ЦИК-06-43/15.10.16г.

ОТГОВОРИ

ВЪВ ВРЪЗКА СЪС СИГУРНОСТТА НА МАШИННОТО ГЛАСУВАНЕ В ИЗБОРИТЕ ЗА ПРЕЗИДЕНТ И ВИЦЕПРЕЗИДЕНТ НА РЕПУБЛИКАТА

1. Има ли изпълнителят предварително разработени процедури и правила за работа с компютърните системи за машинно гласуване (КСМГ), които да предостави в ЦИК?

Да, Сиела Норма АД има предварително разработени процедури и правила за работа с компютърните системи за машинно гласуване (КСМГ), които да предостави в ЦИК.

Сиела Норма АД, като изпълнител на досегашните две експериментални машинни гласувания и едно с реално отчитане на гласовете, винаги е предоставяло на ЦИК процедурите и правилата за работа с КСМГ. Част от процедурите са:

- Процедура за работа на изборите и в предизборния ден, и при евентуален балотаж.
- Процедура за инсталиране на машините в градовете.
- Подробен план-график за провеждане на логистиката по места, с часове, отговорни лица от името на изпълнителя и контакти.
- Процедура за оформяне на необходимата документация – оформяне на Приемо-предавателни протоколи на КСМГ в предизборния ден и в изборния ден, както и на евентуален балотаж.
- Процедура за подмяна на дефектирала машина в изборния ден

2. Има ли определен служител по сигурността на компютърните системи за машинно гласуване (КСМГ[4])?

Да, има определен служители в организацията по сигурността на компютърните системи за машинно гласуване (КСМГ) и техните имена са: Христо Филипов, Явор Иванов.

2.1 Какво гражданство има посоченото лице?

Българско

3. Има ли определен администратор по сигурността на КСМГ? 3,1 Какво гражданство има посоченото лице?

Да, има определени администратори по сигурността на КСМГ и техните имена са: Иван Тодоров, Веселин Тодоров и Елеонора Вълова и имат българско гражданство.

4. Определени ли са задълженията на посочените по-горе лица в длъжностните им характеристики или договори?

Да, определени са задълженията на оторизираните лица в длъжностните им характеристики.

5. Кои лица в организацията имат достъп до документите за сигурност на КСМГ?

Лицата в организацията с достъп до документи за сигурност на КСМГ са: Христо Филипов, Явор Иванов, Веселин Тодоров и Елеонора Вълова.

5.1 Как е регламентиран този процес и с какъв акт?

Този процес е регламентиран в ISMPR-1_Процедура за Управление на сигурността на информацията и ISMPR-13_Процедура Контрол на достъпа, които са част от Система за управление на информационна сигурност ISO\IEC 27001:2013. Утвърден е със заповед на комите по ИС.

6. Определено ли е кой периодично ще ревизира документите по сигурността и ще извършва актуализацията при необходимост?

Да, има екип в организацията, които периодично ревизира документите по сигурността и извършва необходимата актуализация. Имената на лицата в екипа са: Веселин Тодоров, Христо Филипов и Явор Иванов.

6.1 Периоди на ревизия и актуализация и къде е отразено това?

В организацията периода за ревизия и актуализация е постоянен и непрекъснат и това е отразено в ISMPR-6_Процедура Управление на непрекъснатостта и ISMPR-4_Процедура Мониторинг, анализ и подобрения, които са част от Система за управление на информационна сигурност ISO\IEC 27001:2013.

ФИЗИЧЕСКА СИГУРНОСТ В ПОМЕЩЕНИЯТА НА ИЗПЪЛНИТЕЛЯ

7. Определена ли е средата, в която ще се извършва получаването, инсталирането, верифицирането и извеждането на КСМГ?

Чл. 2 от ЗЗЛД

Да, определена е средата, в която ще се извършва получаването, инсталирането, верифицирането и извеждането на КСМГ. Сиела Норма АД разполага с площ от 800 кв.м., специално осигурена за извършване на дейностите, описани по-горе.

8. Осигурен ли е контрол и защита на достъпа до КСМГ и по какъв начин?

Да, осигурени са контрол и защита на достъпа до КСМГ.
Сградата, в която ще се извършват дейностите по обслужване на КСМГ е защитена със СОТ и денонощна жива охрана.
Допълнително ще бъде уведомено местното районно управление на МВР, за дейността, която ще се извършва в обекта, периода, както и обема на дейностите. Това е практика за Сиела Норма АД, като разбира се, ще уведомим МВР, след като подпишем договор, като изпълнител.

9. Определени ли са лицата, имащи достъп до помещенията, в които се получава, инсталира, верифицира и извежда от експлоатация на КСМГ?

