Становище на Българския институт за стандартизация

(становището се отнася само до материята, свързана с прилагане на технически стандарти и оценяване на съответствието, по която Българският институт за стандартизация е компетентен)

Забележка: Оценяване на съответствието включва: изпитване, проверка, одит и сертификация, както и акредитация на органи за оценяване на съответствието

1. **По проекта на ЗИД на ИК, внесен от народни представители на ДБ и заведен под номер 154-01-2**

   По отношение предложението за създаване на нов чл. 213б със заглавие „Независим одит на системата за машинно гласуване“

По принцип всяка система за електронно гласуване трябва да позволява извършването на одит и това е разписано в Препоръката на Съвета на Европа CM(2017)50E (пар.VII, т.39) и обяснителния меморандум към нея (стандарт №39).

Обръщам внимание, че разписаните в Препоръката и обяснителния меморандум стандарти, се наричат **правни стандарти** и освен тях има други стандарти, които се наричат **технически стандарти, които са предмет на дейност на Българския институт за стандартизация (БИС).**

В ИК липсва определение за система за електронно гласуване.

Такова определение е дадено в Препоръката на Съвета на Европа CM(2017)50E.

Електронна система за гласуване (ЕСГ): хардуер, софтуер и процеси, които позволяват гласоподавателите да гласуват с електронни средства на избори или на референдум.

При ясно дефиниране на ЕСГ възникват няколко въпроса:

- Какво се одитира, какъв е обхватът на одитиране – предмет на одита са процесите така, както са разписани в чл.213, ал.2 и в техническите изисквания определени от ЦИК в чл.213, ал.3;
- Как се извършва одитът, по какви правила и по каква методология – ако се приеме, че това е технически одит, то правилата и методологията са определени в БДС EN ISO 19011 Указания за извършване на одит на системи за управление. Правилата, по които се извършва одита трябва да са едни същи за всички заинтересовани. В противен случай ще се получат различни резултати и системата ще се компрометира;
- Кой може да одитира – обикновено одитът се извършва от експерти, наречени сертифицирани одитори, които са преминали обучение, са положили изпит и им е издаден сертификат, в който задължително присъства кодът на икономическата дейност, по която имат нужното образование и професионален опит;
- В случай на установени несъответствия (съществени и несъществени), предвидено ли е време за коригиращи действия – обикновено това е подходът който се прилага, а не да се отменя машинното гласуване (заради една бълха да се изгаря юрганът).

Централната избирателна комисия (ЦИК) **не е компетентна** да определя реда за извършване на одита.

Освен от процеси ЕСГ се състои от хардуер и софтуер.

Ако приемем, че хардуерът е вече с оценено и удостоверено съответствие, а софтуерът е системен и приложен, то на оценяване подлежи отново и единствено приложният софтуер.

Това оценяване на приложния софтуер се нарича верифициране (проверка) и валидиране. Валидирането е предоставяне на доказателство, че софтуерът отговаря на предназначението си. Правилата за верифициране и валидиране са разписани в серия международни стандарти. Обръщам внимание, че в България **няма акредитиран орган за извършване на верифициране и валидиране. До този момент тази дейност се извършва от Държавната агенция „Електронно управление" по определена методика.**

Предложение: Всички заинтересовани страни, посочени в чл.213б, ал.2, да доказват своята компетентност за извършване на одит по определените правила и методология в БДС EN ISO 19011-Указания за извършване на одит на системи за управление . В случай, че не могат да докажат такава компетентност, да наемат сертифицираща организация, която да извърши одита.

2. **По проекта на ЗИД на ИК, внесен от народни представители на ИТН и заведен под номер 154-01-9**

   По отношение предложението за промяна в чл. 213а, ал.3 – числото „30" се заменя с „20"

Първото впечатление е, че в мотивите към предложението липсват аргументи за намаляване срока за оценяване и удостоверяване на съответствието на доставения тип техническо устройство за машинно гласуване с изискванията по чл. 213, ал. 3 и изискванията на техническата спецификация.

