

СПРАВКА

за отразяване на предложенията, становищата и възраженията, постъпили при проведената обществена 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

№	Подател	Предложение	Приема/не приема	Мотиви
1.	Ангел Петров	1. Видно от официалните доклади за оценяване на съответствието от предходни избори (напр. Доклад рег. № 1980/11.10.2024 г.), функционалните и хардуерни тестове на ТУМГ от страна на екипите на БИМ и МЕУ се извършват върху машини, предоставени от Изпълнителя по обществената поръчка с „предварително инсталиран демонстрационен софтуер и смарткарти от тестова верига“. Тази практика, установена от Централната избирателна комисия, създава процедурен дефицит, който може лесно да бъде отстранен, за да отговори на най-високите съвременни стандарти за независим одит. В момента удостоверяващите органи тестват система (инсталиран софтуер и параметризация), която е компилирана и подготвена от външен Изпълнител. Удостоверяването на сорс кода и довереното изграждане се извършват	1. Приема се по принцип.	1. Описано в т. 2 на Приложение № 4.

		паралелно, но функционалните тестове се правят върху устройства, подготвени от частната фирма. Въвеждането на изцяло държавен контрол върху тази стъпка ще гарантира 100% предвидимост на процеса. 2. Въз основа на предходния одит е установено, че устройствата работят с операционна система Ubuntu Linux 20.04.6. Към днешна дата тази системна база навлиза в етап от своя жизнен цикъл, който изисква рутинно технологично обновяване: • Стандартният цикъл на поддръжка за Ubuntu 20.04 LTS приключи през април 2025 г. Използването на операционна система в режим на удължена поддръжка (ESM) е стандартна ИТ практика, но генерира риск, който е напълно управляем и следва да бъде изрично анализиран и описан в доклада от удостоверяването. • Предходните доклади потвърждават използването на модифицирано Linux ядро. Ако версията му е в серия 5.3 (която е „End of Life“ от края на 2019 г.), преминаването към актуално LTS ядро (напр. версия 6.x) е силно препоръчително. Това е рутинна мярка за информационна хигиена, която напълно неутрализира стандартните технологични уязвимости за по-стари версии, които иначе са напълно изолирани и управляеми в затворената среда на ТУМГ.	2. Приема се по принцип.	2. Извършва се в рамките на дейностите, предвидени в Приложение № 4.
--	--	--	---------------------------------	---

	• През 2023 г. са констатирани шест библиотеки (напр. libgtk-3-0), върху които Изпълнителят прилага собствени „кръпки“ (patches) за оптимизация. Като стандартна добра практика, препоръчвам извършването на детайлен одит на тези промени, за да се гарантира максимална съвместимост и придържане към системните защиты. 3. Предлагам в Методиката да бъде предвиден нов Раздел „Процедури за тестване“ (или в съответния приложим раздел в новата Методика), в който изрично да бъдат заложени следните нови изисквания: 3.1. Самостоятелно държавно изграждане: „За целите на функционалното тестване и хардуерните изпитвания, Министерството на електронното управление (МЕУ) извършва самостоятелно инсталиране и конфигуриране на операционната система и приложния софтуер върху тестовите ТУМГ от извадката. Инсталационният образ задължително се генерира от МЕУ чрез детерминистично изграждане от вече проверения изходен код, в контролирана лабораторна среда на министерството.“ 3.2. Забрана за външна намеса: „Не се допуска извършване на функционални и сертификационни тестове върху ТУМГ, чиято операционна система или параметризация са инсталирани или	3.1 Приема се по принцип. 3.2 Приема се по принцип.	3.1 Извършва се в рамките на дейностите, предвидени в Приложение № 4. Методиката съдържа общи текстове, свързани с описание на схемата за удостоверяване, касаещи основните принципи на проверките, тестването и оценяването, а конкретни текстове се съдържат в съответните приложения. 3.2 От описаното в т. 2 от Приложение № 4 е видно, че няма да има намеса на външен изпълнител.
--	---	---	---

	подготвени от Изпълнителя по логистиката на машинното гласуване.“ 3.3 Независима параметризация: „Параметризацията на тестовите машини се извършва изцяло от експерти на МЕУ, чрез специализирания софтуер за параметризиране (EMS), собственост на ЦИК.“ 4. Независими тестови активи: „Необходимите за тестването смарткарти (съдържащи тестови криптографски сертификати) се генерират и предоставят на МЕУ и БИМ директно от държавния системен интегратор „Информационно обслужване“ АД.“ 5. Публичност и управление на уязвимостите (CVE Transparency): Предлагам МЕУ да публикува пълен списък на идентифицираните уязвимости в системата и мерките за тяхното ограничаване. По този начин гражданското общество ще има увереност, че „ниското ниво на заплахата“ (CVSS 3.0), декларирано в предходни доклади, остава напълно валидно и технически обезпечено и през 2026 г.	3.3 Приема се по принцип. 4. Не се приема. 5. Не се приема.	3.3 Извършва се в рамките на дейностите, предвидени в Приложение № 4. 4. Всички информационни активи се предоставят на органите по удостоверяване на съответствието от ЦИК. 5. При вземане на решение за удостоверяване откритите уязвимости са преценени като такива с нисък риск в зависимост от средата, в която функционира ТУМГ и в зависимост от неговото предназначение и не оказват въздействие върху вземането на решение. В случаите на висок риск, трите институции не биха постановили решение за удостоверяване на съответствието.
	6. В основния текст на Методиката, раздел 4 (Проверка и оценка за съответствие с изискванията към сигурността на информацията...), изрично е посочено, че	6. Приема се.	6. Отражено е в т. 3 от Приложение № 4.

