

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

СПРАВКА ЗА ОТРАЗЯВАНЕ НА ПОСТЪПИЛИТЕ ПРЕДЛОЖЕНИЯ, СТАНОВИЩА И ВЪЗРАЖЕНИЯ ОТ ПРОВЕДЕНАТА ОБЩЕСТВЕНАТА КОНСУЛТАЦИЯ НА ПРОЕКТА НА АКТУАЛИЗИРАНА 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

№	Дата и начин на постъпване на становището (официално, по ел. поща, чрез Портала за обществен и консултации и т.н.)	Име на лице/наименование на ЮЛ	Декларирани данни дали лицето действа от свое име или защитава позиция от името на друго лице/група лица	Предложения становища	Приети/не приети	Мотиви
1	25.09.2026 г. чрез docs@migt.government.bg	Обединение Честни Избори	☐ Лицето защитава позиция от името на друго лице/група лица:	I. ПРЕДЛОЖЕНИЯ КЪМ ТЕКСТА НА МЕТОДИКАТА 1. Проследимост между удостоверения изходен код и софтуера, инсталиран на машините Съгласно т. 7.4 от Методиката удостоверяването на съответствието е към момента на предоставяне на ТУМГ от ЦИК и всяка последваща промяна в софтуера не попада в обхвата му. Съгласно т. 3 от Решение № 216-ПВР от 15.09.2026 г. на ЦИК след удостоверяването се извършва доверено изграждане от удостоверения изходен код с UEFI ключове,	Не се приема	Съгласно разпоредбите на ИК институциите по чл. 213а, ал.2 „удостоверяват съответствието на доставения тип техническо устройство за машинно гласуване с изискванията по чл. 213, ал. 3 и изискванията на техническата спецификация“. В т. 4.3 от Методиката изрично е записано, че „за

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				притежавани от ЦИК. Правилата за доверено изграждане (отново уточняваме – в итерацията от изборите през април 2026 г.) предвиждат ЦИК да предостави изходен код, „преминал през проверка и оценка по т. 6.4 от Методиката“ (чл. 3, ал. 3, т. 1 от Правилата, приети с Решение № 4640-НС), но нито Методиката, нито Правилата предвиждат начин това да бъде установено. Методиката не изисква криптографските идентификатори на удостоверения изходен код да бъдат записани в Доклада или в Решението за удостоверяване. Веригата на доверие включва следните последователни звена: а) изходният код, проверен и удостоверен по реда на Методиката; б) изходният код, до който се предоставя достъп на граждани по чл. 213б, ал. 1 ИК; в) изходният код, подаден за довереното изграждане; г) резултатът от довереното изграждане – FSA архивът, инсталационното изображение и инструментите HashExtractor, Unlocker и LogExtractor (чл. 5, ал. 7 от Правилата); д) софтуерът, инсталиран на машините в избирателните секции. Звената от г) до д) са частично обезпечени чрез системния хеш код, системната разписка по чл. 218, ал. 7 ИК и извадковите проверки по чл. 213б, ал. 4, т. 1 и 2 ИК. Връзките между а), б) и в) обаче остават необезпечени. Не е установено, че изходният код, до който наблюдателите получават достъп по чл. 213б, ал. 1 ИК, е същият, който е удостоверен, нито че удостовереният код е същият, който се подава за довереното изграждане. Въпреки някои гранични срокове в	начало на дейностите по реална проверка, изпитване/тестване, оценяване и удостоверяване на съответствието се определя датата на установяване на пълно окомплектоване на ТУМГ, предоставени от ЦИК за процеса по удостоверяване във вида, в който предстои да бъдат използвани в изборния ден.“ В т.2. на Методиката са посочени нормативни основания и обхвата на удостоверяването. Удостоверяването на съответствието не може да включва процеси и компоненти, за които не са посочени съответстващи изисквания в ИК, подзаконовите нормативни актове и международните стандарти. Довереното изграждане е процес, с който са ангажирани Възложителят и Изпълнителят по конкретната обществена поръчка. Това е част от дейностите за подготовката на ТУМГ за нуждите на удостоверяването.
--	--	--	--	---	---

