БЪЛГАРСКИ ИНСТИТУТ ПО МЕТРОЛОГИЯ

МИНИСТЕРСТВО НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ

БЪЛГАРСКИ ИНСТИТУТ ЗА СТАНДАРТИЗАЦИЯ

Проект!

Утвърдена със Заповед №……..

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

1. Общи положения

Цел на настоящата Методика е дефиниране на схема за оценяване и удостоверяване на съответствието на доставения/ите тип/ове техническо устройство за машинно гласуване (ТУМГ) с техническите изисквания към апаратната и програмната част на техническите устройства за машинно гласуване, които са определени от Централната избирателна комисия съгласно чл. 213, ал. 3 от Изборния кодекс и изискванията на приложимата/те техническа/и спецификация/и.

Удостоверяването на съответствието включва:

- преглед на предоставените информационни активи, анализ на документите и изготвяне на план за оценяване на съответствието;

- процесите по оценяване на съответствието на доставения тип ТУМГ, както и на вече доставени и използвани ТУМГ, с изискванията на чл. 213, ал. 3 от Изборния кодекс и на приложимата техническа спецификация;

- изготвянето на протоколи от тестовете и проверките и на доклад за оценяване на съответствието (по-нататък в текста „Доклада“);

- постановяване на решение за удостоверяване на съответствието от министъра на електронното управление (МЕУ), съвместно с председателя на Българския институт по метрология (БИМ) и председателя на Управителния съвет на Българския институт за стандартизация (БИС), съгласно чл. 213а, ал. 2 от Изборния кодекс.

В международната практика е установено и прието, че оценяването на съответствието спрямо определени изисквания се извършва от независим и компетентен орган под формата на сертифициране (следвайки определена сертификационна схема) или посредством друг подходящ начин. В документа Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting и Насоките и Меморандума към него е посочено, че съответствието на системата за електронно гласуване и на всеки ИКТ компонент с техническите изисквания трябва да се оцени от независим и компетентен орган, а схемата на удостоверяване трябва да бъде публично достъпна и всеобхватна.

Министерство на електронното управление (МЕУ), съвместно с Българския институт по метрология (БИМ) и Българския институт за стандартизация (БИС) не са акредитирани органи за сертификация на продукти, услуги и процеси по смисъла на БДС EN ISO/IEC 17065, а осъществяват дейностите по удостоверяване на съответствието на типа техническо устройство за машинно гласуване на основание изричното им оправомощаване с нормативен акт - Изборния кодекс и на базата на настоящата Методика.

При разработването на Методиката са взети предвид основните принципи на сертификацията на продукти и указанията за схеми за сертификация на продукти, посочени в БДС EN ISO/IEC 17067, както и тези, посочени в Recommendation CM/Rec(2017)5. Избраната от стандарта БДС EN ISO/IEC 17067 схема за сертификация, която служи като основа за разработване на настоящата Методика, не е приложена изцяло предвид спецификата на изискванията в посочените по-горе документи.

Оценяването на съответствието включва методи и процедури за проверка на валидността и автентичността на документите за съответствие, издадени от трета независима страна (сертификати, доклади и др.), техническо изследване на доставения тип ТУМГ, тестови сценарии за проверка на функционалността на системния и приложния софтуер и проверка на сигурността на информацията в апаратните и програмните средства, предназначени за обезпечаване на машинното гласуване в избирателните секции.

Методите и процедурите, в резултат на които се удостоверява съответствието, са подробно описани в приложение № 1, № 2, № 3 и № 4 към настоящата Методика.

2. Нормативни основания и обхват

Удостоверяването на съответствието се осъществява на основание чл. 213а, ал. 2 от Изборния кодекс като се имат предвид изискванията на чл. 213, ал. 3 и изискванията на

приложимата техническа спецификация. Изискванията на чл. 213, ал. 3 от Изборния кодекс се определят от Централната избирателна комисия (ЦИК).

Дейностите по удостоверяване на съответствието на доставения тип ТУМГ с изискванията на Изборния кодекс, описани в приложения № 1 - № 4, започват след предоставяне от страна на ЦИК на:

- представителна извадка от образци на ТУМГ с инсталирани операционна система и приложен софтуер. Правилата, по които се прави извадката, са подробно описани в т. 4. 2 на настоящата Методика;

- Декларация за съответствие и идентичност на техническите устройства за машинно гласуване, издадена от Изпълнителя/ите;

- цялата придружаваща документация за ТУМГ, в т.ч., Ръководства, Указания, Декларации, документи за оценяване на съответствието от трета независима страна, Техническото предложение на Изпълнителя по обществената поръчка, както и всяка друга документация, която ЦИК и Изпълнителя/ите са преценили за уместна и достатъчна с цел доказване на съответствието;

- администраторски пароли и средства за оторизация - за осъществяване на пълен администраторски достъп, както до хардуерните компоненти на ТУМГ, периферните устройства, записващите технически устройства и смарткартите, така и до базовия (системен) и приложен (реализиращ изборните процеси) софтуер, включително и до софтуера, който управлява специализираните хардуерни устройства;

Обхватът на дейностите по проверка и тестване на ТУМГ е описан подробно в т. 6 и в Приложения № 1 - № 4 от Методиката.

Дейностите по удостоверяване на съответствието завършват с издаване на решение за удостоверение за съответствието от министъра на електронното управление, председателя на БИМ и председателя на Управителния съвет на БИС. Решението за удостоверяване на съответствието се издава на български език и е валидно само и единствено в комплект с Доклада за оценяване на съответствието и Декларацията за съответствие и идентичност на ТУМГ, издадена от Изпълнителя/ите на дейностите по инсталиране и настройка на компонентите на ТУМГ и логистиката.

В случаите, в които за произвеждането на конкретни избори се използват вече доставени и използвани в предходни избори ТУМГ, обхватът на дейностите по проверка, тестване и удостоверяване на съответствието се определя по правилата, описани в т. 8 на настоящата Методика.