		проверката на софтуерната реализация включва: - „Проверка за уязвимости в параметризиращия софтуер;“ - „Оценка на нивото на въздействие на евентуално открити уязвимости в параметризиращия софтуер;“ Въпреки това категорично изискване, заложено в основния документ, в табличната част на Приложение № 4 (по която реално работят екипите за оценяване), тези конкретни проверки липсват. Вместо тях е записана единствено „Проверка на приложния код при взаимодействие с параметризиращите компоненти...“. Това противоречие води до абсурдната ситуация, в която основният текст на Методиката изисква одит за уязвимости на самия софтуер за параметризация, но в приложението, служещо за чек-лист на експертите, такова задължение не е предвидено. Тъй като параметризацията е най-критичният етап от подготовката на изборния процес (генерирането на данните за секциите и записът им върху флаш паметите), изключването на този софтуер от реалните стъпки за проверка създава недопустим риск за сигурността. С оглед на гореизложеното, се прави следното конкретно предложение: За да се отстрани вътрешното противоречие в документа и да се изпълнят изискванията		
--	--	---	--	--

		на собствения му раздел 6.4, се предлага в Приложение № 4, в раздел 3 , да се добави нов ред със следното съдържание: • Действие: Проверка на параметризиращия софтуер, използван за подготовка на ТУМГ. • Очакван резултат/ Критерий за оценяване: Установяване на липса или на наличие на уязвимости в параметризиращия софтуер. Оценка на нивото на въздействие при открити уязвимости в параметризиращия софтуер съгласно CVSS 3.1.		
2.	Ангел Славчев, народен представител от ПГ „Възраждане“	1. Да се въведе изричен принцип, че при съмнение удостоверяване не се издава. Методиката следва да предвиди, че при всяко останало неразсеяно съмнение относно идентичност, цялост на софтуера, работещи защити, проследимост на версиите или достоверност на доказателствата удостоверение не се издава, докато съмнението не бъде изцяло отстранено с нова проверка. При изборите липсата на доказан дефект не е достатъчна необходима е доказана надеждност и сигурност. 2. Да се въведе задължение всички критични стъпки от процедурата по удостоверяване да се отразяват в единен официален регистър / досие на удостоверяването. Този регистър трябва да съдържа задължително следните вписвания:	1. Приема се. 2. Приема се частично.	1. Отразено в т. 7 от Методиката. 2. За всяко удостоверяване се води документация, в която посочените стъпки се протоколират подробно. Чл. 4а от ЗЕУ изисква законово основание за водене на регистър, каквото липсва в настоящия случай.

	• предаване и приемане на устройствата • идентификация на серийни номера • версии на инсталирания софтуер • използвани носители / среди • точни дати и часове на извършените тестове • участници във всеки етап • установени проблеми • предприети коригиращи действия • резултати от повторни проверки • окончателно заключение Регистърът следва да бъде подписван от представителите на участващите институции и да бъде защитен срещу нерегламентирани промени (т.е. всяка промяна да оставя ясна следа / одитна следа). 3. Да се въведе изискване за пълна персонална отговорност на участниците в критичните етапи. При всички действия, свързани с приемане на активи, инсталация, конфигуриране, генериране на контролни стойности, подписване на протоколи и заключения, следва да се отбелязва конкретното длъжностно лице, което е извършило действието, както и основанието, на което го извършва. Процедура без ясна персонална отговорност лесно се превръща в колективна безотговорност. 4. Да се въведе задължителен принцип на четири очи при всички критични действия.	3. Приема се по принцип. 4. Приема се по принцип.	3. Носи се отговорност съгласно българското законодателство. 4. Удостоверяването на съответствието се извършва от специално назначени за
--	--	---	--

	Да се въведе стриктно правило „четири очи“ – никой критичен етап да не може да се минава от един човек сам. Когато се прави хеш, подписва протокол, предава флашка с инсталация, одобрява версия на софтуера, запечатва или разпечатва устройство, приема/предава машини или прави повторна проверка, винаги трябва да присъстват и да подписват поне две лица от различни институции. Не бива да е възможно една институция или един човек да решава сам на тези важни места. 5. Да се добави отделен раздел за физическата сигурност на устройствата и носителите. Освен софтуерната и функционалната проверка, методиката следва да включва изрични правила за физическа проследимост на устройствата, носителите и средствата за персонализация: условия за съхранение, контрол върху достъпа, пломбиране, правила за транспортиране, регистриране на всяко отваряне или намеса, както и задължителна проверка за следи от физическа манипулация. Реалният риск за изборния процес не е само в кода, а и в достъпа до самото устройство и до носителите около него. Това е в съзвучие и с вече предложената идея контролът да обхваща не само самото ТУМГ, а и свързаните процеси около него.	5. Не се приема.	целта екипи. Наред с посоченото, в процеса по удостоверяване могат да участват и лицата съгласно чл. 213а, ал. 3 от Изборния кодекс. 5. Въпросът е извън обхвата на методиката.
--	--	------------------	---