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				ИК, няма съвсем ясна хронологична верига между достъпа по чл. 213б, ал. 1 ИК, удостоверяването и довереното изграждане. Допълнително, тъй като инструментите за проверка (включително HashExtractor) се генерират от същото изграждане, а изходният им код също не е проследим до удостоверения, резултатът от проверката с тях също би следвало да се подsigури като проверимост. Предлагаме: 1.1. В т. 7.2 и т. 7.4 да се предвиди, че Докладът и Решението за удостоверяване съдържат криптографските идентификатори (хеш стойности с посочен алгоритъм) на удостоверения изходен код – поотделно за базовия софтуер, приложния софтуер, параметризиращия софтуер, инструментите HashExtractor, Unlocker, LogExtractor и инсталатора, както и на резултатите от тестовото изграждане по Приложение № 4.	1.1 Не се приема	Довереното изграждане не се реализира като резултат от удостоверяване на съответствието на ТУМГ. То е елемент от подготовката и привеждането на ТУМГ във „вида, в който предстои да бъдат използвани в изборния ден.“ от Възложителя и Изпълнителя по конкретната обществена поръчка. Съгласно разпоредбите на ИК институциите по чл. 213а, ал.2 „удостоверяват съответствието на доставения тип техническо устройство за машинно гласуване с изискванията по чл. 213, ал. 3 и изискванията на техническата спецификация“ Процесът по удостоверяване предвижда оценяване и удостоверяване на съответствието на ТУМГ в цялост, „във вида в който ще бъдат ползвани в деня на изборите“. В този контекст употребата на термини като „удостоверен софтуер“, „удостоверен хардуер“ или „удостоверени
--	--	--	--	---	--------------------------------	---

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				1.2. Тази препоръка не е обвързана стриктно с Методиката, но я включваме тук, тъй като логически следва от горното. Препоръчваме да се определи хронология на действията за всяка версия на софтуера. При предоставянето на достъп по чл. 213б, ал. 1 ИК, при което министерството подпомага ЦИК, да се посочват версията на изходния код и идентификаторите ѝ, както и статусът на процеса по удостоверяване към съответната дата, а лицата с достъп да имат право сами да изчислят идентификаторите или да наблюдават изчисляването им, и да ги съпоставят със записаните в Решението за удостоверяване съгласно т. 1.1. Би могло допълнително когато достъп се предоставя до версия, която още не е удостоверена, това да се посочва изрично, а след удостоверяването да се установява дали удостоверената версия съвпада с нея. 1.3. Да е публично достъпен методът за изчисляване на идентификаторите на изходния код, който се прилага във всички звена от а) до в), в това число хеш алгоритъм, допълнително елементи на хеширането, канонична форма на входните данни и всички останали необходими за повторимост инструменти. Допълнително препоръчваме употребата на поне един	1.2 Не се приема. 1.3 Не се приема	компоненти“ е недопустимо и неприложимо. Дефиницията за ТУМГ е посочена в т. 3 на Методиката. 1.2 Всички операции на институциите по чл. 213а, ал 2 от ИК, реализирани преди привеждането на машините във „вида, в който ще бъдат ползвани в изборния ден“ се определят като подготвителни дейности за осъществяване на реалните дейности по оценяване и удостоверяване. 1.3 Предоставянето на публичен достъп до информационните активи, използвани в, или свързани с процеса по удостоверяване, е от компетенцията на собственика на тези активи.
--	--	--	--	--	--	--