В обхвата на Методиката не се включват организационно-технически дейности, които се извършват от изборната администрация и Изпълнителя/ите; дейности, свързани с удостоверяване на организацията и технологията на компютърната обработка на резултатите от гласуването, осъществявана от „Информационно обслужване“ АД, както и такива, свързани с логистиката и техническото обслужване, които ще се извършват по отношение на ТУМГ.

Съгласно чл. 213а, ал. 4 от Изборния кодекс срокът за осъществяване на процесите по удостоверяване на съответствието от страна на трите институции е 20 работни дни, който започва да тече от датата на предоставяне от страна на ЦИК на ТУМГ с инсталиран софтуер и окомплектовани с всички информационни активи, необходими за произвеждане на съответните избори.

Приложимите документи за изпитване, проверка, оценяване и удостоверяване на съответствието са описани в Библиографията, но не са ограничени и като списък могат да бъдат допълвани в плана за оценяване, след преглед и анализ на предоставените от страна на ЦИК информационни активи и съпътстващата ги документация.

3. Термини, определения и съкращения

Техническо устройство за машинно гласуване (ТУМГ) - съвкупност от компоненти на апаратни и програмни средства, които в своята цялост осигуряват технологичния процес в избирателните секции по произвеждане на избори чрез машинно гласуване в Република България, в съответствие с изискванията на Изборния кодекс. В Изборния кодекс и в техническите изисквания са използвани различни термини, описващи устройствата за машинно гласуване, като например: специализирано устройство за гласуване; специализирано устройство за машинно гласуване; устройство; техническо устройство; специализирано устройство; устройство за електронно машинно гласуване**;** специализирано устройство за електронно машинно гласуване (СУЕМГ); машина; машина за гласуване и др. За целите на настоящия документ и в съответствие с разпоредбата на чл. 213а от Изборния кодекс, в тази Методика е използван обобщаващия термин - „техническо устройство за машинно гласуване“.

Технически изисквания към апаратната и програмната част на ТУМГ по чл. 213, ал. 3 от Изборния кодекс, които са определени от ЦИК (по-нататък в текста „технически изисквания“) - за целите на настоящия документ, обобщаващият термин „технически изисквания“ включва документите на ЦИК, определящи характеристики и параметри, които даден тип ТУМГ и/или негови съставни части, периферия и консумативи следва да притежават и които подлежат на удостоверяване. Това може да са официални документи на ЦИК под различни наименования, например: техническа спецификация (по чл. 213а, ал. 2 от ИК), техническо задание, технически параметри, технически характеристики и т.н., както и указания, които са предоставени от ЦИК в следствие на възникнали въпроси в процеса на удостоверяване.

Техническо предложение на Изпълнителя – документ по чл. 101, ал. 3 от Закона за обществените поръчки.

Техническа спецификация - документ, създаден за конкретна обществена поръчка, в който се определят изискваните характеристики на продукта или услугата, като равнище на качество, ниво на изпълнение спрямо изискванията за опазване на околната среда и климата, проектиране, което да отговаря на всички изисквания (включително достъп за хора с увреждания) и оценяване на съответствието, работни характеристики, приложение на продукта, безопасност или размери, включително съотносими към продукта изисквания по отношение на наименованието, под което се продава,

терминология, символи, изпитване и методи на изпитване, опаковане, маркиране и етикетиране, инструкции за употреба, производствени процеси и методи на всеки етап от жизнения цикъл на доставката или услугата и процедури за оценяване на съответствието.

Тип техническо устройство за машинно гласуване е съвкупност от технически устройства за машинно гласуване с еднакво предназначение, основани на един и същи принцип, имащи еднаква конструкция, функционалност и програмни средства, и изработени от един и същи производител по една и съща техническа документация и технология**.**

Доклад за оценяване на съответствието - документ, предоставящ оценка на съответствието с предварително определените критерии за оценяване, в резултат на извършените дейности, описани в приложенията към настоящата Методика.

Екип за оценяване на съответствието - специализирана група от експерти, която съобразно своята компетентност осъществява дейностите по изпитване/проверка и оценяване на съответствието на доставения тип ТУМГ, описани в приложенията към Методиката.

Записващо техническо устройство (ЗТУ)/ контролна памет - носител на информация по чл. 268, ал. 4 от Изборния кодекс, върху който са записани и криптирани уникални за всяка изборна секция данни, както и софтуера за криптиране на информацията. За да се избегне рискът от объркване, по-нататък в този документ се използва само термина записващо техническо устройство /ЗТУ/.

Проверка - планирани дейности като тестване, изпитване, изследване и др., в резултат на които се получават доказателства, информация и констатации, на базата на които се извършва оценяване на съответствието с предварително определените критерии за оценяване.

Съответствие - изпълнение на изискване, условие или очакване, което е документирано, обикновено е подразбиращо се или задължително. В случая - изпълнение на изискванията на чл. 213, ал. 3 от Изборния кодекс и на техническите изисквания към апаратната и програмната част на ТУМГ, които допълнително се определят от Централната избирателна комисия.

Доказателства от изпитвания и/или проверки - записи, излагане на факти или друга информация, които са свързани с критериите за оценяване, и които може да бъдат проверени.

Констатации от изпитвания и/или проверки, извършени по отношение на доставения тип ТУМГ - резултати от оценяването на събраните доказателства и информация от изпитванията/проверките на ТУМГ спрямо критериите за оценяване.

Критерии за оценяване - стандарти, законови, нормативни и договорни изисквания, условия или набор от изисквания и условия, на които следва да отговаря обектът на оценяване. Критериите за оценяване се използват като указания и еталон, с който се

сравняват получените резултати, доказателства и констатации от изпитванията и проверките, за да се определи съответствието. В процеса на удостоверяване на съответствието се използва подход за оценяване, основан на доказателства и констатации от извършените изпитвания и проверки на доставения тип ТУМГ.

Коригиращо действие - действие за отстраняване на причината за констатирано несъответствие и/или за предотвратяване на повторното му възникване.

СИК - секционна избирателна комисия.

Смарткарта - средство за оторизация по чл. 268, ал. 2 от Изборния кодекс, предназначено за използване от оторизирани представители на изборната администрация и от избирателите за удостоверяване правото за извършване на дадено действие. Ведно с апаратните и програмните средства на ТУМГ осигурява тайната на гласуването по чл. 213, ал. 2, т. 4, 9 и 10 от Изборния кодекс, както и идентификацията на оторизираните лица от СИК в рамките на конкретния изборен процес.