	6. Да се предвиди задължителна случайна извадка за задълбочена допълнителна проверка. Наред с основната проверка следва да се въведе и задължителен механизъм за разширена проверка на случайно избрана извадка от устройствата, определена по прозрачен ред. Това е необходимо, за да не остане удостоверяването ограничено до формален преглед на представен набор, без реална гаранция, че същите характеристики са налице и в останалите устройства от доставения тип. 7. Да се забрани допускането на удостоверяване при непълен комплект активи и документация. Следва изрично да се запише, че ако не бъдат представени всички изискуеми активи, инсталационни носители, изходен код, описания на конфигурации, техническа документация, протоколи, зависимости, версии и други необходими материали, срокът за удостоверяване не тече и процедурата не може да завърши с положителен резултат. Не бива държавата да удостоверява система, за която няма пълна информация. 8. Въвежда се задължително правило всяка проверка да е 100% възпроизводима.	6. Не се приема. 7. Не се приема. 8. Приема се по принцип.	6. Удостоверява се типа ТУМГ. Основната проверка е задълбочена; устройствата са избрани на случаен принцип. Задължително се представя и декларация за съответствие и идентичност. 7. Условията за стартиране на процеса по удостоверяване са описани в т. 4 от Методиката. 8. Всички процеси по проверка могат да бъдат повторени и се документират подробно.
--	---	---	--

	Описание на тестове, хешове, контролни суми, функционални сценарии и конфигурационни проверки трябва да позволява независимо повторение със същия резултат. Ако дадено действие не може да бъде точно повторено по документи и процедура, то не се зачита като валидно основание за удостоверяване. 9. Да се добави задължителна проверка за съответствие между одобрената документация и реалното състояние на устройството. Необходимо е методиката да изисква не само представяне на документация, а и доказване, че тя съответства на реално доставеното устройство, на реално инсталирания софтуер и на фактическата конфигурация. При разминаване между документ и реално установено състояние трябва да се приема наличие на съществено несъответствие. 10. Да се въведе отделно изискване за проверка на изключените функционалности. Освен какво устройството прави, трябва да се проверява и какво не може да прави. Следва да се валидира, че са изключени всички несъвместими с изборния процес функционалности, включително ненужни услуги, комуникационни интерфейси, възможности за външно зареждане, нерегламентиран достъп до системно ниво и	9. Приема се по принцип. 10. Приема се по принцип.	9. Целта на методиката е именно предложението в т. 9. 10. Проверката се извършва при работата на екипите по удостоверяване на съответствието.
--	---	--	---

	други механизми, които не са необходими за гласуването, но биха могли да увеличат риска. 11. Да се добави задължение всички установени несъответствия да се публикуват в обобщен вид. След приключване на процедурата следва да се публикува обобщена информация за установените несъответствия, тяхната категория, предприетите коригиращи действия и резултата от повторната проверка. Без да се разкриват чувствителни технически детайли, обществото трябва да знае дали в хода на удостоверяването са констатирани проблеми и как са били преодолені. Това доразвива вече заложената логика, че прозрачността не следва да е само формална. 12. Да се въведе задължителна повторна пълна проверка при всяка промяна в критичен елемент. Следва да се запише, че всяка промяна в софтуер, библиотека, конфигурация, сертификат, ключ, носител, механизъм за стартиране или защитна настройка води до нова пълна проверка, а не само до частично преразглеждане. Вече подготвените предложения правилно поставят въпроса за повторната проверка, но според мен тук е необходимо още по-категорично правило.	11. Приема се по принцип. 12. Приема се.	11. Резултатите в обобщен вид се описват в доклада, който е публичен. 12. Предвидено е в т.7.1 от Методиката.
--	---	--	---

	13. Да се предвиди отделен раздел за извънредна проверка по сигнал. Необходимо е методиката да предвиди, че при постъпили данни, сигнал или основателно съмнение от компетентен орган, парламентарно представена партия или участник в изборите, може да се разпорежи извънредна допълнителна проверка на вече удостоверен тип устройство, включително по конкретен аспект на сигурността, конфигурацията или проследимостта. 14. Да се въведе кратък публичен отчет след всяка процедура по удостоверяване. След приключване на удостоверяването да се публикува кратък официален отчет, съдържащ най-малко: предмет на проверката, обхват, дата, участвали институции, общ резултат, наличие на несъответствия, извършени повторни проверки и основание за крайното решение. При толкова чувствителен обществен процес липсата на отчет засилва недоверието. 15. Да се въведе забрана удостоверяването да се основава единствено на представени от доставчика твърдения. Методиката следва изрично да подчертае, че всяко твърдение на доставчика или производителя трябва да бъде подложено на самостоятелна проверка, когато се отнася до сигурността, конфигурацията,	13. Не се приема. 14. Приема се по принцип. 15. Не се приема.	13. Няма правно основание за исканата извънредна проверка. 14. Резултатите в обобщен вид се описват в доклада, който е публичен. 15. В Методиката изрично са посочени информационните активи и документи, въз основа на които се извършва удостоверяването; не се разчита на твърдения на доставчика или друг субект, в който и да е етап от удостоверяването. Наред с посоченото, на самостоятелна
--	--	--	--

		идентичността на софтуера, целостта на носителите и коректното функциониране на критични механизми. Държавата следва да установява фактите сама, а не да удостоверява въз основа на доверие. 16. Да се въведе задължителна архивируемост на доказателствата от удостоверяването. Всички протоколи, хешове, снимков материал, логове, резултати от проверки, технически справки и документи от процедурата следва да се съхраняват за определен минимален срок по ред, който позволява последваща проверка, парламентарен контрол, съдебен контрол и експертен анализ при необходимост.	16. Не се приема.	проверка се подлагат всички компоненти на ТУМГ. 16. Не е предмет на Методиката. Всяка организация, ангажирана с удостоверяването изготвя свои вътрешни правила за архивиране на доказателствата от него.
3.	Благовест Кирилов	1. Приложение №1 – „документите ... следва да бъдат безусловно признати“, а при наличие на валидни и автентични сертификати/докладите могат да се ползват като доказателство за съответствие в съответния обхват. Да се замени с текст: „Документите, издадени от трета независима страна, могат да се използват като допълнително доказателство, което подпомага оценяването, но не освобождава екипите от задължението им да извършат собствена проверка и преценка на съответствието на конкретно доставения тип ТУМГ.“	1. Не се приема.	Проверките по т. 6.1 и Приложение 1 от Методиката се извършват с оглед установяване на автентичността и валидността на документите за оценяване на съответствието, издадени от трета независима страна, както и доколко те са признати на територията на РБ или в законодателството на ЕС, като и по линия на двустранни и многостранни споразумения за взаимно признаване. Директният отказ от признаването на такъв документ, което на практика се предлага, е грубо нарушение на разпоредбите на РЕГЛАМЕНТ (ЕО) №