При липсата на мотиви може да се предположи, че намаляването на срока е свързано с факта, че устройствата за машинно гласуване са вече с удостоверено съответствие.

При липсата на конкретен текст в ИК как се извършва първоначално и последващо удостоверяване на съответствието се предполага, че това трябва да бъде уредено с Методиката, утвърдена от председателите на трите институции.

От една страна се предполага, че при последващо удостоверяване на съответствието няма да се прилагат всички процедури към Методиката и конкретно Процедура 1 и Процедура 2, а от Процедури 3 и 4 ще се приложат само конкретни изпитвания и проверки, отнасящи се до спецификите на провежданите избори. **Но, тъй като отделните процедури се изпълняват от различни екипи и паралелно, това няма да доведе до съкращаването на срока за изпълнение.**

От друга страна предвиденият срок от 30 работни дни не взема в предвид какво се случва при наличието на несъответствия (съществени и/или несъществени) и **не предполага време за извършване на коригиращи действия.**

Предложение: срокът от 30 работни дни да остане

3. **По проекта на ЗИД на ИК, внесен от народни представители на ИМВ и заведен под номер 154-01-18**

По отношение предложението за създаване нов раздел IV със заглавие „Дистанционно електронно гласуване“ и конкретно по чл.214в, ал.2, т.12

Разписано е изискването „системата трябва да бъде сертифицирана по най-висок ISO стандарт за качество и устойчивост на използвания хардуер и софтуер“.

В стандартизацията не съществува класификация на стандартите по „височина“, нещо повече съществува строго правило, че за един обект на стандартизация може да има само един стандарт.

Стандартите за информационни технологии не се разработват в ISO и не носят означението ISO.

Стандартите за информационни технологии се разработват и приемат в съвместния технически комитет JTC 1 на ISO и IEC (Международната електротехническа комисия) и носят означението ISO/IEC – например ISO/IEC 27001 – Система за управление сигурността на информацията, който е приложим в случая.

За да бъде сертифицирана по ISO/IEC 27001, системата не може да се състои само от хардуер и софтуер. Това вече беше обяснено по-горе, че предмет на одит и сертифициране са процесите, от които се състои системата.

По отношение чл.214в, ал.2, т.20 и т.21

За извършването на одит и проверка (комбинацията от одит и проверка има логика, тъй като одитът се извършва на процесите, а проверката на софтуера) от упълномощени органи важи становището по законопроект 154-01-2 с добавянето на следния коментар:

Не е ясно кой, как и на каква основа упълномощава въпросните „упълномощени органи“.

По отношение чл.214в, ал.3 – ЦИК определя техническите изисквания към апаратната (хардуер) и програмната (софтуер) отново са пропуснати процесите от системата, които са предмет на одит и сертифициране.

4. По проекта на ЗИД на ИК, внесен от народни представители на ДБ и заведен под номер 154-01-21

По отношение създаването на нов раздел IXа със заглавие „Дистанционно електронно гласуване“

В новосъздаденият чл.214а, ал.3 отново системата е дефинирана като съвкупност само от софтуерни и хардуерни компоненти и са пропуснати процесите на системата.

Отново в т.12 на ал.3 е предвидена сертификация на системата по ISO 27001, а такъв стандарт не съществува. Правилното изписване на стандарта е ISO/IEC 27001.

Предвидено е и сертифициране на модела на качество на софтуера по ISO 25010. Правилното изписване е ISO/IEC 25010. Трябва да се има в предвид факта, че в България няма орган за сертификация по ISO/IEC 25010 и пак някоя организация трябва да бъде набеждавана за компетентна.

По отношение на одита и проверката от страна на упълномощени органи, становището е същото като при 154-01-18.

Проектите на ЗИД на ИК под номера 154-01-26 и 154-01-28 нямат отношение към материята стандарти и оценяване на съответствието

Ивелин Буров

Председател на УС на БИС