Достъп до механизмите за машинно гласуване - качество на ТУМГ, осигуряващо на избирателите и оторизираните представители на СИК възможност и удобство при участието им в изборния процес чрез предоставения потребителски интерфейс и за опазване тайната на вота.

Декларация за съответствие на продукт - документ, в който се декларира, че са изпълнени изискванията на актове на Европейския съюз, на стандарти, схеми и други документи. Издава се от производителя на дадения продукт. Декларацията се издава или превежда на български език. За определени ИТ продукти или компоненти може да се изисква издаването на декларация за съответствие от нотифициран орган.

Декларация за съответствие и идентичност на техническите устройства за машинно гласуване от Изпълнителя - документ, в който Изпълнителят/ите декларира/т, че са изпълнени изискванията на Изборния кодекс и техническите изисквания към апаратната и програмната част, които са определени от ЦИК, както за типа ТУМГ, които са били обект на удостоверяване на съответствието, така и за всички останали доставени устройства за машинно гласуване от същия тип, които се ползват за произвеждане на конкретните избори. Изпълнителят декларира и носи отговорност доставените устройства да имат идентични параметри на хардуер, софтуер, системни настройки, функционални характеристики и средства за защита с тези, които са били обект на удостоверяване на съответствието по време на подготовката, реализацията и приключване на изборния ден.

CE маркировка - знак за съответствие. С поставянето на този знак, производителят декларира, че продуктът му отговаря на изискванията и са изпълнени процедурите за оценяване на съответствието, описани в съответната европейска директива или регламент. За маркировката „CE“ се прилагат основните принципи, установени в чл. 30 от Регламент (ЕО) № 765/2008.

Автентичност - свойството, че дадената единица, обект на оценяване, е наистина това, за което претендира че е.

Механизъм за контрол - мярка или съвкупност от мерки, които имат за цел да изменят величината на риска за сигурността на информацията.

Контрол на достъпа - начин да се гарантира, че достъпът до ТУМГ или негови съставни части, е оторизиран и ограничен на базата на изискванията на Изборния кодекс.

Електронен дневник на изборния процес - носител или набор от носители на информация, които се ползват за отбелязване на особености и отклонения от предвидения режим в процеса на гласуване и обработка на информацията. Терминът „електронен дневник“ е посочен в чл. 213, ал. 2, т. 14 от Изборния кодекс. В техническата документация за този информационен актив са използвани и множество други термини като log файлове, лог файл и електронни log-ове.

Електронна избирателна кутия - папка (директория) върху криптираната част на ЗТУ, която съдържа всички електронни записи със съдържанието на подадените и потвърдени гласове (вот) на избирателите. Всеки запис е отделен файл в криптиран вид, записан по начин, който гарантира непроследимостта на вота.

Приложен софтуер - специализирани програми, предназначени за решаване на конкретните задачи по подготовка, осъществяване на процеса на гласуване и отчитане на резултатите от него.

Криптиращ/декриптиращ софтуер - софтуер, който осигурява интегритета и конфиденциалността на прехвърляната информация чрез криптиране на данните.

Модул за валидация и обобщаване - софтуерен модул, чрез който да се разпознава 2D баркодът, отпечатван на бюлетината от машинно гласуване и да се обобщават данните в рамките на избирателната секция.

4. Подготовка за оценяване на съответствието

Ръководителите на институциите по чл. 213а, ал. 2 могат със заповед да упълномощят компетентно лице от ръководството на съответната институция, което да изпълнява дейностите, свързани с удостоверяване на типа на техническите устройства за машинно гласуване.

Подготовката на процеса за оценяване на съответствието включва:

4. 1. Назначаване на екипи за оценяване на съответствието на доставения тип ТУМГ - извършва се със заповед на министъра на електронното управление, председателя на БИМ и председателя на УС на БИС. Екипите включват експерти от МЕУ, БИМ и БИС, както и външни експерти с подходящата професионална квалификация, компетентност и опит в съответната област, удостоверени с документи. В заповедта изрично се посочва кои експерти ще бъдат включени в съответните екипи за извършване на дейностите, описани в т. 6. от настоящата Методика. Със заповедта се определят и ръководителите на конкретните екипи.

Преди започване на дейностите по изпитване, проверка, оценяване и удостоверяване, членовете на екипите и министъра на електронното управление, председателя на БИМ

и председателя на УС на БИС подписват декларации за неразкриване на информация и за липса на конфликт на интереси.

4.2. Получаване на образци от представителна извадка от ТУМГ, както и на съпътстващата ги документация, с която ЦИК и Изпълнителят/ите на дейностите по техническата подготовка, логистика и провеждането на машинно гласуване разполагат относно тях и за които са преценили, че са достатъчни за целите на удостоверяване на съответствието.

Наборът от представените документи включва, но не се ограничава до:

- Списък на ТУМГ, които ще бъдат ползвани в предстоящите избори, включително и резервните такива, в електронен машинночетим формат;
- Техническото/ите предложение/я на Изпълнителя/ите по договора/ите за доставка на продукти и услуги;
- Договорът/ите с Изпълнителя/ите, в който/които са фиксирани техническите изисквания към доставяните продукти и/или услуги, определени от ЦИК, съгласно чл. 213, ал 3 от Изборния кодекс;
- Планът за провеждане на избори с използване на машинно гласуване, съгласно чл. 213б, ал. 3 от Изборния кодекс;
- Техническа документация, спецификации, инструкции, указания, ръководства, свързани с ТУМГ и дейностите на Изпълнителя/ите в процесите по надграждане на софтуера, подготовка, инсталиране, тестване и логистика;
- Документи, доказващи съответствието на ТУМГ или техни компоненти с изискванията на ИК, които са издадени от трета независима страна;
- Сертификати за съответствие на Изпълнителя/ите с изискванията на български, европейски и международни стандарти, според техническите изисквания на ЦИК, като БДС EN ISO/IEC 27001, БДС ISO/IEC 20000 и др., които доказват компетентност в предметната област;
- Политики, правила и процедури за управление на сигурността на информацията и за процесите по подготовка, логистика и поддръжка на ТУМГ, прилагани от ЦИК и Изпълнителя/ите на дейностите по подготовка, логистика и поддръжка на ТУМГ;
- Декларация за съответствие и идентичност от Изпълнителя/ите на дейностите по подготовка, логистика и поддръжка на ТУМГ;
- Списък на актуализациите, промените и корекциите в системното и приложното програмно осигуряване и в управлението и настройките на апаратните средства, периферните устройства, средствата за достъп и консумативите за ТУМГ;
- Опис на предоставените информационни активи.