	Мотиви: Формулировката е прекалено силна и на практика допуска външен сертификат/доклад да замести собствената проверка на МЕУ, БИМ и БИС.. Изборният кодекс възлага удостоверяването именно на МЕУ, БИМ и БИС, а не на външни органи. Външните документи могат да подпомагат, но не и да подменят държавната оценка. Освен това европейските стандарти за е-гласуване изискват схемата за удостоверяване да е публична и всеобхватна, а оценяването да се извършва от независим и компетентен орган. 2. Методиката допуска ползване на документи от трета страна като част от схемата за оценяване, а приложенията не поставят достатъчно твърда граница кога това е допустимо и кога не. Да се добави изрично правило, че не могат да бъдат замествани чрез външни сертификати минимум следните проверки: идентичност на доставения тип, хешове и build артефакти, конфигурация на ОС, активни интерфейси, зависимости, управление на ключове/сертификати, функционални сценарии в българската изборна среда. Мотиви: Има риск важни зони от проверката да бъдат „извадени“ от реално изпитване и оставени само на документална основа. Външен документ може да описва	2. Приема се по принцип.	765/2008 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА и на производните на него документи и на многостранните споразумения за взаимно признаване на ЕА, ILAC, IAF и др. Използваните в Методиката и Приложение 1 текстове допускат нови, в т.ч. и цялостни проверки в съответната област, без те да предпоставят категоричен отказ от признаване на сертификатите/докладите, издадени от трета независима страна. 2. Всички документи, предоставени от ЦИК, издадени от трета независима страна, които са били оценени като автентични, валидни, отговарящи на изискванията на националното и европейското законодателство и относими към проверка на съответствието с изискванията към продукта (ТУМГ) се предоставят на техническите екипи за използване по целесъобразност и професионална компетентност. Методиката съдържа по-общ текстове, свързани с описание на схемата за удостоверяване, касаещи принципите на проверки, тестване и оценяване, а конкретните текстове се съдържат в съответните Приложения.
--	--	---------------------------------	--

	друг екземпляр, друга версия или друг контекст на тестване. При изборни технологии трябва да се проверява именно конкретният доставен тип, а не абстрактно сходен продукт. Това следва и от логиката на самата методика, която изисква образци, build информация, пароли и пълен достъп до активите. 3. Методиката и приложенията изброяват множество проверки, но не съдържат достатъчно ясна матрица на последиците при констатирани несъответствия. В Приложение № 4 има проверки за уязвимости, CVSS, зависимости, хешове, сертификати и др. Да се въведе матрица на несъответствията с минимум 3 категории: критично, съществено, несъществено. Да се добави правило, че при критично несъответствие удостоверяване не се издава. Мотиви: Има тестове, но липсва достатъчно твърдо правило кога удостоверяването се отказва, кога се допуска корекция и кога се иска повторна проверка. Това ще премахне прекомерната оперативна преценка и ще направи режима предвидим, прозрачен и защитим. Особено важно е за уязвимости, засягащи тайната на вота, целостта на данните, удостоверяването на софтуера, веригата на доверие и проследимостта на build-a.	3. Приема се.	3. Отразено е в т. 6.4. от Методиката
--	--	---------------	---------------------------------------

	4. Приложение № 4 предвижда проверка за уязвимости в ОС и приложния софтуер, както и оценка по CVSS 3.1. Да се добави текст: „Уязвимости с оценка съществено/критично, както и всяка уязвимост, която може да засегне тайната на вота, целостта на резултата, удостоверяването на софтуера, криптографските механизми или веригата на доверие, водят до отказ за удостоверяване до пълното им отстраняване и повторна проверка. Мотиви: Самото наличие на CVSS-оценяване е добро, но липсват нормативни прагове и задължителни последици. В противен случай CVSS остава информативен инструмент. Не е достатъчно да се знае за проблема - трябва да е ясно какво следва от него. 5. Методиката допуска допълване на приложимите документи за изпитване, проверка и оценяване в Плана за оценяване след преглед на предоставените активи и документация. Да се предвиди, че основният минимален набор от проверки и критерии е фиксиран и публичен, а допълване е допустимо само ако: 1) не намалява обхвата; 2) е мотивирано писмено; 3) се публикува незабавно като приложение към плана. Мотиви: Това ще повиши предвидимостта и общественото доверие. Европейската добра	4. Приема се. 5. Приема се.	4. Отражено в т. 6.4 от Методиката и Приложение № 4. 5. Направено е допълнение в т. 2 от Методиката: „Допълване е допустимо само, ако не намалява обхвата и е мотивирано писмено.“
--	--	---	--