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				публичен инструмент за изчисляване – общодостъпен, с публикуван изходен код, независим от производителя на софтуера, с посочена версия. Резултатът да включва както общ идентификатор, така и списък с идентификатор за всеки файл, за да може евентуално несъответствие да бъде локализирано. 1.4. Да се създаде в Методиката нова точка „Проследимост на удостоверения софтуер“, която описва в хронологичен ред звената а)–д) и за всяко от тях определя извършваната проверка, отговорната институция и документа, в който се отразява резултатът. За прехода от а) към в) да се предвиди публично сравнение, преди началото на довереното изграждане и в присъствието на представители на удостоверяващите институции, на идентификаторите на подадения изходен код с идентификаторите по т. 1.1. При несъвпадение това обстоятелство се протоколира, а изграденият софтуер не се счита за обхванат от удостоверяването. 1.5. В т. 7.4 да се уточни, че довереното изграждане от удостоверения изходен код при потвърдено съвпадение по т. 1.4 не представлява последваща промяна по смисъла на тази точка, а всяко несъвпадение представлява такава промяна.	1.4 Не се приема 1.5 Не се приема	1.4 В процеса по удостоверяване и в изходните документи никъде не се използват термини като „уверен софтуер“, „уверен хардуер“ или „уверени компоненти“ (вижте т.1.1 по-горе). 1.5 Довереното изграждане не е част от процеса по удостоверяване. Не съществува такъв термин кат „уверен изходен код“ (вижте т.1.1 по-горе). Отделно от това, довереното изграждане се провежда от ЦИК.
--	--	--	--	---	---	--

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				1.6. В Приложение № 4, в дейността „Подготовка на базов образ на операционната система и базовия софтуер“, да се добави изискване за възпроизводимост на изграждането: документирана среда на изграждане, версии на компилаторите и зависимостите и проверка, че повторно изграждане от същия изходен код дава идентичен резултат. Идентификаторите от тестовото изграждане да се съпоставят с тези от довереното изграждане, като разликите, дължащи се единствено на подписването с различни UEFI ключове, се описват изрично.	1.6 Не се приема	1.6 Тестовото изграждане е неформална, вътрешна проверка, чиято цел е да провери доколко изходните резултати съвпадат с тези, получени от ЦИК вследствие на довереното изграждане. На оценяване на съответствието подлежат само криптографски примитиви, за които са посочени изисквания в техническата/ите спецификация/и.
				1.7. Инструментите HashExtractor, Unlocker, LogExtractor и инсталаторът да се удостоверяват като самостоятелни компоненти, включително техният изходен код. Проверката на HashExtractor да установява, че инструментът визуализира изчислената, а не очакваната стойност, и че резултатът „верен“/„неверен“ зависи единствено от сравнението с въведената при изграждането стойност. Да се предвиди и извадкова проверка с инструмент, който не е резултат от същото изграждане, включително чрез изчитане на вътрешната памет извън машината върху образа по т. 6.2 от Методиката, във връзка и с предложенията по т. 1.3.	1.7 Не се приема	1.7 ТУМГ се удостоверяват за съответствие в цялост, спрямо изискванията, посочени в техническата/ите спецификация/и. Предоставянето на достъп по чл. 213б, ал. 1 ИК е от компетентността на ЦИК. МИДТ само подпомага ЦИК и това не е предмет на Методиката.
				1.8 В т. 2 „Нормативни основания и обхват“ би могло да се добави позоваване на чл. 213б, ал. 3	1.8 Не се приема.	1.8 Т.2 определя основанието и обхвата на

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				и 4 ИК, тъй като резултатите от удостоверяването са основа за действията по плана за машинно гласуване и за публикуването на криптографските идентификатори по чл. 213б, ал. 4, т. 3 ИК. 2. Изискванията, спрямо които се удостоверява съответствието Методиката многократно препраща към техническите изисквания, определени от ЦИК по чл. 213, ал. 3 ИК, и към техническата спецификация. Техническата спецификация към текущата обществена поръчка (Приложение № 1 към Решение № 53-ПВР от 26.08.2026 г.) има за предмет услуги по профилактика, инсталиране, логистика и поддръжка и не съдържа функционални изисквания към поведението на машините. Но техническите изисквания изглежда липсват в публичен и актуален вид на сайта на ЦИК. В резултат очакваните резултати в Приложения № 2–4 нямат проверим външен източник. Методиката сама посочва, че съгласно Recommendation CM/Rec(2017)5 схемата на удостоверяване трябва да бъде публично достъпна и всеобхватна. Предлагаме:		удостоверяването по чл. 213а, ал. 2 ИК. Чл. 213б, ал. 3 и 4 ИК уреждат действия, които извършва ЦИК: изготвянето на плана за машинно гласуване, извадковите проверки и публикуването на криптографските идентификатори. Тези действия са извън обхвата на Методиката.
--	--	--	--	--	--	--