Дейностите по Процедурите по тестване/изпитване, проверка и оценяване се извършват върху представителна извадка на образци от ТУМГ, които предстои да бъдат ползвани в предстоящите избори. Представителността на извадката се гарантира от използването на т.нар. „метод на извадка с произволни числа“, при който шансът или вероятността да

се избере дадено ТУМГ е същият, както вероятността да се избере всяко друго устройство, което ще бъде използвано за нуждите на предстоящите избори.

Случайността на избора на образците се осигурява посредством т.нар. „генератор на случайни числа“, който се използва за определяне на серийните номера на ТУМГ, които ще бъдат подложени на изпитвания/тестове, проверки, оценяване и удостоверяване, съгласно изискванията на настоящата Методика.

За целите на гореописаните дейности, след обявяване на датата на произвеждане на изборите, институциите по чл. 213а, ал.2 от Изборния кодекс изискват с писмо до ЦИК пълния списък на устройствата за машинно гласуване, които ще бъдат ползвани в предстоящите избори, който включва и резервните устройства, ако са предвидени такива.

Ръководителите на екипите по т. 4. 1. определят, посредством генератор на случайни числа, серийните номера на устройствата, които ще бъдат ползвани за нуждите на процеса по удостоверяване на съответствието. За извършените действия се съставя протокол, който се изпраща на ЦИК, за предоставяне в срок на ТУМГ, подлежащи на изпитване/тестване, проверка, оценяване и удостоверяване на съответствието, съгласно т. 4 на настоящата Методика. ЦИК предоставя образците от представителна извадка от ТУМГ, които предстои да бъдат ползвани в изборите и които имат идентични характеристики и функционалност с тези на останалите устройства, което се доказва с декларация за съответствие и идентичност от Изпълнителя/ите, в комплект с инсталирани и настроени базов и приложен софтуер. Наред с посоченото, се предоставят всички останали компоненти, като смарткарти, записващи технически устройства със софтуер за криптиране/декриптиране и тестови, и реални данни за конкретни СИК - за провеждане на технологични и функционални изпитвания, необходимите консумативи, както и всяка друга документация, която е преценена за уместна и достатъчна с цел доказване на съответствието на характеристиките, функционалността и сигурността на ТУМГ с изискванията на чл. 213, ал. 3 от Изборния кодекс и изискванията на техническата спецификация.

Предвид обстоятелството, че изборната администрация може да прави промени в регистрираните кандидатски листи до 7 дни преди изборния ден и поради факта, че информацията в тези листи не е предмет на удостоверяване от институциите по чл. 213а, ал. 2, е допустимо сценариите по процедурите за изпитвания/тестване да бъдат реализирани с първоначално регистрираните кандидатски листи или с примерни/тестови данни и кандидатски листи, в които броят на кандидатите задължително трябва да съвпада или да е по-голям от този на регистрираните кандидатски листи.

За извършването на пълноценни изпитвания от страна на специализираните екипи за оценяване на съответствието институциите по чл. 213а, ал. 2 от Изборния кодекс изискват от ЦИК програмния (изходния) код на приложния (реализиращ изборните процеси) софтуер, наличния софтуер за тестване и диагностика и всички администраторски права и средства за оторизация с цел осигуряване на пълен достъп

до базовия, приложния, криптиращия софтуер и до софтуера за оторизация, както и за достъп до компонентите на апаратната част на предоставения тип ТУМГ.

4.3. Преглед на предоставените информационни активи и анализ на документацията - извършва се от екипите по т. 4. 1. и включва запознаване с предоставената от ЦИК документация по т. 4. 2., в т.ч. ръководства, инструкции, указания, технически спецификации, резултати от оценки, извършени от трета независима страна, както и всички други документи, предоставени от Производителя и Изпълнителя, които според тях доказват съответствие на отделна съставна част, периферно устройство, консумативи или на ТУМГ в цялост с изискванията на чл. 213, ал. 3 от Изборния кодекс и изискванията на техническата спецификация.

В случай на установяване на неокомплектованост или липса на отделна съставна част, компоненти, периферно устройство, консумативи и/или документация, незабавно писмено се информира ЦИК и Изпълнителя/ите по договорите за доставка и/или техническо осигуряване и се определя срок за отстраняване на констатирания недостатък.

5. План за оценяване и удостоверяване на съответствието

Планът за оценяване и удостоверяване на съответствието (по-нататък „Плана“) се разработва от ръководителите на екипите по т. 4. 1. от настоящата Методика в 3-дневен срок от извършване на прегледа на предоставените информационни активи и анализа на документите по реда на т. 4. 3 от настоящата Методика.

В Плана за оценяване и удостоверяване на съответствието се включват дейностите по тестване/изпитване, проверка и оценяване, които предстои да бъдат извършени, съставът и задълженията на екипите по т. 4. 1., както и сроковете за извършване на дейностите, описани в приложенията към настоящата Методика и за изготвянето на Протоколи за резултатите от тези дейности и Доклад за оценяване на съответствието.

6. Методи и процедури за оценяване на съответствието

Наборът от методи и процедури за оценяване на съответствието, предвидени в приложенията към настоящата Методика , включва, но не се ограничава до:

- Проверка на валидността и автентичността на документи за оценяване на съответствието на Изпълнителя/ите и на доставения тип ТУМГ, негова съставна част, периферно устройство или консумативи, издадени от трета независима страна;
- Проверка за съответствие с изискванията към хардуерната конфигурация на доставения тип ТУМГ;
- Проверка и оценка на функционалността на ТУМГ за съответствие с техническите и функционалните изисквания към него;

- Проверка за съответствие с изискванията по отношение сигурността на информацията, която се въвежда, обработва, съхранява и извежда от доставения тип ТУМГ.

