**СПРАВКА**

**за отразяване на предложенията, становищата и възраженията, постъпили при проведената обществена консултация на проекта на Методика за удостоверяване на съответствието на доставения тип техническо устройство за машинно гласуване с изискванията по чл.213, ал. 3 от Изборния кодекс и изискванията на техническата спецификация**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Подател** | **Предложение** | **Приема/не приема** | **Мотиви** |
| 1.  | **Жоро Маринов - писмо вх. № ДАЕУ-16613/ 07.10.2021 г.** | 1. В т. 2 на Методиката да се дефинира еднозначно и детайлно обхвата на дейностите по тестване и оценяване на устройствата за машинно гласуване. Липсва обхват на дейностите по тестване и оценяване при доставка на нови машини; при ресертифициране за следващи избори от същия тип и при ресертифициране на следващи избори от друг тип, в т. ч. избори 2 в 1. 2. Да се добавят в процедура 4 текстове, предвиждащи анализ и оценка на Политиките за сигурност на информацията и документите за управление на риска на ЦИК и на изпълнителя. 3. Липсва цялостен подход за оценяване на сигурността на информацията в т.ч. и на Базовата СА верига, която е детайлно описана в Техническата спецификация по обществената поръчка за техническо осигуряване на изборите. Не става ясно кой, кога и по какъв начин издава цифровите сертификати и криптографските ключове, които се ползват масово в системата за машинно гласуване, както и механизмите за сигурност, които са внедрени за защита на Root CA, PIN кодове, пароли и другите средства за идентификация и оторизация, които се ползват от ТУМГ.4. Да се изготви набор от стандартни тестови процедури (Acceptance Test Procedures) за различните компоненти на системата за машинно гласуване, с които ДАЕУ/ ЦИК или друг орган да верифицира готовността на машините и софтуера за даден всеки вид избор за който ще се използват в бъдеще. | 1. Не приема предложението.2. Не приема предложението3. Приема предложението по принцип. 4. Не приема предложението. | 1. В т. 2 от Методиката е дефиниран обхвата на дейностите, които се включват в удостоверяване на съответствието, така че да е видно от къде започват и къде свършват ангажиментите на ДАЕУ, БИМ и БИС. В т. 8 от Методиката. „Удостоверяване на съответствието на технически устройства за машинно гласуване, които вече са използвани в предходни избори“ е предвиден реда за реализиране на тези процеси, като в Плана за оценяване и удостоверяване на съответствието се включват само дейностите, които ще бъдат извършени с оглед резултатите от направения анализ на документацията и състоянието на предоставените образци на технически устройства за машинно гласуване.Този процес на последващо удостоверяване на съответствието по своята същност би могъл да бъде определен като ресертификация. 2. Политиките за сигурност на информацията и подхода за управление на риска за сигурността на информацията на изпълнителя и на ЦИК не попадат в обхвата на методиката, тъй като се отнасят до организацията и процесите на изпълнителя/доставчика или ЦИК. Удостоверяването на съответствието, което ще се извършва от ДАЕУ, БИМ и БИС е само по отношение на типа техническо устройство за машинно гласуване и това е изрично посочено в чл. 213а, ал. 2 от Изборния кодекс.3. В Приложение 4 е разписан сценарии за проверка на базовата СА верига в рамките на правомощията на удостоверяващите институции.  4. Към настоящия момент няма утвърдени стандартни разработки за софтуер за отделните видове избори.  |