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				2.1. В т. 2 да се посочат с номер и дата актът или актовете на ЦИК по чл. 213, ал. 3 ИК и техническата спецификация, спрямо които се извършва удостоверяването, по възможност и с хипервръзки. 2.2. Очакваните резултати в Приложения № 2–4 да се обвържат с конкретните разпоредби на чл. 213, ал. 2 ИК и с конкретните изисквания от актовете по т. 2.1, например чрез колона „Основание“. 2.3. Указанията на ЦИК, дадени в хода на удостоверяването, които съгласно определението в т. 3 се включват в понятието „технически изисквания“, да се дават писмено, да се протоколират и да се прилагат към Доклада. 2.4. Всяка промяна на очакван резултат спрямо предходната редакция на Методиката да се придружава от посочване на изискването, на което се основава. Пример за такава промяна без посочено основание е допълнителен сценарий 1 в т. 3.1 от Приложение № 3 (вж. т. 5.2 по-долу).	2.1 Приема се по принцип 2.2 Приема се по принцип. 2.3 Не се приема. 2.4 Приема се частично.	2.1 Методиката е рамков документ, който се прилага по отношение на всички видове избори. Затова конкретните актове на ЦИК се посочват с номер и дата в Плана за оценяване (т. 5), както и в Доклада. 2.2 В доклада се съдържа необходимата информация. 2.3 ЦИК не разполага с правомощия да дава указания на институциите по чл. 213а, в хода на процеса по удостоверяване. Цялата останала документация между органите по удостоверяване и ЦИК е описана в доклада. 2.4 Основанията за промените в очакваните резултати се посочват в справката за обществените консултации, а при нужда и в мотивите към проекта.
--	--	--	--	--	--	---

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				3. Основен документ на Методиката 3.1. Т. 6.2: проверката „възможно ли е един избирател да гласува повече от веднъж“ е заменена с по-обща формулировка. Предлагаме тя да бъде запазена наред с новата формулировка, тъй като пряко съответства на чл. 213, ал. 2, т. 9 ИК. 3.2. Т. 6.4, новото правило за преоценка на уязвимостите: да се посочи системата за оценка (CVSS 3.1 или по-нова версия, в съответствие с Приложение № 4) и да се изисква преоценката на всяка уязвимост, заедно с мотивите за нея, да се отразява в протоколите и в Доклада. 3.3. Т. 4.2: техническото предложение на изпълнителя е изключено от списъка на предоставяните документи, но продължава да фигурира в т. 2 и в Забележката към т. 10. Предлагаме текстовете да бъдат уеднаквени.	3.1 Приема се. 3.2 Не се приема. 3.3 Приема се.	Самата Методика не съдържа история на редакциите. Допълнителен сценарий е добавен в т.6 от Приложение №3, който е във връзка с последните изменения на ИК 3.1 Отражено е в текста. 3.2 В т.6.4 на Приложение 4 вече е посочена системата за оценка CVSS 3.1 или по-нова версия. Преоценката се отразява в протоколите и в Доклада. 3.3 Отражено е в текста
--	--	--	--	--	---	--

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				3.4. Т. 7: да се определи минимално съдържание на Решението за удостоверяване – версии и криптографски идентификатори на удостоверения софтуер (т. 1.1), серийни номера на изпитаните образци, непредоставени информационни активи (т. 7.6), констатирани незначителни несъответствия и участвалите наблюдатели по чл. 213а, ал. 3 ИК. Допълнително по-долу (т. 8 и т. 9) предлагаме протоколите и решението да бъдат публикувани в интерактивен, достъпен и четим в уеб-формат вид извън официалния си документален вид.	3.4 Не се приема.	3.4. Решението е функция на доклада и протоколите към него, поради това не е целесъобразно предварително да бъдат определени неговото минимално съдържание.
				3.5. Т. 10: би могло да се възстанови заключителното изречение, че Методиката се утвърждава със заповед на министъра на иновациите и дигиталната трансформация, председателя на БИМ и председателя на УС на БИС, в съответствие с чл. 213а, ал. 2 ИК, тъй като отпадането му не е съвсем изяснено.	3.5 Приема се.	3.5 Отразено е в текста.
				4. Приложение № 2		
				4.1. Т. 5.2: заглавието („...според техническата документация“) може да се приведе в съответствие с новото съдържание, което представлява функционална проверка по време на тестов изборен ден.	4.1 Не се приема.	4.1. Функционалната проверка се извършва на базата на техническата документация.
				4.2. Т. 5.2, стъпка 9, и т. 6 от Приложение № 3 предвиждат сходни проверки, извършвани от различни екипи. Би могло да се посочи как се съпоставят резултатите и как се процедира при	4.2 Не се приема .	4.2. При констатиране на несъответствие с изискванията, от който и да е от екипите, се издава