Обхватът на проверките, продължителността на тестовете, както и крайният резултат са в пряка зависимост от комплектността, количеството и качеството на документите, предоставени от ЦИК, както и от времевия отрязък, който е наличен за целите на удостоверяване на съответствието.

При извършване на проверките за съответствие, ТУМГ, кодът и всички предоставени материали и информация, се обработват и съхраняват в контролирана среда - отделни, защитени физически помещения, недостъпни от неоторизиран персонал, с въведени технически и/или организационни мерки за контрол на достъп и видео наблюдение, за целия срок на извършване на проверките. Достъпът до помещенията е ограничен само до упълномощените за това лица като всяко влизане и излизане задължително се документира най-малко със следните атрибути: дата, три имена, ведомство, час на влизане, час на излизане, подпис или номер на персонална карта за достъп, при техническа реализация.

Всяка от институциите (МЕУ, БИМ И БИС), която участва в процеса по проверка и удостоверяване на съотвествието, разработва и приема вътрешни правила за дейността, която осъществява. Правилата следва да осигуряват минимално общо ниво на защитеност, както и да гарантират пълнотата, интегритета и конфиденциалността на дейността.

6.1 Проверка на валидността и автентичността на документи за оценяване на съответствието, издадени от трета независима страна

Предвид специфичните характеристики и функционалност на техническите устройства за електронна обработка на данни, в световен мащаб се е наложила практиката производителят и Изпълнителят по договора за доставка и инсталиране да подлагат своите продукти и/или техни съставни части на оценяване на съответствието от трета независима страна. Резултатът от това оценяване се изразява в издаване на официални документи - сертификати (certificates), доклади (technical reports) или протоколи, в зависимост от критериите и документите, спрямо които е било оценено съответствието.

Компетентните органи за сертифициране на продукти трябва да са акредитирани, т.е. да са били приведени в съответствие с EN ISO/IEC 17065 „Оценка на съответствието - Изисквания към органите за сертификация на продукти, процеси и услуги“ - международен стандарт за доказване на компетентността на органи за оценяване на съответствието (ООС), които извършват сертифициране на продукти, процеси и услуги.

Оценяването и акредитацията на ООС се извършва от националните органи за акредитация, които са общопризнати на базата на многостранни споразумения. На свой ред, самите национални органи за акредитация се оценяват и признават от международните партньори в съответствие със стандарта EN ISO/IEC 17011. Европейската организация ЕА е институцията, официално определена от Европейската комисия в Регламент (ЕО) № 765/2008 в областта на разработването и поддържането на

многостранното споразумение за взаимно признаване (EA MLA), основано на хармонизираната инфраструктура за акредитация в рамките на Европейския съюз.

Органите за оценка на съответствие, които са акредитирани в конкретната област на компетентност, изпълняват функциите на трета, независима страна за сертифициране на продукти, процеси и услуги спрямо съответните стандарти за сигурност на информацията, безопасност, електромагнитни смущения, влагоустойчивост, температурни параметри и т.н.

В международен мащаб на принципа на взаимното признаване се прилага и подхода на сертифициране на продукти, процеси и услуги за съответствие по общопризнати схеми за сертификация. Така например, за електротехнически съоръжения и техни съставни части, които попадат в обхвата на стандартите на IEC (*International Electrotechnical Commission)*, одобрени за използване в системата на IECEE, се прилага специфична схема на сертифициране, известна под наименованието "сертификационна CB схема на IECEE за взаимно признаване на сертификати на база изпитване на електротехнически съоръжения и съставни части", която е наричана за краткост "сертификационна CB схема".

За да се потвърди валидността и автентичността на представените документи за съответствие, се извършва проверка, която се отнася, но не е ограничена до:

- Формално съдържание на документите;
- Обект/предмет на оценяваното съответствие;
- Основание за издаване на документа за съответствие - нормативен акт, стандарт, схема, метод, ръководство, процедура и/или друг документ, регламентиращ процеса на изпитване и оценка на съответствието;
- Критерии за оценяване на съответствието;
- Орган за оценяване на съответствието (ООС), издал съответния документ за оценка;
- Допълнителна информация и приложения;
- Орган, който е акредитирал/оторизирал органа за оценяване на съответствието да издава сертификати/доклади за оценяване на съответствие в конкретната област.

Преди да пристъпи към проверка на документите, екипът за оценяване извършва проверка относно съответствието на модела, серийния номер и партидата на предоставените ТУМГ от ЦИК с тези, описани в списъка на доставените технически устройства, които престои да се използват в рамките на изборния ден.

При установяването на валиден и автентичен сертификат/доклад за оценено съответствие, издаден от общопризната трета независима страна, не е необходимо да бъдат извършвани изпитвания/тестване и проверки в областта и в обхвата на тази сертификация.

Процедурата за проверка и потвърждаване на валидността и автентичността на представени от Изпълнителя документи, издадени от трета независима страна за съответствие на Изпълнителя/ите и на доставения тип ТУМГ и/или негови компоненти с изискванията на ИК и техническите изисквания към апаратната и програмната част на ТУМГ, които са определени от ЦИК, е описана в Приложение № 1 на настоящата Методика.