	практика за е-гласуване е схемата за удостоверяване да бъде публично достъпна и всеобхватна. 6. В обхвата на методиката не се включват организационно-технически дейности, логистика, техническо обслужване и дейности, свързани с компютърната обработка на резултатите от „Информационно обслужване“ АД. Да се допълни, че към методиката се прилага задължителен свързан модул/процедура за: chain-of-custody, инсталационни носители, персонализация, параметризация, логистика, сервизна намеса, интерфейси към последващата обработка и контрол върху версиите/конфигурациите. Мотиви: Формално обхватът е ограничен до ТУМГ, но реалният риск за изборния процес е по-широк. Много потенциални грешки могат да се случат „в машината“, а около нея — при build, пренос, инсталация, конфигуриране, подмяна на носители и обработка. Съветът на Европа и насоките за ICT в изборите гледат на изборния процес като на по-широка цифрова екосистема, а не само на едно устройство. 7. Методиката предвижда достъп на лицата по чл. 213а, ал. 3 до информационните активи и	6. Не се приема. 7. Не се приема.	6. Предложените дейности са извън обхвата на чл. 213а, ал. 2 от Изборния кодекс. 7. Достъпът не е част от процеса по удостоверяване, а се урежда с решение на
--	---	---	---

	процедурите по време на проверките и изпитванията. Да се конкретизира минимален пакет достъп, което може да се случи и чрез отделна заповед на министъра на електронното управление, до: source snapshot, build logs, dependency list/SBOM, списък на констатираните несъответствия, доказателства за отстраняване, финални хешове, протоколи от повторните тестове. Мотиви: Текстът е правилен като идея, но е прекалено общ и може да остане само формален достъп. Наблюдението трябва да е реално, а не церемониално. Без минимално гарантиран обем информация прозрачността е слаба и лесно се свежда до присъствие без проверимост. Европейската практика акцентира върху прозрачност и проверимост. 8. Приложение № 4 изисква тестово изграждане на базов образ, проверка на контролни суми, генериране на хеш, проверка на зависимости и изпълнимост на бинарния файл в друга среда. Да се добавят изрични изисквания за reproducible build, SBOM, подписан manifest на зависимостите, описана build среда, provenance/attestation на артефактите и публикуване на финалните криптографски идентификатори. Мотиви: Това е добра основа, но не е доведено до пълна проследимост на	8. Приема се по принцип.	ЦИК. Има и вътрешни правила на министъра на електронното управление. 8. Има го описано по общо в Приложение № 4, а се документира подробно в доклада и протоколите. Ще бъде документирано в предложения вариант.
--	---	---------------------------------	--

	софтуерната верига. Международната добра практика при чувствителен софтуер е да има проследимост от изходния код до инсталирания образ. NIST SSDF препоръчва управление на компонентите и защитен жизнен цикъл, а NIST и ENISA поставят силен акцент върху software supply chain, SBOM и доказуем произход на артефактите. 9. Приложение № 4 проверява наличие на външни зависимости и библиотеки, но не формализира тяхното управление като постоянен контрол. Да се добави изискване, че всяка външна зависимост трябва да е описана в SBOM, отбелязана по версия, проверена за известни уязвимости, лицензно допустима и включена в контролирана build среда. Мотиви: Проверка „има/няма“ не е достатъчна за критична система. Третите страни и зависимостите са един от основните рискове за компрометиране на веригата за доставки. Добрата международна практика вече третира прозрачността на компонентите като базово, а не екзотично изискване. 10. Методиката работи в рамките на 20 работни дни от предоставяне на ТУМГ с всички активи. Да се добавят твърди freeze моменти: code freeze, dependency freeze, config freeze, key/certificate freeze и media	9. Приема се по принцип. 10. Не се приема.	9. Има го описано по общо в Приложение № 4, а се документира подробно в доклада и протоколите. Ще бъде документирано в предложения вариант. 10. Не се разработва софтуер, не се променя код и не се издават различни freeze етапи на софтуерна разработка, а се извършва експертен и SAST анализ на кода.
--	---	--	---

	freeze; след всеки freeze да има протокол, хеш и подписване. Мотиви: Така се ограничава рискът от късни промени, а процесът става по-управляем и проверим. При кратки срокове дисциплината в контролните точки е критична. 11. Приложение № 3 описва функционални сценарии: окомплектоване, документация, персонализиране за секция, валидиране на смарткарти, старт на изборния ден, визуализация и отпечатване. Да се добави отделен раздел „негативни и злоупотребни сценарии“: невалидни карти, опит за прехвърляне на данни от чужда секция, подмяна на ЗТУ, downgrade, невалиден сертификат, модифициран носител, компрометирана конфигурация, опит за boot от външен носител, несъответствие между build и инсталиран образ. Мотиви: Сценариите са полезни, но са ориентирани основно към „успешно протичане“, а не достатъчно към злоупотреби и атаки. За изборна технология е важно не само дали системата работи правилно „когато всичко е наред“, а дали отказва безопасно при опит за злоупотреба или подмяна. Това е ядрото на security testing-a. 12. Методиката не съдържа достатъчно силно правило за повторна проверка след	11. Приема се по принцип. 12. Приема се.	11. Извършва се в рамките на дейностите, осъществявани съгласно Приложение № 3. 12. Отражено е в т. 7.1 от Методиката.
--	---	--	--