| 2. | **Николета Минекова****писмо вх.№ ДАЕУ-16536/ 06.10.2021 г.**  | 1. Да се добави т. 2 „Нормативни основания и обхват“ следния текст:„Дейностите по тестване и оценяване на съответствието на информационните активи с изискванията на Изборния кодекс започват от момента на инсталиране на Операционната система (или на Приложния софтуер) и завършват с тестване на реконсилация на разписките, издадени от специализираните устройства за машинно гласуване и прочитане на контролната памет в Изчислителните пунктове на РИК и ЦИК.“Мотиви: Отговорностите по отношение техническото и функционалното състояние на машините трябва да са ясно разграничени, а именно:- какви дейности извършват трите страни – Възложител, Изпълнител и Орган по сертификация (удостоверяване)?- до къде резултатът от работата на Изпълнителя е бил тестван?- къде ЦИК определя административно-организационни мерки за удовлетворяване на изискванията на спецификацията?- какви са границите на тестовете - от къде започват и до къде свършват ангажиментите на ДАЕУ, БИС и БИМ да тестват, оценяват и удостоверят съответствието на типа?2. В т. 2 да се добави следния текст : „Решението за удостоверяване се издава на български език и е валидно само и единствено в комплект с Доклада за оценяване на съответствието и Декларацията за съответствие, издадена от Изпълнителя.“Мотиви: Това е задължително условие за валидност на този документ. Ако липсва актуална версия на който и да било от документите – то удостоверението би трябвало да е невалидно.3. В т. 3 следва да се добавят дефиниции за „електронна избирателна кутия“ и „специална кутия за машинно гласуване“ по чл. 268, ал. 4 от Изборния кодекс.Мотиви: Трябва да се определи разликата между двете кутии, за да не се объркват с други наименования за същите активи като „урна“, „непрозрачна урна за контролни разписки“, „кутии за разписките от машинното гласуване“, „непрозрачна кутия“, „кутии за разписките от електронното машинно гласуване“ и т.н.4. В т. 6. 3 и т. 6. 4 не са описани сценарии за провеждане на тестове за проверка на съдържание, интегритет и сигурност на „електронната избирателна кутия“ и „електронния дневник на изборния процес“. 5. В т. 4.3. следва да се регламентира подходът на екипите за тестове и оценка при липса на някой от задължителните информационни активи, описани в коригирания текст на т. 4. 1., съгласно т. 6 от Методиката и да се определи реда за тяхното придобиване от ЦИК и изпълнителя.Мотиви: Подобен казус трябва да се изясни предварително, още преди да се стартира процеса. ЦИК и изпълнителят (а и обществото) трябва да знаят какви информационни активи са необходими за извършване на пълноценни и ефективни тестове на оборудването, софтуера и сигурността на информацията. В противен случай евентуално посочване на отсъствие на някой актив като причина за неизвършване на тестовете/оценката ще бъде тълкувано като опит за „измъкване“ на екипа от отговорност за вземане на решение – положително или отрицателно.6. При обществено обсъждане следва да се публикуват и Приложения № 1 - 4, както и текстовете на декларациите за конфликт на интереси и за конфиденциалност. Мотиви: Позоваването на приложения, които не са публикувани, възпрепятства еднозначното разбиране на процеса и оставя празнини, които водят до съмнения в цялостния процес на удостоверяване (сертифициране). 7. В т. 6. 3 не е разгледан варианта за работа на 2 машини в една секция, както и тестовите сценарии при произвеждане на избори 2 в 1, каквито ни предстоят.Мотиви: След като към момента на актуализиране на Методиката е било ясно, че предстои произвеждане на избори 2 в 1, би следвало в т. 6. 3 да залегнат основните принципни положения за предстоящите тестови сценарии. 8. В т. 6.4 и процедура Приложение 4 да се предвиди тестване и оценяване на базовите компоненти на сигурността на информацията, а именно: * Смарткарти Full size, ISO/IEC 7816;
* Четец за смарт карта - Full size PC/SC SmartCard четец за контактни смарткарти по стандарт ISO/IEC 7816;
* Базова CA верига за подписване и верификация на системните компоненти и за издаване на цифровите сертификати на смарткартите;
* Системен асиметричен криптографски ключ (системен сертификат) за подписване на номенклатурните данни и софтуера за извършване на гласуване;
* Базов образ (image) на операционната система и базовият софтуер за машинно електронно гласуване
* Ключ за full disk криптиране;
* Подход за пълно криптиране на вътрешната памет
* Криптографски алгоритми;
* Подход за инсталация, конфигурация и параметризация на машините за гласуване, включително и подготовката при провеждане на евентуален втори тур на изборите.