6.2. Проверка и оценка за съответствие с изискванията към хардуерната конфигурация на ТУМГ

Методите и процедурите за изследване на доставения тип ТУМГ включват, но не са ограничени до:

- Проверка на външен вид и маркировка на вградените компоненти и съответствие с техническата документация, по отношение заложените в техническите изисквания към апаратната и програмната част на ТУМГ по определени от ЦИК параметри на компонентите;
- Проверка на вградените периферни устройства по отношение на техническите характеристики, начина им на функциониране и обслужване;
- Проверка за наличие на неидентифицирани или неописани в документацията компоненти;
- Определяне на критичните за функционирането на ТУМГ компоненти и системи;
- Проверка на конструктивното изпълнение на монолитния корпус на ТУМГ по отношение на ограничаване на физическия достъп до критичните за работата компоненти, осигуряване на оторизиран достъп до компоненти, за които е предвидено обслужване, предвидените нива на физически достъп при експлоатация от членове на секционните избирателни комисии и избирателите;
- Технически преглед на представените доклади, декларации и протоколи за електробезопасност, електромагнитна съвместимост, температурен диапазон на използване, допустими вибрации, както и на други приложими документи, правила и начини на транспорт и съхранение;
- Проверка за работата на ТУМГ при самия процес на гласуване - възможно ли е един избирател да гласува повече от веднъж;
- Проверка дали физически има достъп до комуникационните интерфейси на машината и проверка дали те са изключени;
- Проверка дали има възможност само за гласуване и дали е възможен неразрешен достъп до машината за други цели.

Преди да пристъпи към реализиране на дейностите по Плана за оценяване, екипът за оценяване извършва проверка относно съответствието на модела, серийния номер и партидата на предоставените ТУМГ от ЦИК с тези, описани в списъка на доставените технически устройства.

Предвид естеството на дейностите по тази точка от настоящата Методика, които са свързани с отваряне на монолитния корпус и изследване на съставните части на ТУМГ, устройството, което е предоставено за целите на техническото изследване, не трябва да бъде използвано в последствие в рамките на изборния процес и остава на разположение на удостоверяващите институции.

Процедурата по проверка и оценка за съответствие с изискванията към хардуерната конфигурация на доставения тип ТУМГ е описана в Приложение № 2 на настоящата Методика.

6.3. Проверка и оценяване на функционалността на ТУМГ за съответствие с техническите и функционалните изисквания към ТУМГ

Проверява се и се оценява функционалността на техническото устройство за машинно гласуване за съответствие с техническите и функционалните изисквания към него.

За целта процедурата по проверката е структурирана в последователност, съответстваща на технологичните процеси по време на изборния ден с използване на ТУМГ и обхваща проверка на функциите и дейностите, извършвани непосредствено от членовете на СИК и избирателите в процеса на гласуване с ТУМГ в рамките на изборния ден:

- Проверка на комплектността на ТУМГ и потребителската документация;
- Проверка за удостоверяване на оторизиран достъп до ТУМГ и базови функционалности на ТУМГ:
  - Стартиране на ТУМГ със смарткарта за управление, верификация на електронния сертификат и визуализиране на номенклатурните данни заредени от ЗТУ;
  - Валидация на смарткартите за конкретна избирателна секция;
  - Визуализация на номенклатурните данни и бюлетина;
  - Проверка на функционалността на периферните устройства на ТУМГ чрез вътрешен тест.
- Проверка на функциите на ТУМГ по време на изборния процес:
  - Активиране на ТУМГ в режим на за гласуване с вид бюлетини според конфигурацията на съответния избор;
  - Реализиране на избор на партия/коалиция/независим кандидат или не подкрепям никого;
  - Проверка на избора;
  - Отпечатване на бюлетина от машинно гласуване;

- Показване броя на гласувалите след въвеждане на смарткарта за управление.

- Проверка за допълнителни функционалности на ТУМГ по време на изборния ден;
- Проверка на функциите на ТУМГ, свързани с края на изборния ден;
- Проверка на функциите на ТУМГ, свързани със записване на резултатите от гласуването върху ЗТУ;
- Проверка на ТУМГ за функциониране в аварийни ситуации;
- Проверка на функциите на ТУМГ за реализиране на подход за използване на повече от една ТУМГ в една избирателна секция;
- Подготовка на ТУМГ за избори, провеждани в чужбина (ако е приложима).

Процедурата за **Проверка и оценяване на функционалността на ТУМГ за съответствие с техническите и функционалните изисквания към ТУМГ** е описана в Приложение № 3.

6.4. Проверка и оценка за съответствие с изискванията към сигурността на информацията, която се въвежда, обработва, съхранява и извежда от ТУМГ

Проверката на сигурността включва физическа проверка и проверка на софтуера. Проверката включва, но не се ограничава до следните компоненти:

Проверка на конфигурацията на операционната система

- Проверка актуализирани ли са софтуерните компоненти;
- Проверка деактивирани ли са ненужни процеси в операционната система на ТУМГ;
- Проверка премахнати ли са ненужни firmware драйвери и модули на ядрото в операционната система;
- Проверка за уязвимости в операционната система;
- Оценка на нивото на въздействие на евентуално открити уязвимости в операционната система.

Проверка на софтуерната реализация

- Проверка за уязвимости в приложния софтуер;
- Оценка на нивото на въздействие на евентуално открити уязвимости в приложния софтуер;
- Проверка за зависимости в изходния код;
- Проверка за уязвимости в параметризиращия софтуер;

- Оценка на нивото на въздействие на евентуално открити уязвимости в параметризиращия софтуер;
- Проверка на базова/и СА верига/и, използвана/и при конкретните избори;
- Проверка за възможност за разкриване на вота;
- Проверка на заложената функционалност и обхвата на хешираните файлове и директории, участващите в приложението за проверка на хеш кода (HashExtractor);
- Детайлна проверка на предвиденото поведение на всички места в изходния код, които работят с файла или файловете за съхранение на гласове;
- Проверка за наличие на обфускиран (прикрит) код, в стандартните функционалности на операционната система;

Процедурата за проверка и оценка за съответствие с изискванията към сигурността на информацията, която се въвежда, обработва, съхранява и извежда от ТУМГ е описана в Приложение № 4 на настоящата Методика.

7. Процес на удостоверяване на съответствието

7.1. Констатациите и резултатите от извършените проверки и тестове се отразяват в Протоколи от проверки и изпитвания/тестове, които се изготвят и подписват от екипите по т. 4. 1.

7.2. На базата на Протоколите по т. 7. 1. ръководителите на екипи изготвят Доклад за оценяване на съответствието на типа ТУМГ с изискванията по чл. 213, ал. 3 от Изборния кодекс и изискванията на техническата спецификация. Докладът се подписва от ръководителите на екипите.