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				разлика между тях. Изискването за пълна идентичност на данните да се допълни със сценариите по т. 5.6 по-долу. 4.3. Т. 9 и т. 1.1 от Приложение № 3 предвиждат комплект от 5 смарткарти (2 управляващи и 3 за избиратели). Техническата спецификация за доставката на модел А4-517 (Приложение № 1 към Решение № 268-НС от 21.06.2021 г.) предвижда комплект от 6 смарткарти (4 за избиратели и 2 за членове на СИК). Предлагаме да се уточни актуалният комплект, а проверките да обхващат всички смарткарти за избиратели в него. 4.4. Т. 17: в проверките на хардуерните интерфейси изрично да се включат Ethernet портът и допълнителните USB портове, описани в спецификацията на модела. 5. Приложение № 3 5.1. Т. 2.1: новият текст разграничава мастер ключ и ключ на избирателната секция, но мастер ключът не е включен в предпоставките. Предлагаме да се добави като предпоставка и да се уточни дали е общ за всички машини или уникален за всяка, кой го съхранява и как се предоставя.	4.3 Не се приема. 4.4 Приема се. 5.1 Приема се частично.	решение, с което не се удостоверява съответствието. 4.3 В цитираното решение са определени минимален и максимален брой на смарткартите, посочените в приложение № 3 към Методиката 5 бр. смарткарти – 2 за управление и 3 бр. за гласуване влизат в посочените граници. 4.4 Отражено е в текста на Приложение 2 5.1 Мастерключът е добавен като предпоставка в Приложение № 3. Всички информационни активи за целите на удостоверяването са собственост на ЦИК и се предоставят от нея.
--	--	--	--	--	--	---

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				5.2. Т. 3.1, допълнителен сценарий 1: очакваният резултат при изваждане на смарткартата преди края на гласуването е променен от „ТУМГ прекъсва вота и връща към начален екран“ на „Гласуването продължава успешно“. Предлагаме да се посочи основанийето за промяната (т. 2.4) и очакваният резултат да се допълни с проверими критерии: правото за гласуване, свързано със смарткартата, се изчерпва в момента на активиране на сесията за гласуване, така че картата не може да активира повторно гласуване на същата или на друга ТУМГ; сесията приключва с точно една контролна разписка и един запис в електронната избирателна кутия.	5.2 Приема се.	5.2. Отражено в текста на Приложение № 3.
				5.3. Т. 3.1, предпоставка 2: отпада ПИН кодът на смарткартата за управление, която се използва за отключване след заключване на екрана (допълнителен сценарий 4). Предлагаме да се уточни дали отключването изисква ПИН код. Ако не изисква, това да бъде изрично посочено и обосновано, тъй като в т. 3.2, 5.1 и 7 ПИН кодът е запазен. В противен случай този текст не следва да отпада, тъй като няма проверка на оторизацията за това действие.	5.3 Приема се.	5.3. Отражено в текста на Приложение № 3.
				5.4. Т. 3.1: отпада изречението „При потвърждение, гласът се отчита без възможност да се променя“. Новата стъпка 4 описва отнемане на възможността за друг избор, но не и записа на гласа. Предлагаме да се възстанови описанието на момента на запис в съответствие с чл. 268, ал. 4 ИК (след потвърждаване гласът се визуализира и се записва на записващото техническо устройство, след което се отпечатва	5.4 Не се приема.	5.4 Описано е в колона „Очакван резултат“.