Мотиви: Липсата на посочените по-горе тестове и оценявания ще постави под съмнение комплексния характер на тестовете в целия диапазон на сигурността на информацията, ефективността на процеса и компетентността на експертите, които са извършили дейностите.В докладите от последните две удостоверяване никъде не е засегнат въпроса за сигурността на Базовата СА верига, която има ключова роля по отношение сигурността на информацията вътре и извън ТУМГ (на ЗТУ). Пред външния наблюдател възникват съвсем закономерно следните въпроси:* Кой, как, къде и при какви механизми за сигурност генерира, поддържа и съхранява Root CA keys?
* Кой има достъп до ROOT CA, ROOT Keys, Master PIN-a, както и до PIN кодовете за смарткартите преди те да бъдат поставени в запечатаните пликове?
* Възможно ли е лицето, което е отговорно за генерирането на 60-те хиляди сертификата да генерира неоторизирано и безконтролно допълнителни количества сертификати, които да бъдат възприети от определени ТУМГ като „оригинални такива“?

Докато не бъде „разнищена“, тествана и проверена Базовата СА верига, винаги ще съществува риск от компрометиране на машинното гласуване.9. В Методиката не става ясно спрямо коя Техническа спецификация ще се извърши оценяване и сертифициране (удостоверяване). Мотиви: При предстоящите удостоверявания на машини за гласуване ще бъдат използвани машини от две/три последователни доставки с различни доставчици и един производител. Тези машини следва да отговарят на изисквания, посочени в най-малко три Технически спецификации по ОП с рег. № 04312-2020-0001, ОП с рег. № 04312-2021-0006 и ОП с рег. № 04312-2021-0009. Отделно от това ЦИК има изисквания, посочени в Техническата спецификация по ОП с рег. № 04312-2021-0013 за дейности по техническо осигуряване на машинното гласуване със СУЕМГ (ТУМГ).10. В т.6. 4 и процедура Приложение 4 следва да се предвиди тестване и оценяване на сигурността на информацията при всички процеси, апаратни средства, софтуер и компоненти по т. 2.8, 2.9, 2.10, 2.11 и т.3 от Приложение № 1 към Решение №548 -ПВР/НС на ЦИК от 17.09.2021г . Мотиви: Това са изцяло нови изисквания към ТУМГ (СУЕМГ), които са заложени в Техническата спецификация от 17.09.2021г. и тяхното изпълнение следва да бъде надлежно проверено и оценено, за което няма никакви данни в Методиката от 30.09.2021г.

|  |
| --- |
|  |

 | 1. Приема предложението по принцип.2. Приема предложението.3. Приема предложението.4. Не приема предложението. 5. Приема предложението.6. Приема предложението по принцип. 7. Приема предложението. 8. Приема предложението.9. Приема предложението по принцип. 10. Не приема предложението.  | 1. В Методиката и Процедурите, разписани в приложения към методиката, е предложен съответния обхват за всеки екип. В текста на актуализираните Процедури са ясно дефинирани задълженията на експертите в съответния екип и обхвата на изпитванията/тестовете, проверките и оценяването на съответните компоненти и характеристики на техническите устройства за машинно гласуване. Въпреки посоченото в т. 2 е добавен текст относно обхватът на дейностите.Част от поставените въпроси не са от компетентността на трите институции и следва да бъдат отправени към ЦИК и/или Изпълнителя.2. Добавен е текст в т. 2. 3. В т. 3 от Методиката са дадени определения за „електронен дневник на изборния процес“ и „електронна избирателна кутия“. 4. В Методиката и приложенията се съдържат сценарии, които по същество съответстват на проверка на посочените компоненти.  5. В т. 4. 1 е добавен текст, който регламентира въпросния подход. 6. При настоящото обществено обсъждане не са публикувани приложенията, тъй като няма изменения в тях спрямо предишния вариант на методиката и това е изрично посочено в анотацията към общественото обсъждане. 