Като отбелязваме, че в зададеният въпрос фигурира термина – „извежда от експлоатация", което не е част от процеса, т.е. машината се въвежда в експлоатация, нашият отговор е:
Да, определени са лицата, които имат достъп до помещенията, в които се получава, инсталира, верифицира и въвежда в експлоатация КСМГ. Извеждат се готовите машини, за да бъдат разпределени по места по строго определен график, съгласуван с ЦИК, като всеки път подаваме освен график за логистиката и имената на лицата, които са включени в процеса.

10. Как и по какъв начин е предвидено да се предотврати неоторизиран достъп до съдържанието (хардуер и софтуер на КСМГ)?

Предотвратяването на неотозириран достъп до съдържанието (хардуер и софтуер на КСМГ) е предвидено да се осъществи, **чрез осигуряване на оторизиран достъп на лицата**, които са част от процесите.

ПЕРСОНАЛНА СИГУРНОСТ НА СЛУЖИТЕЛИТЕ НА ИЗПЪЛНИТЕЛЯ

11. Има ли готовност и в какъв срок изпълнителят да предостави доказателства за наличие на необходимата квалификация на системния персонал за работа с КСМГ със съответното оборудване?

Да, организацията има готовност да предостави поисканата информация в срок от 10 работни дни считано, от постъпилото искане.

12. Има ли възможност изпълнителят да представя детайлна техническа и експлоатационна документация за използваната техника за машинно гласуване на системния персонал и с какъв акт ще бъде извършвано това?

Да, организацията има възможност да представи протоколи от проведени обучения, издадени сертификати на персонала за проведените обучения на системния персонал. Протокол от компанията производител на машините за гласуване, за проведени обучения на обручители, на наши служители, които могат да водят обучения и да издават сертификати

13. Извършено ли е или в какъв срок ще бъде извършено обучение на различните категории служители на изпълнителя?

Да, извършено е обучение на различните категории служители на изпълнителя. Обучението е организирано на няколко етапа, като може да отбележим, че като три пъти вече изпълнител на машинното гласуване в България, голяма част от екипа е бил вече част от процеса и е преминавал няколко обучения в течение на три години.
До края на изпълнение на договора, който би се сключил с Възложителя се планират провеждането на още 3 броя присъствени обучения за екипа на Сиела Норма АД, както и вдигане в защитена среда на всички обучителни материали, включително и видео материали, които да са на разположение на служителите.
Видео обучителен материал е предвиден и за екипите на Секционните избирателни комисии.
Срокът за приключване на обучителния процес е до 14 дни преди изборите.

14.Определени ли са правомощията на персонала, работещ с КСМГ така че да не се допуска възможността едно лице да познава или контролира изцяло важните елементи на сигурността?

Да, определени са правомощията на персонала в организацията и стриктно се съблюдават приетите политики, процедури и инструкции по Система за управление на информационна сигурност ISO\IEC 27001:2013.

КОМПЮТЪРНА СИГУРНОСТ

15.Възможно ли е изпълнителят да предостави пълно описание на инсталирания хардуер и софтуер в КСМГ на възложителя?

Описание на хардуера и софтуера на КСМГ:

1. Компоненти на машината за гласуване

Машината за гласуване трябва да се състои от:

1.1. Сензорен екран с размер 17" – който позволява удобно разполагане на всички елементи, съдържащи се на хартиената бюлетина, без да се сбива текстът. Екранът разполага с достатъчно място за визуализиране на полетата за избор на избраната партия или коалиция, с цел предотвратяване на възможност за грешка при трепване на пръста.

1.2. Компютърен модул.

1.3. Принтер за отпечатване на разписка за подадения вот (електронна бюлетина), на начален и на финален протокол.

- Принтерът работи с ролкова хартия и има възможност за автоматично отрязване на разписките;
- Използваната ролкова хартия е непрозрачна;
- Принтерът има предвиден механизъм за сигурност при зареждането на хартия - защитен с ключ.

1.4. Резервно токозахранване (UPS) – предназначено да осигури работата на машината при кратковременно прекъсване на електрическото захранване, както и да предотврати евентуална загуба на данни в случаите на токов удар.

2. Компонентите на машината са комплектувани по следният начин:

- Като монолитен блок, разположен в специално проектиран корпус,

3. Характеристики на компонентите на машината за гласуване:

3.1. Сензорният екран е ориентиран под 90 градуса спрямо пръста на избирателя. Екранът е произведен по модерна технология, която не изисква процедура по калибриране на сензорния панел.

3.2. Компютърният модул разполага с препоръчителни оперативна памет и процесор в зависимост от избраната операционна система:

- Windows XP или Windows Embedded-процесор с тактова честота минимум 800 MHZ и оперативна памет минимум 1 GB;
- Windows 7/8 – процесор с тактова честота минимум 1.2 GHz и оперативна памет минимум 1 GB;
- Linux - процесор с тактова честота минимум 500 MHz и оперативна памет минимум 1 GB.