	промяна. Налична е логика за промени и документиране, но не и достатъчно категорично задължение за ge-certification по обхват. Да се въведе правило: „Всяка промяна в изходния код, библиотека, конфигурация, драйвър, ключ, сертификат, boot policy, параметризация, инсталационен носител или процес на изграждане задейства повторна проверка поне в засегнатия обхват, а при промяна с влияние върху сигурността – пълна повторна проверка.“ Мотиви: Това е необходимо за защита на веригата на доверие. Иначе удостоверяването рискува да важи за една версия, а реално да се използва друга. 13. Методиката е насочена към предварително удостоверяване, но не урежда достатъчно пост фактум проверяемост след изборния ден. Да се препоръча нов раздел или свързана процедура за постизборен одит: статистическа/рискова извадка, съпоставка между разписки, електронни записи, протоколи и логове. Мотиви: Това е силен механизъм за доверие и обратна връзка към методиката. Международната практика все повече търси не само предварителна, но и последваща проверяемост на ИКТ в изборите. 14. Методиката и приложенията са технически подробни, но не изискват в		13. Не се приема. 13. Предложените дейности са извън обхвата на чл. 213а от Изборния кодекс. Правомощието е на ЦИК. 14. Приема се по принцип. 14. Всяка информация, която може да бъде публикувана без да се засегне
--	---	--	--

	достатъчна степен публикуване на минимален комплект данни за обществен контрол. Да се добави изискване за публикуване на: версия на методиката, план за оценяване, обхват, открити несъответствия по категории, коригиращи действия, финални хешове, версии на ОС/софтуера, дата на freeze и дата на удостоверяване. Мотиви: Това не разкрива опасно чувствителна информация, но значително повишава доверието, прозрачността и възможността за обществен и експертен контрол. Европейските стандарти. 15. В действащото приложение вече има тестово изграждане на базов образ на ОС и приложния софтуер от предоставения изходен код и подготовка на инсталационни артефакти, но текстът не е достатъчно категоричен, че това трябва да се прави самостоятелно от държавния проверяващ орган. Да се въведе текст: За целите на функционалното тестване, изпитванията и удостоверяването Министерството на електронното управление извършва самостоятелно инсталиране, изграждане и конфигуриране на операционната система и приложния софтуер върху тестовите ТУМГ от извадката. Инсталационният образ се генерира от МЕУ в контролирана	15. Приема се.	сигурността на процеса, е публикувана на сайта на МЕУ. 15. Отражено е в приложение № 4 към методиката.
--	--	-----------------------	--

	лабораторна среда чрез детерминистично изграждане от вече проверки изходен код и валидираните зависимости, предоставени по реда на методиката. Мотиви: Този текст премахва риска изпълнителят да влияе върху средата на изпитване. Сегашната рамка допуска широк достъп на изпълнителя чрез предоставяне на документация, технически данни и активи, а методиката разчита и на данни, предоставени от него при проверките на ОС и хардуера. Това създава риск проверката да стъпи върху вече подготвена от външен субект среда. 16. Параметризацията на тестовите машини за целите на удостоверяването се извършва изцяло от експерти на МЕУ в контролирана среда, чрез одобрения от ЦИК софтуер за параметризиране (EMS) или чрез друг изрично одобрен от ЦИК еквивалентен инструмент. Всеки акт на параметризация се протоколира, подписва и свързва с конкретен хеш на използвания софтуер и конфигурация. Мотиви: В Приложение № 4 вече има отделна проверка на приложния код при взаимодействие с параметризиращите компоненти, използвани за подготовка на ТУМГ. Логичната следваща стъпка е не само да се проверява взаимодействието, а и самата	16. Приема се.	16. Отражено е в Приложение № 4.
--	--	----------------	----------------------------------

	параметризация на тестовите машини да бъде независима и проследима. 17. Тестови активи - смарткартите, сертификатите, тестовите ключове и другите криптографски активи, използвани за удостоверяване, се генерират, предоставят и управляват по начин, който изключва едноличен контрол на външен изпълнител. Когато държавен системен интегратор участва в процеса, активите се предават на МЕУ и БИМ по формализирана процедура с протокол, идентификатори, хешове и проследимост на произхода. Мотиви: Методиката вече поставя акцент върху сертификатите, СА веригата и смарткартите, а хардуерното приложение изисква конкретни характеристики на смарткартите и тяхната съвместимост. Но липсва достатъчно ясен режим за произход, предаване и независим контрол върху тестовите криптографски активи. 18. Проверка на версиите на операционната Система - за всяко тестово ТУМГ задължително се установяват и описват: точната версия на операционната система, версията на ядрото, използваните системни компоненти, нивото на приложените кръпки за сигурност, датата на последното обновяване и статутът на поддръжка от	17. Не се приема. 18. Приема се по принцип.	17. Въпросът не попада в обхвата на методиката, а е в правомощията на ЦИК. 18. Дейностите са посочени в Приложение № 4 и резултатите се описват в окончателния доклад, каквато е досегашната практика.
--	---	---	--

	производителя. Резултатите се отразяват в отделен протокол за версия и поддръжка. Мотиви: Сегашното приложение вече изисква да се установи дали софтуерните компоненти на ОС са актуализирани спрямо последните публикувани версии и дали има крёпки за уязвимости. Полезно е това да се превърне в изрично задължение за описване, а не само за проверка. Иначе остава неясно какво точно е проверено и в коя версия. 19. Описване на рисковете от използваната ОС - при установяване на остаряла, ограничено поддържана или рискова версия на операционната система, в констативната част задължително се описват конкретните рискове за сигурността, техният потенциален ефект върху тайната на вота, целостта на данните, надеждността и автентичността на процеса, както и приложимото ниво на въздействие. Мотиви: Методиката предвижда проверка за наличие на уязвимости в ОС и оценка по CVSS 3.1, но не казва достатъчно ясно, че тези рискове трябва да бъдат описани разбираемо и свързани с последици за изборния процес. 20. Задължителни действия при риск от ОС - когато бъдат установени уязвимости, липса на поддръжка, липсващи крёпки или други рискове, свързани с използваната	19. Приема се. 20. Приема се.	19. Отражено е в т. 6.4. от Методиката. 20. Направени са допълнения в т. 6.4. и т. 7.1 от Методиката и Приложение № 4.
--	--	---	--