7.3. Докладът, ведно с Протоколите по т. 7. 1., се предоставят на министъра на електронното управление, председателя на БИМ и председателя на УС на БИС за произнасяне съгласно чл. 213а, ал. 2 от Изборния кодекс с оглед удостоверяване или отказ от удостоверяване на съответствието.

7.4. В 2-дневен срок от предоставянето на документите по т. 7. 3. министърът на електронно управление, съвместно с председателя на БИМ и председателя на УС на БИС издават решение за удостоверяване/неудостоверяване на съответствието на доставения тип ТУМГ с изискванията на чл. 213, ал. 3 от Изборния кодекс и изискванията на техническата спецификация. Удостоверяването на съответствието е към момента на предоставяне на ТУМГ със съответния софтуер (базов, приложен, криптиращ и софтуер за оторизация) и периферни устройства. Всяка последваща промяна в софтуера, хардуера и/или консумативите, извършена след изготвянето на Доклада и издаване на решението за удостоверяване не попада в обхвата на извършеното удостоверяване.

7.5. В случай на констатирани несъответствия с изискванията на чл. 213, ал. 3 от Изборния кодекс и изисквания на техническата спецификация, същите се отразяват в

Протоколите по т. 7. 1. и ведно с Доклада по т. 7. 2., и решението по т. 7. 4. се предоставят на ЦИК за предприемане на последващи коригиращи действия от организационно или технологично естество.

7.6. С цел осигуряване на прозрачност на дейностите, възможност за допълнителни проверки и за сравнителни анализи при възникване на спорове и инциденти с ТУМГ в рамките на изборния процес, предоставените от ЦИК ТУМГ и други информационни активи се съхраняват в институциите по чл. 213а, ал. 2 от ИК до един месец след обявяване на окончателните резултати от изборите, след което се предават на собственика им.

7.7. В случай, че за целите на удостоверяването не бъдат предоставени в цялост или отчасти изисканите от МЕУ, БИМ и БИС информационни активи, в т.ч. системен и приложен софтуер,драйвъри, хардуер, средства и права за достъп, криптографски инструменти, консумативи и други, това обстоятелство задължително се вписва в Доклада за оценяване на съответствието и в Решението за удостоверяване/неудостоверяване на съответствието.

8. Удостоверяване на съответствието на технически устройства за машинно гласуване, които вече са използвани в предходни избори

В случаите, в които се извършва удостоверяване на съответствието с изискванията на Изборния кодекс и изискванията на техническата спецификация на използвани в предходни избори ТУМГ, екипите за оценяване на съответствието извършват следните дейности:

- Преглед за промени в релевантното европейско и национално законодателство;

- Преглед за промени в предоставената от ЦИК документация;

- Преглед за промени в приложния софтуер (деинсталиране на приложния софтуер от предходните избори, модифициране и инсталиране на софтуера за текущите избори, генериране на криптографските ключове, криптиране на системата, частичен одит на елементи от системата за управление сигурността на информацията (БДС EN ISO/IEC 27001) на изпълнителя на посочените дейности (ако това е приложимо);

- Анализ на документи, отразяващи опита и поуките от предходни избори в контекста на изискванията за предстоящите избори (ако това е приложимо);

- Преглед на състоянието на взетите/предоставените образци на ТУМГ.

Ръководителите на екипи разработват актуализиран План за оценяване и удостоверяване на съответствието по т. 5 от настоящата Методика, съдържащ само дейностите, които ще бъдат реализирани с оглед резултатите от посочените по-горе дейности и резултатите от реализираните във връзка с предходни избори процедури по тестване/изпитване, проверка и оценяване.

Дейностите по Процедурите по тестване/изпитване, проверка и оценяване се извършват върху представителна извадка на образци от ТУМГ, които предстои да бъдат ползвани в предстоящите избори. Осигуряването на случайност на избора на образците и представителността на извадката и действията по вземане/предоставяне на образците се осъществяват по реда на т. 4. 2 на настоящата Методика.

След изпълнение на дейностите, съгласно актуализирания План за оценяване и удостоверяване на съответствието, се изготвят Протоколи по т. 7. 1., които следват формата на Процедурите № 1 - 4. След подписването на Протоколите от членовете на съответните екипи, ръководителите на екипи разработват Доклад за оценяване на съответствието, който се предоставя на министъра на електронното управление, председателя на БИМ и председателя на УС на БИС за вземане на решение съгласно чл. 213а, ал. 2 от Изборния кодекс с оглед удостоверяване на съответствието.

9. Участие на външни наблюдатели в процеса на удостоверяването

В съответствие с чл. 213а, ал. 3 от Изборния кодекс в процеса на удостоверяването може да участват и представители на партиите, коалициите и инициативните комитети, регистрирани за участие в изборите, на български неправителствени организации, които са регистрирали наблюдатели за съответния вид избор и на Българската академия на науките.

В съответствие с разпоредбите на чл. 213б от Изборния кодекс, лицата по чл. 213а, ал. 3 от кодекса получават достъп до информационните активи и до дейностите по изпитване, проверка и оценяване на съответствието след подаване на заявление по правила, утвърдени от министъра на електронното управление, председателя на БИМ и председателя на УС на БИС и в съответствие с реда, определен от Централната избирателна комисия.

Наблюдателите, допуснати до участие в процеса по удостоверяване подписват декларации за неразкриване на информация и за липса на конфликт на интереси.

В дейностите, свързани с удостоверяване на съответствието не могат да участват външни наблюдатели, които са били ангажирани по един или друг начин в процесите по организиране, подготовка, инсталиране, настройване, параметризиране и логистика на ТУМГ или негови компоненти, поради наличие на конфликт на интереси.

10. Заключение

Настоящата Методика е изготвена от експертна работна група, определена със заповед № МЕУ-15228/27.09.2023 г. на заместник министъра на електронното управление. При нейното разработване са използвани добрите практики, разписани в европейски и международни стандарти, както и националното и европейското законодателство, изрично посочени в библиография към Методиката.