7. В Методиката и приложение № 3 са добавени съответните текстове. 8. В Методиката и Приложение № 4 са добавени съответните текстове в рамките на правомощията на удостоверяващите институции. 9. Методиката не се изготвя за конкретна техническа спецификация. В тази връзка, в т. 1, абзац 1 изрично е посочено, че се взема предвид приложимата за конкретното удостоверяване техническа спецификация. В Доклада за оценяване на съответствието се посочва в конкретната техническа спецификация. 10. Посочените изисквания в точки 2.8, 2.9 и 2.10 от Приложение № 1 към Решение №548-ПВР/НС на ЦИК от 17.09.2021г. са съобразени и по отношение на тях ще се извършват проверки. По отношение на т. 2.11 - същата се отнася до сроковете, в които изпълнителят следва да предостави определена информация на ЦИК: тези изисквания не са в обхвата на проверката извършвана от ДАЕУ. По отношение на т. 3 - тя се отнася до процеса по инсталиране на софтуера и по подготовка на машините в изборните секции, към който процес ДАЕУ няма отношение. |
| 3.  | **Здравко Костадинов - ДАЕУ-16651/ 08.10.2021 г.** | 1. Да се изясни въпроса какво се разбира под „техническа спецификация“ и дали тя е част от изискванията по чл. 213, ал. 3 от Изборния кодекс. 2. Да се уточни коя от наличните до момента 4 различни технически спецификации ще се прилага от екипите за оценка на съответствието. 3. Т. 6 от Методиката да се актуализира като се предвидят дейности по анализ на политиките за сигурност и цялостно оценяване на рисковете за сигурността на информацията, както от страна на изборната администрация, така и от страна на изпълнителите и подизпълнителите по различните договори за доставка на стоки и услуги. 4. Да се предвидят текстове за одит, контрол, тест или проверка на „Удостоверителната верига“, описана в Приложение № 1 към Решение № 688-ПВР/НС на ЦИК. 5. В Методиката да се добави информация за реакцията и действията при базови критични ситуации като липса на компонент на апаратната или програмната конфигурация, непредоставяне на пълна и актуална документация, закъснения при предоставянето на комплекта машини и документация, наличие на промени от страна на възложителя в техническата спецификация.6. В Методиката да се добавят текстове, че органът по сертификация следва да провежда планирани и непланирани надзорни мероприятия по отношение на сертифицирания продукт/услуга.  | 1. Приема предложението. 2. Приема предложението по принцип.3. Не приема предложението. 4. Приема предложението. 5. Приема предложението. 6. Не приема предложението.  | 1. В т. 3 от Методиката е дадено определение за техническа спецификация. 2. Методиката не се изготвя за конкретна техническа спецификация. В тази връзка, в т. 1, абзац 1 изрично е посочено, че се взема предвид приложимата за конкретното удостоверяване техническа спецификация. В Доклада за оценяване на съответствието се посочва конкретната техническа спецификация, която се взема предвид. 3. Политиките за сигурност на информацията и подхода за управление на риска за сигурността на информацията на изпълнителя и на ЦИК не попадат в обхвата на методиката, тъй като се отнасят до организацията и процесите на изпълнителя/доставчика или ЦИК. Удостоверяването на съответствието, което ще се извършва от ДАЕУ, БИМ и БИС е само по отношение на типа техническо устройство за машинно гласуване и това е изрично посочено в чл. 213а, ал. 2 от Изборния кодекс.4. В Методиката и Приложение 4 са добавени съответните текстове. 5. Добавен е текст в т. 4. 1. 6. Методиката е изготвена на базата на схема за сертификация 1а от БДС EN ISO/IEC 17067, която се отнася за изследване на типа и не предполага дейности по надзор. |