигурност. Допусканията могат да бъдат относно физическата среда, персонала и свързаността на оперативната среда.“ [4] Насоките препоръчват прозрачност относно допусканията и тяхната оценка (вижте Насоки 1 и 7). Техният статус „реалистичен/нереалистичен“ трябва периодично да се преоценява (вижте Насока 9 относно политиката за управление на риска).
* **Автентичност (на информацията)**: свойството, че данните произхождат от техния предполагаем източник. [5]
* **Наличност**: осигуряване на навременен и надежден достъп до и използване на информация и системи. [6]
* **Избори**: политически избори или референдум.
* **Подход/дизайн, ориентиран към човека**: (както се използва в стандартите на ISO) е подход за решаване на проблеми, често използван в рамките на проектирането и управлението, който разработва решения на проблеми чрез включване на човешката гледна точка във всички стъпки на процеса на решаване на проблеми. Човешкото участие обикновено се осъществява при наблюдение на проблема в контекста, мозъчна атака, концептуализиране, разработване и прилагане на решението. [7]
* **ИКТ**: информационни и комуникационни технологии. В тези насоки това се равнява на продукти и процеси, които съхраняват, извличат, манипулират, предават или получават информация по електронен път в цифрова форма.
* **Цялостност (на информацията)**: свойството, че данните не са били променени по неоторизиран начин. Целостта на данните обхваща данните в хранилището, по време на обработка и по време на транзит. [8]
* **Държава-членка**: в тези насоки „държава-членка“ се отнася до органа, който отговаря за регулирането, провеждането или надзора на въпросния изборен процес. Обикновено, но не винаги, се отнася до органа за управление на изборите на местно, регионално или централно ниво. Може да се отнася и за други обществени институции като парламента или правителството.
* **Минимално ниво** **(до което правните принципи трябва да бъдат осигурени)**: често не е възможно да се гарантира пълното зачитане на всички принципи, тъй като може да има противоречащи си или конкуриращи се принципи, като поверителността и защитата на данните от едната страна и прозрачността от другата. В тези случаи трябва да се постигне баланс на интересите и да се определи минималното ниво, до което трябва да се осигури всеки един от конфликтните принципи. Това решение трябва да бъде взето от компетентния орган, обикновено законодателя. Същността на принципите не може да бъде нарушена.
* **Надеждност**: способността на система или компонент да функционира при определени условия за определен период от време. [9]
* **(Техническо) изискване**: условие или способност, която трябва да бъде изпълнена или притежавана от система или системен елемент, за да удовлетвори договор, стандарт, спецификация или други официално наложени документи. [10]
* **(Правно) изискване**: правното изискване е конкретизация на правен принцип. Например правните изисквания, които се прилагат за предаването на резултатите от избирателните секции на централната избирателна комисия (например изисквания за срокове, формати или проверки), произтичат от и са конкретизация на принципите на универсално, равно, свободно и тайно избирателно право.
* **Риск**: нивото на въздействие върху организационните операции (включително мисия, функции, имидж или репутация), организационните активи или лица в резултат на работата на информационна система, като се има предвид потенциалното въздействие на заплаха и вероятността тази заплаха да възникне. [11]
* **Заплаха:** Всяко обстоятелство или събитие с потенциал да навреди на избирателна ИКТ система чрез неоторизиран достъп, унищожаване, разкриване, модифициране на данни и/или отказ на услуга.
* **Използваемост**: използваемостта е свързана с проектирането на продукти, които да бъдат ефективни, ефикасни и удовлетворяващи. Включва дизайн на потребителското изживяване и е тясно свързана с достъпността. [12]

[1]. Кодекс на добрите практики по изборни въпроси (CDL-AD(2002)023rev2-cor), приет от Венецианската комисия на нейната 52 -ра сесия (Венеция, 18-19 октомври 2002 г.).

[2] . [www.iso.org/standard/52075.html](http://www.iso.org/standard/52075.html) .

[[3]](https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a575d9#_ftnref3) . Определението е взето от: [www.w3.org/WAI/fundamentals/accessibility-usability-inclusion/](http://www.w3.org/WAI/fundamentals/accessibility-usability-inclusion/) .

[[4]](https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a575d9#_ftnref4) . Определението е взето от: <https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf>

[[5]](https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a575d9#_ftnref5) . Определението е взето от: <https://csrc.nist.gov/glossary/term/authenticity>.

[[6]](https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a575d9#_ftnref6) . Определението е взето от: <https://csrc.nist.gov/glossary/term/availability>.

[[7]](https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a575d9#_ftnref7) . Определението е взето от: [www.w3.org/WAI/redesign/ucd](http://www.w3.org/WAI/redesign/ucd) .

[[8]](https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a575d9#_ftnref8) . Определението е взето от: <https://csrc.nist.gov/glossary/term/data_integrity>.

[[9]](https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a575d9#_ftnref9) . Определението е взето от: <https://csrc.nist.gov/glossary/term/reliability>.

[[10]](https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a575d9#_ftnref10) . Определението е взето от: <https://csrc.nist.gov/glossary/term/requirement>.

[[11]](https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a575d9#_ftnref11) . Определението е взето от: <https://csrc.nist.gov/glossary/term/risk>.

[[12]](https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a575d9#_ftnref12) . Определението е взето от: [www.w3.org/WAI/fundamentals/accessibility-usability-inclusion](http://www.w3.org/WAI/fundamentals/accessibility-usability-inclusion/) .