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

			контролната разписка) и този ред да бъде проверяван. Да се уточни и дали потвърждението по стъпка 2 и натискането на бутона „Край на гласуването“ по стъпка 4 са едно и също действие. 5.5. Т. 3.1: съгласно чл. 268, ал. 3 ИК избирателят може да промени избора си еднократно преди потвърждаването му. Допълнителен сценарий 5 проверява само възможността за връщане. Предлагаме да се провери внимателно и при нужда да се добави сценарий, който проверява, че втора промяна не е възможна. 5.6. С оглед зачестилите съмнения относно т.нар. празни бюлетини – проблем, който може и да не се реши самостоятелно с минаването обратно към контролни разписки, е добре да се добавят сценарии за дефектна или празна контролна разписка: отказ на печатащото устройство или засядане на хартията след потвърждаване на гласа; непълна или неотпечатана контролна разписка. Очаквани резултати: гласът е записан еднократно; събитието е отразено в електронния дневник по чл. 213, ал. 2, т. 14 ИК; повторно гласуване не е възможно (т. 7 от Решение № 216-ПВР); разминаването между броя на записаните гласове и броя на четимите контролни разписки се установява и документира в протоколите по т. 7 от Методиката.. Добре е да се добавят и сценарии за преминаване към гласуване с хартиени бюлетини по чл. 269 ИК (т. 5 от Решение № 216-ПВР, изменена с Решение № 287-ПВР), при което данните до този момент се запазват и са отчитаеми, и за невъзможност за отпечатване на протокол, при която резултатът	5.5 Не се приема. 5.6 Не се приема.	5.5 Предложението не съответства на ИК. 5.6 Описаният сценарий е нереалистичен, тъй като няма как да се симулира издаването на празна разписка.
--	--	--	---	---	---

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

			от преброяването на контролните разписки (т. 6 от Решение № 216-ПВР) съвпада с данните от записващото техническо устройство. 5.7. Т. 5.1: изразът „При достигане на зададеното време за край на изборния ден“ допуска тълкуване, че закриването зависи от системното време. Съгласно чл. 220 ИК гласуването продължава след 20.00 ч., но не по-късно от 21.00 ч., за избирателите, намиращи се пред изборното помещение, а краят на гласуването се обявява от председателя на СИК. В настоящата редакция текстът оставя неяснота как точно приключва изборния ден и за кои сценарии следва да се тества. Предлагаме да се уточни ръчното прекратяване и да се покрият по-изчерпателно сценарии за: гласуване след зададения час до ръчното обявяване на края; опит за обявяване на края преди зададения час; неточно системно време; часови зони при гласуване извън страната (т. 8) и др. 5.8. Т. 5.1: отпада очакваният резултат „Успешна авторизация“, а номерацията на стъпките и очакваните резултати вече не си съответства. Предлагаме резултатът да се възстанови и да се добави допълнителен сценарий с невалиден ПИН код и със смарткарта за управление на друга избирателна секция при опит за обявяване на края на изборния ден. 7 5.9. Т. 6 (нова): отново с положителен прием на тази точка, предлагаме тя да се допълни с още условия, например: а) уточнение, че предвидената в стъпка 1 проверка на подписания файл с резултата представлява верификация на	5.7 Не се приема. 5.8 Не се приема 5.9 Приема се частично	5.7 Не е обект на техническо удостоверяване, тъй като това е в правомощията на изборната администрация. 5.8. Промяната е свързана с последните изменения в ИК 5.9. Букви а), г), д), е) и ж) се приемат. По буква б) - проверката на криптирането ще се изключи от описанието на
--	--	--	---	---	---