3.3. Принтерът работи с ролкова хартия с достатъчна дължина за отпечатване на минимум 450 разписки за гласуване.

- Използваният шрифт е с достатъчна големина за отчетливо отпечатване на вота върху разписката.
- В разписката е предвидено място за бар код или други контроли, изисквани от предложения „процес за последващ контрол на преброяването по хартиена следа".
- Бързината на разпечатване е достатъчна за отпечатване на разписка за гласуване - не повече от 5 секунди.

ЕЛЕКТРОННАТА МАШИНА ЗА ГЛАСУВАНЕ /ЕМГ/ SAES-3377

SAES-3377 е машина за електронно гласуване от следващо поколение с тъч скрийн за електронно гласуване, с няколко нива на сигурност, което я прави 100% сигурна, включен принтер за изборните бюлетини и контролните списъци, както и специален потребителски интерфейс, разработен за гласоподаватели със специални нужди.

По-конкретно, ЕМГ SAES-3377 EVM има възможности, които позволяват и увеличават изборния опит на всички гласоподаватели, независимо от нивото на тяхната компютърна грамотност и физически способности. „Сиела Норма" АД ще достави 535 машини SAES-3377 (500 машини + 35 резервни), които ще се разположат в определените секции за гласуване в страната, като във всяка избирателна секция ще има един комплект оборудване. SAES-3377 предлага предимства в няколко аспекта, а именно:

СИГУРНОСТ

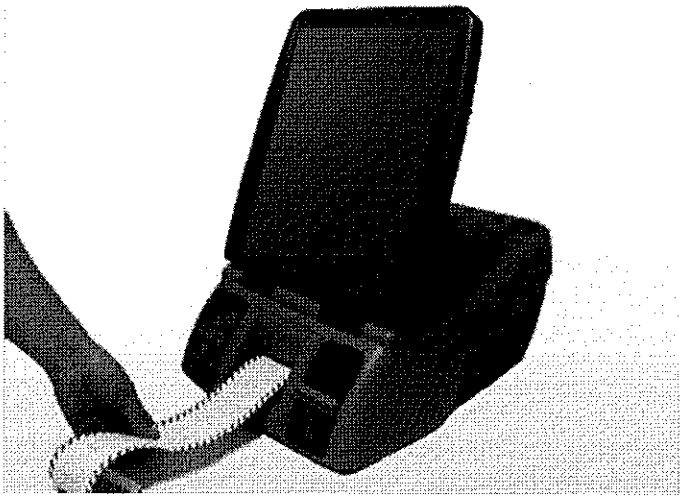
Чл. 2 от 331д

SAES-3377 е най-сигурната съществуваща машина за електронно гласуване. Тя предлага 100% сигурно електронно гласуване, включително:

- ✓ Най-модерни алгоритми за цифрово криптиране, включващи няколко нива на сигурност, гарантиращи цялостност и конфиденциалност на всички запазени данни;
- ✓ Широкомащабно запаметяване на информацията и избягване на загубата на информация;
- ✓ Вграден принтер за изборните бюлетини в реално време и за контролни списъци след приключване на гласуването и преди изпращането.
- ✓ Сигурни и разнообразни начини за изпращане

ПРИЛОЖИМОСТ И ПОДДРЪЖКА НА ВСЯКАКЪВ ТИП ИЗБОРИ

- ✓ Машината SAES-3377 има 17" (инчов) екран, разработен за избори, изискващи една или няколко изборни конфигурации.
- ✓ ЕМГ SAES-3377 EVM е снабдена със специален модул в помощ на гласоподаватели със специални нужди;
- ✓ Лесна за транспортиране и за съхранение – благодарение на специално разработените системи за транспортиране и съхранение.
- ✓ SAES-3377 се нуждае от малка поддръжка и е лесна за инсталиране при бъдещи избори;
- ✓ Гласоподавателите няма да се нуждаят от специални компютърни умения, за да използват машината за гласуване SAES-3377
- ✓ Благодарение на монолитната си блокова конструкция, машината за гласуване SAES-3377 е лесна за транспортиране до всяко предвидено място и е лесна за инсталиране, както и за опаковане след приключване на изборите.