Методиката за удостоверяване на съответствието се актуализира при промяна в европейското или националното законодателство, промени в типа на ТУМГ, промени в процеса по подготовката и логистиката на ТУМГ, при промяна в техническите изисквания към апаратната и програмната част на ТУМГ, които са определени от Централната

избирателна комисия съгласно чл. 213, ал. 3 от Изборния кодекс и/или по предложение на две от институциите по чл. 213а, ал. 2 от Изборния кодекс. Новата версия на Методиката се представя от работната група и се утвърждава от министъра на електронното управление, председателя на БИМ и председателя на УС на БИС, или от упълномощени от тях лица.

Забележка: Методите и процедурите, чрез които ще се оценява съответствието, могат да бъдат актуализирани след преглед и анализ на получените от ЦИК информационни активи, техническа документация, техническото предложение и декларацията за съответствие и идентичност на Изпълнителя, софтуера и представителна извадка от образците на ТУМГ, които ще бъдат използвани в съответните избори.

Приложения:

1. Процедура за проверка на валидността и автентичността на документи за оценяване на съответствието на Изпълнителя/ите и на ТУМГ или негова съставна част, издадени от трета независима страна - Приложение № 1;
2. Процедура по проверка и оценка за съответствие с изискванията към хардуерната конфигурация на устройствата - Приложение № 2;
3. Процедура по проверка и оценяване на функционалността на ТУМГ за съответствие с техническите и функционалните изискванията към ТУМГ - Приложение № 3;
4. Процедура по проверка и оценка за съответствие с изискванията към сигурността на информацията, която се въвежда, обработва, съхранява и извежда от ТУМГ - Приложение № 4.

Настоящата Методика е утвърдена на 12.02.201 г., изменена и допълнена на 14.06.2021 г. със заповед № ДАЕУ-9513/14.06.21 г., изменена и допълнена на 19.10.2021 г. със заповед № ДАЕУ-17250/19.10.2021г., изменената и допълнена на 01.09.2022 г. със заповед № МЕУ-8701/01.09.2022 г., изменена и допълнена на 13.03.2023 г. със заповед № МЕУ-4159/13.03.2023г.

БИБЛИОГРАФИЯ

Регламент (ЕО) № 765/2008

Закон за електронното управление

Закон за киберсигурността

Закон за електронния документ и електронните удостоверителни услуги

Закон за електронната идентификация

Закон за измерванията

Закон за техническите изисквания към продуктите

Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги

Наредба за минималните изисквания за мрежова и информационна сигурност

Наредба за съществените изисквания и оценяване на съответствието на електрически съоръжения, предназначени за използване в определени граници на напрежението

Наредба за условията и реда за пускане на пазара на електрическо и електронно оборудване във връзка с ограниченията за употреба на определени опасни вещества

Наредба за излязлото от употреба електрическо и електронно оборудване

Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States

on standards for e-voting

Решение № 768/2008/ЕО на ЕП и на Съвета от 9 юли 2008 година относно обща рамка за предлагането на пазара на продукти и за отмяна на Решение 93/465/ЕИО

БДС EN ISO/IEC 17000 Оценяване на съответствието. Речник и общи принципи (ISO/IEC 17000:2020)

БДС EN ISO 19011 Указания за извършване на одит на системи за управление

БДС EN ISO/IEC 17020 Оценяване на съответствието. Изисквания за дейността на различни видове органи, извършващи контрол

БДС EN ISO/IEC 17025 Оценяване на съответствието. Общи изисквания за компетентността на лаборатории за изпитване и калибриране

БДС EN ISO/IEC 17065 Оценяване на съответствието. Изисквания към органите за сертификация на продукти, процеси и услуги (ISO/IEC 17065:2012)

БДС EN ISO/IEC 17067 Оценяване на съответствието. Основни принципи на сертификацията на продукти и указания за схеми за сертификация на продукти (ISO/IEC 17067:2013)

БДС EN ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model

БДС EN ISO/IEC 15408-2:2022 — Evaluation criteria for IT security — Part 2: Security functional components

БДС EN ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components

БДС ISO/IEC 20000-1:2018 Информационни технологии. Управление на услуги. Част 1: Изисквания относно системата за управление на услуги (ISO/IEC 20000-1:2018)

БДС ISO/IEC 20000-2:2019 Информационни технологии. Управление на услуги. Част 2: Ръководство за прилагане на системи за управление на услуги (ISO/IEC 20000-2:2019)

Всички приложими стандарти от групата ISO/IEC 200xx

БДС EN ISO/IEC 27000:2020 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Общ преглед и речник

БДС EN ISO/IEC 27001:2022 Сигурност на информацията, киберсигурност и защита на поверителността. Системи за управление на сигурността на информацията. Изисквания (ISO/IEC 27001:2022)

БДС ISO/IEC 27005:2023 Сигурност на информацията, киберсигурност и защита на поверителността.Управление на риска за сигурността на информацията (ISO/IEC 27005:2022).

Всички приложими стандарти от групата EN ISO/IEC 270xx

БДС ISO 31000:2018 Управление на риска. Указания

БДС EN 31010:2019 Управление на риска. Методи за оценяване на риска

NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations

NIST SP 800-30-1: Guide forConducting Risk Assessments

ISO/IEC 7816-1;2;3….. Identification cards — Integrated circuit cards:

- *— Part 1: Cards with contacts — Physical characteristics*
- *— Part 2: Cards with contacts — Dimensions and location of the contacts*
- *— Part 3: Cards with contacts — Electrical interface and transmission protocols*
- *— Part 4: Organization, security and commands for interchange*
- *— Part 5: Registration of application providers*
- *— Part 6: Interindustry data elements for interchange*
- *— Part 7: Interindustry commands for Structured Card Query Language (SCQL)*
- *— Part 8: Commands for security operations*
- *— Part 9: Commands for card management*
- *— Part 10: Electronic signals and answer to reset for synchronous cards*
- *— Part 11: Personal verification through biometric methods*
- *— Part 12: Cards with contacts — USB electrical interface and operating procedures*
- *— Part 13: Commands for application management in a multi-application environment*
- *— Part 15: Cryptographic information application*

БДС EN 62368-1 Аудио-/видеоустройства, устройства/съоръжения за информационни и комуникационни технологии. Част 1: Изисквания за безопасност