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

			електронния подпис спрямо удостоверителната верига на ЦИК, извършвана с инструмент, независим от софтуера на ТУМГ; б) стъпка в основния сценарий за проверка на криптирането, което е посочено в описанието на т. 6, но не е включено в сценария, с уточнение с какви средства проверяващите изчитат съдържанието; в) негативни сценарии – модифициран файл, разлика между двете флаш памет, извадена или повредена флаш памет по време на изборния ден, запълнена памет, липсваща втора памет при стартиране, в съответствие със случаите, при които съгласно т. А.2.1 от Изискванията, приети с Решение № 65-ПВР на ЦИК, данните не се изчитат (липсващи носители, неуспешна верификация на подписа, невалиден формат, несъответствие на хеш кода на софтуера); г) съответствие между данните във файла и данните преди и след рестартиране, смяна на хартиената ролка и работа на резервно хранване (т. 7); д) съответствие между броя на записите в електронната избирателна кутия и броя на гласувалите по т. 3.2; е) отразяване в електронния дневник на събитията, генерирани в хода на теста; ж) проверка на допълнителното записващо техническо устройство при възможност за нов избор. 5.10. Във всички сценарии, при които се генерират особености и отклонения от нормалния режим (невалиден ПИН код, рестартиране, смяна на хартия, прекъсване на хранването), да се проверява отразяването им в електронния дневник по чл. 213, ал. 2, т. 14 ИК.	5.10. Приема се	сценария, тъй като права за проверката му има само производителя. Буква в) ще се прилага в обем, съобразен със срока по чл. 213а, ал. 4 ИК. 5.10. Отражено е в текста на Приложение № 3.
--	--	--	---	--	---

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				6. Приложение № 4 6.1. Да се добави проверка, съответстваща на чл. 213б, ал. 4, т. 2 ИК, че ТУМГ стартира единствено софтуер, подписан с ключовете на ЦИК: че в модула за сигурност на стартирането на операционната система са записани само ключовете на ЦИК; че софтуер без подпис или подписан с друг ключ не може да бъде стартиран; и че тази защита е включена и не може да бъде изключена без парола. 6.2. Инструментът Unlocker позволява криптографско отключване на машините. Наред с проверката на неговото функциониране да се предвиди проверка на реда за съхранението и употребата му и изискване всяка употреба след довереното изграждане да бъде протоколирана. 6.3. Параметризиращият софтуер да се проверява не само за уязвимости, но и за съответствие: генериране на електронни бюлетини от тестови кандидатски листи и сравнение с утвърдения от ЦИК образец (ред, пълнота, еднаква по обем и качество информация по чл. 213, ал. 2, т. 3 ИК); коректно съответствие между секции и изборни райони; негативни случаи. Криптографският идентификатор на параметризиращия софтуер да се включва в Доклада. Тъй като реалните параметризационни образи се изготвят след удостоверяването, да се предвиди извадкова проверка на тези образи от удостоверяващите институции преди инсталирането им.	6.1 Не се приема 6.2 Не се приема 6.3 Не се приема	6.1 Дейността по чл. 213б, ал. 4, т. 2 ИК не е свързана с процеса по удостоверяване, тя се извършва от ЦИК. 6.2 Редът за съхранение на информационните активи не е предмет на удостоверяването на съответствието. 6.3 Параметризиращият софтуер не е елемент от електронната система за гласуване по чл. 213 от ИК.
--	--	--	--	---	--	--

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				6.4. При проверката на смарткартите да се установява срокът на валидност на сертификатите към изборния ден. Крайните сертификати по спецификацията от 2021 г. са със срок на валидност 40 месеца, считано от 01.03.2021 г. 7. Редакционни бележки Изброяваме само няколко по-съществени: Приложение № 2: т. 9.1: номерацията на втората стъпка е „10.“ вместо „2.“; Приложение № 3: т. 7.3, стъпка 2: „Отпечатват се множество бюлетини“ да се замени с „Отпечатват се множество контролни разписки“, в съответствие с останалия текст. Приложение № 4: „механизъм за непоследователно записване на подадените.“ – липсва думата „гласове“; 8. Публикуване на протоколите, Доклада и Решението за удостоверяване Методиката е публичен документ и определя в подробности проверките, които се извършват. Протоколите по т. 7.1, изготвени по табличните форми на Приложения № 1–4, не съдържат информация, чието оповестяване би застрашило сигурността на системата, с изключение на	6.4 Не се приема. 7. Приема се. Приема се Приема се Не се приема	6.4. Отговорността за валидността на сертификатите на смарткартите е на ЦИК. 7. Отражено е в текста на Приложение №2 Отражено е в текста на Приложение № 3 Отражено е в текста на Приложение № 4 8. Институциите по удостоверяване нямат право да дават достъп и/или да публикуват чувствителна информация, която е обект на авторски права и/или е собственост на други ЮЛ, както и такава, за която се счита че би подпомогнала злонамерени лица и/или би
--	--	--	--	---	--	--