	операционна система, се описват задължителните компенсаторни мерки, срокът за изпълнението им, органът, който ги изпълнява, и редът за повторна проверка. При висок или критичен риск не се допуска удостоверяване до доказано отстраняване на проблема и повторно валидиране. Мотиви: Сегашният текст стига до оценка на въздействието, но не отива достатъчно далеч до задължително действие. 21. Проследимост на build и инсталация Всяка инсталация на тестово ТУМГ се извършва от артефакти, за които са налични криптографски идентификатори, журнал на изграждането и протокол за съвпадение между проверения изходен код, генерирания образ и инсталираната система. При несъответствие между който и да е от тези елементи тестовете се прекратяват до отстраняване на несъответствието. Мотиви: Това е естествено продължение на вече заложените в приложението HashExtractor, LogExtractor, тестово изграждане и генериране на уникален системен хеш. Добре е да се превърнат от техническа възможност в изрично условие за валидност на теста. 22. Проверка на външните зависимости на ОС и софтуера - към всеки тестов build се прилага пълен списък на използваните	21. Приема се. 22. Приема се по принцип.	21. Отражено е в т. 3 на Приложение № 4 като е добавена проверка на Log-Extractor. 22. Съществува в т. 2 на Приложение № 4.
--	--	--	---

		зависимости, системни пакети, драйвери, библиотеки и криптографски модули, включително версия, произход и статус на поддръжка. За всеки компонент се проверява наличие на известни уязвимости и необходимост от компенсаторни мерки. Мотиви: Сегашното приложение изисква тестване за наличието на зависимости в програмния код и проверка за ненужни драйвери и модули в ядрото. Полезно е това да стане по-формално и по-пълно. 23. Протокол за държавната подготовка на тестовата среда - за всяка тестова машина се съставя отделен протокол, съдържащ: дата и час на изграждане, участващи експерти, използвана лабораторна среда, версия на ОС, версия на приложния софтуер, използвани параметризиращи компоненти, използвани смарткарти и сертификати, хешове на артефактите и резултат от проверката за съвпадение. Мотиви: В момента методиката е богата на проверки, но не е достатъчно строга в документалната проследимост на цялата подготовка.	23. Не се приема.	23. В процеса по удостоверяване се изготвя достатъчно пълна и подробна информация.
4.	Обществен съвет към централната избирателна комисия	1. Да се предвиди интензивно тестване на машините с отпечатване на бюлетини, използвайки ролки хартия, произведени от Печатницата на БНБ, идентични по всички параметри на тези, които ще се ползват в изборния ден, с изключение, разбира се, на	1. Приема се по принцип.	1. Изпълнява се в рамките на дейностите, описани в Приложение № 3.

		специалните защиты по ал. 1 на чл. 213в от Изборния кодекс. 2. Тестовите да се направят както с билд, съответстващ на актуалния софтуерен пакет, така и с билд, съответстващ на версията на софтуера, използван преди промените в ИК от декември 2022 г. (например от юли 2021 г.).	2. Не се приема.	2. Обхватът на удостоверяването е изрично посочен в чл. 213а, ал. 2 от Изборния кодекс.
5.	Централна избирателна комисия	1. В Приложение № 3 „Процедура за проверка и оценка на функционалността на техническото устройство за машинно гласуване (ТУМГ) за съответствие с техническите и функционалните изисквания към него“, в т. 3.1. „Проверка на основните функции на ТУМГ при гласуване да бъде добавен тест за техническа издръжливост на принтиращите устройства. Тестът да се проведе в екстремни условия - максимално натоварване на принтера чрез непрекъснато гласуване, докато свърши ролката със специализирана хартия, при достатъчно висока температура на околната среда. 2. В Приложение № 4 „Процедура за проверка на сигурността на информацията, която се въвежда, обработка, съхранява и извежда от ТУМГ да бъде добавена процедура за изготвяне на образ на тестови параметризиращи компоненти чрез предоставен от ЦИК параметризиращ	1. Приема се по принцип. 2. Приема се.	1. Тестовите вече се извършват в рамките на дейностите, предвидени в приложения № 2 и 3. 2. Добавено е в т. 3 от Приложение № 4.

		софтуер (тестово въвеждане и настройка на данните, необходими за параметризация на ТУМГ). 3. Приложение № 2 „Процедура за проверка на изискванията на хардуерната конфигурация на устройствата“ в т. 15 е посочен текст, който не съответства на нормативната уредба в Изборния кодекс. Към настоящия момент Изборният кодекс предвижда вместо „контролни разписки“ бюлетини от машинно гласуване, които се пускат в специална кутия за машинно гласуване.	3. Приема се.	3. Извършена е корекция в Приложение № 2.
6.	Даниел Стефанов	След преглеждането на приложения № 2 и 3 от Проект на актуализираната Методика за удостоверяване на съответствието на доставения тип техническо устройство за машинно гласуване (ТУМГ) с изискванията на чл. 213, ал. 3 от Изборния кодекс и изискванията на техническата спецификация е видимо, че има няколко сценария, които тестват принтера: като част от функционалностите на периферните устройства, ролката е под 5%, процес на гласуване и др. Не видно обаче, да има сценарий, при който се тества частично възникващия проблем с липса на разписка, частично отпечатване или пълна липса на печат на разписката. Препоръката е да се заложи сценарий, при който: извършват се последователни тестови	Приема се по принцип.	Тестовите вече се извършват в рамките на дейностите, предвидени в приложения № 2 и 3.