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				пароли, частни ключове и лични данни. Предлагаме Министерството да обсъди: 8.1. Протоколите от всички проверки да се изготвят в цифров вид като попълнени контролни списъци, съответстващи на табличните форми от приложенията, с отразени констатации и оценка за всяка дейност. 8.2. Протоколите, Докладът за оценяване на съответствието и Решението за удостоверяване/неудостоверяване да се публикуват на интернет страницата на министерството в срок, определен в Методиката, след постановяване на Решението, като се заличават единствено пароли, частни ключове и лични данни и във вид, който е атрактивен, удачен за четене и анализ (т.е. не представлява сканиран документ, а пълноценен уеб-документ).		компрометирала по някакъв начин машинното гласуване.
--	--	--	--	--	--	---

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				8.3. Заедно с тях да се публикуват списъкът на изпитаните образци, криптографските идентификатори по т. 1.1 и информация за участвалите наблюдатели по чл. 213а, ал. 3 ИК съгласно препоръките, направени по-горе относно проследимост. Публикуването ще позволи на наблюдателите, експертите и обществеността да проследят какво точно е проверено, с какъв резултат и спрямо кой софтуер. Това е необходимо условие за доверие в удостоверяването, особено при изборен процес, в който машинното гласуване е основен начин на гласуване. 9. Информационна страница за машинното гласуване Документите, свързани с машинното гласуване, се издават от различни институции, публикуват се на различни места, често в неудобни за четене формати, а някои от тях не са публикувани. Предлагаме министерството да поддържа специална страница или подсайт, на който в лесно четим вид да се публикуват или препубликуват всички ключови документи за съответните избори, включително: а) Методиката и приложенията към нея, в сила за съответните избори, както и документите по т. 8; б) техническите изисквания на ЦИК по чл. 213, ал. 3 ИК, а ако част от тях не подлежи на публикуване – поне номерът и датата на акта и публичната му част;	8.3 Не се приема. 9. Не се приема.	8.3.Списъкът с изпитаните образци е част от доклада. Списъкът на участвалите наблюдатели може да се намери на страницата на ЦИК. 9. Предложенията не са предмет на Методиката. Предложението е организационно. Актовете на ЦИК и „Информационно обслужване“ АД са извън компетентността на министерството по Методиката.
--	--	--	--	--	--	--

МИНИСТЕРСТВО НА ИНОВАЦИИТЕ И ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

				в) техническата спецификация към обществената поръчка за машинното гласуване (Приложение № 1 към Решение № 53-ПВР) и приложимите технически спецификации за доставката на машините; г) Решение № 216-ПВР от 15.09.2026 г. на ЦИК, с измененията по Решение № 287-ПВР, и другите решения на ЦИК, свързани с машинното гласуване; д) методическите указания на ЦИК за изборите в частта за машинното гласуване, след приемането им; е) образците на системната разписка, контролната разписка и протокола, отпечатван от ТУМГ, както и образците на електронните бюлетини; ж) плана по чл. 213б, ал. 3 ИК, Правилата за доверено изграждане за съответните избори, след приемането им, и публикуваните криптографски идентификатори по чл. 213б, ал. 4, т. 3 ИК. Предлагаме също министерството, в качеството си на министерство, упражняващо правата на държавата в „Информационно обслужване“ АД, да съдейства за публикуването в същия формат на документите, свързани с компютърната обработка на резултатите: Изискванията, приети с Решение № 65-ПВР от 28.08.2026 г. на ЦИК и съответните линкове и обобщена информация от портала за изборни резултати, поддържан от ИО.		
--	--	--	--	--	--	--