		гласувания с валидна смарткарта, при които след всеки подаден и потвърден вот се наблюдава процеса на отпечатване и се проверява, дали разписката е пълна, четлива и напълно съответства на избора на екрана; Ключовият елемент е повторението в серия (напр. 20–50 гласувания с различни типове избор), чрез което се цели да се установят отделни или натрупващи се дефекти в печата (частичен печат, избледняване, разместване, засичане), които не биха се проявили при единичен тест, като очакването е при всяко повторение да се отпечата точно една коректна бюлетина без отклонения в качеството. Вкарването на подобен сценарий и резултатите от него би трябвало да потвърди или отхвърли натрупаните подозрения, че проблемът с разпечатването се дължи на хартия, която се различава от спецификациите.		
7.	Петър Пенчев	Да бъдат предоставени за тестване различни мостри на ролки с хартия за тестване	Не се приема.	Тестовите се извършват с вида хартия, предоставена от ЦИК.
8.	Коалиция „Продължаваме промяната - Демократична България“	1. По т. 7.5 – Предлага се въвеждане на изрична класификация на констатациите по тежест (критични, съществени, несъществени, административни), както и ясно разграничение на тяхното влияние върху изборния процес. С оглед ограничаване на възможностите за различна интерпретация и повишаване на прозрачността на процеса, предлагаме при	1. Приема се по принцип.	1. Отражено е в т. 6.4 и 7.1 от Методиката.

	констатиране на т.нар. „незначителни несъответствия“ задължително да се въвежда стандартизиран механизъм за тяхното документиране който да включва най-малко следната информация: • дата и етап от процеса, на който е установено несъответствието; • кратко описание на констатацията и нейната класификация по тежест; • изрична оценка за липса или наличие на влияние върху изборния процес; • експертна препоръка за необходими коригиращи действия (ако такива са необходими); В случаите, когато несъответствието е класифицирано като несъществено и не влияе върху изборния процес, предлагаме това да бъде изрично отбелязано с мотивирана обосновка, като се посочи, че не се изискват коригиращи действия, за да се избегне последващо погрешно тълкуване на констатацията. Считаме, че въвеждането на подобен механизъм ще осигури проследимост, яснота и пропорционалност при отчитането на резултатите от удостоверяването, както и ще ограничи риска от неправилно представяне на несъответствията като съществени проблеми на системата. 2. По т. 4.2 (извадков подход): изрично да се разпише механизъм за допълнително		
	2. По т. 4.2 (извадков подход): изрично да се разпише механизъм за допълнително	2. Не се приема.	2. Удостоверява се типа ТУМГ. Основната проверка е задълбочена;

	удостоверяване на идентичността на всички устройства извън извадката, с цел ограничаване на възможностите за различна интерпретация. 3. По т. 6.4 (уязвимости, сигурност, оценка на уязвимости): 3.1. Предлага се въвеждане на стандарт за публична интерпретация на установените уязвимости, включително разграничение между теоретични и експлоатируеми рискове. 3.2. С оглед предвидените в методиката дейности по установяване и оценка на уязвимости в операционната система и приложния софтуер, предлагаме да се въведе праг (threshold) за значимост на констатираните уязвимости, който да определя кои от тях подлежат на задължително отразяване в крайния доклад и кои следва да бъдат разглеждани като технически незначителни. Предвид факта, че при всеки комплексен софтуер е възможно да бъдат установени значителен брой уязвимости с ниска или теоретична степен на въздействие, липсата на подобен праг създава риск от: • непропорционално натрупване на голям брой констатации без реално значение за изборния процес;	устройствата са избрани на случаен принцип. Задължително се представя и декларация за съответствие и идентичност. 3.1. Приема се по принцип. 3.2. Приема се по принцип.	3.1. Отражено е в т. 6.4 и 7.1 от Методиката. 3.2. Отражено е в т. 6.4 и 7.1 от Методиката и в Приложение № 4.
--	---	--	--

		• затруднена експертна оценка поради липса на приоритизация; • възможност за неправилна интерпретация, при която технически незначителни находки се представят като съществени рискове. В тази връзка се предлага въвеждане на: • минимален праг за значимост (напр. базиран на CVSS или еквивалентна система), под който уязвимостите се отразяват само в технически приложения, но не и в обобщения доклад; • изрично разграничение между: - експлоатируеми уязвимости с потенциално влияние върху изборния процес; - уязвимости без практическо приложение в контекста на ТУМГ; - механизъм за агрегиране на сходни уязвимости, с цел избягване на изкуствено увеличаване на броя на констатациите. 4. Да се създаде публично обобщено табло (dashboard), което да представя ключовите резултати от удостоверяването в разбираем формат за широката общественост.	4. Не се приема.	4. Предложението не попада в обхвата на Методиката. Докладът от удостоверяването е общодостъпен и се публикува на официалната интернет страницата на МЕУ.
--	--	---	------------------	---

9.	Георги Станчев	В Приложение № 4 към Методиката да се добави следното: Проверка на това дали Secure Boot е включен на ТУМГ, както и какво е съдържанието на ключовете РК (Platform Key), КЕК (Key Exchange Key) и базата данни на разрешените подписи (DB) в UEFI.	Приема се.	Проверката е включена в обхвата на Приложение № 4.