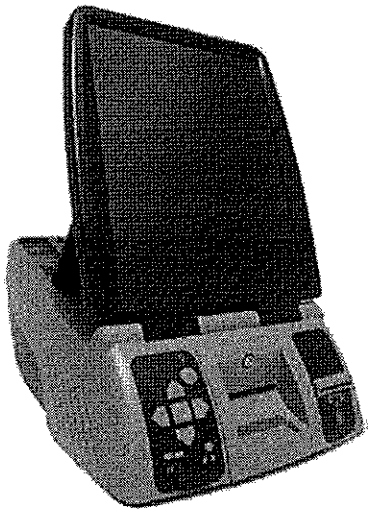


Фигура 1: SAES-3377 позволява да се правят проверки на всички етапи от изборния процес, в предизборния период, по време на гласуването и след гласуването, както преди изпращането на изборните резултати на центъра за предварителните изборни резултати, така и след това. благодарение на постоянния носител за запазване на данни и пълен опис на изпълнените операции.

ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ

41-2 от 331А

- Дъно
  - ✓ **Вградена памет**: SSD
  - ✓ **BIOS:** Phoenix-Award 4Mbit
  - ✓ **CPU:** VIA Eden 1GHz
  - ✓ **Оперативна система:** Клиентска версия на Windows XP вградена
  - ✓ **RAM:** 2GB
- Памети
  - ✓ **Обем**: От 512 MB до 4 GB, 1 слот за флаш-памет
  - ✓ **Вградена памет**: 1 GB
  - ✓ **Външна памет**: Устройство за резервиране на данни за осигуряване и за електорален контрол
- Монитор
  - **Размер на екрана**: 17" – ориентация : портрет
  - **Резолюция**: 1024 x 1280 VGA
  - **Тъч скрийн**: Самокалибрираща се омична технология – не изисква калибриране по време на изборния процес
  - **Ъгъл на позициониране на екрана**: 0° - 90°



Фигура 2: Машината за електронно гласуване SAES-3377 поддържа всякакви видове избори – от референдуми до многопартийни избори и избори между множество кандидати.

- Принтер
  - **Технология**: Автокалибриращ се с минимална резолюция 200 dpi
  - **Нож за хартия:** Нож за цялостно/частично рязане
  - **Вид хартия:** Непрозрачна термо чувствителна хартия
  - **Спецификация на хартията**
    - Тегло: 78 грама, дебелина: 82 µm
    - Широчина: 79.5 mm - 80mm
    - Тръба: 12.5 mm вътрешен диаметър 16.0 mm външен диаметър
  - **Бюлетини:** Осигурява разпечатване на над 450 изборни бюлетини с едно зареждане на хартията
  - **Сигурност:** Принтерът съдържа блокиращ механизъм с цел предпазване от сваляне на хартиеното руло по време на изборния процес
  - **Скорост**: Разпечатва изборната бюлетина з по-малко от 5 секунди.
- Машина
  - ✓ **Размери:**
    - Широчина: 13.78 in
    - Височина: 9.72 in
    - Дължина: 19.88 in
  - ✓ **Тегло:** 24.91 lbs
  - ✓ **Диапазон на работната температура:** 41 °F - 140 °F
- Електрозахранване
  - **Променлив ток на входа**: 240VAC / 50Hz
  - **Резервно напрежение:** Предлаганата система включва UPS за повече от 15 минути автономна работа в случай на прекъсване на захранването.

- Аксесоари
  - **Устройства за гласуване:** Конфигурация от кандидатските листи в дигитална система, имитираща използването на хартиени бюлетини.

- **Защитен калъф**
- **Външна батерия за дългосрочна работа:** Може да бъде добавено резервно външно захранващо устройство.
- **Опции за активация**
  - Бутон за дистанционно активиране – това е опция, която се предлага за проекта по време на изборите
  - Устройство за активиране на смарткарти;
  - Биометрично устройство SAES-RSA 100

- Други
  - **Сертификации:** FCC, CE
  - **Транспортиране:** SAES-3377 с бутона за дистанционно активиране се доставя в куфар, който предпазва устройствата и улеснява транспортирането и съхранението.

4. Функционалност на машините за гласуване:

- Всички подадени гласове се съхраняват цифрово подписани и криптирани;

- Гласовете се съхраняват на два отделни физически носителя на памет (върху носителя, на който е инсталирана операционната система и допълнително копие на втори носител);

- Машината поддържа журнал на гласовете (Log), съдържащ информация за всеки един акт на гласуване. Самият лог може да бъде криптиран или не, но информацията за отделните подадени гласове задължително е криптирана.

- Машината поддържа системен журнал (Log), съдържащ информация за всички настъпили събития: стартиране на изборния ден, приключване на изборния ден, евентуални прекъсвания в работата на машината поради липса на електрическо захранване, евентуални повреди и неправилно функциониране на части от машината и др.

- Машината може да осигурява back-up на постоянно въвеждаща се информация през деня – в случай на отказ/техническа повреда с флашката – за да може информацията да бъде възстановена дори и при повреда на флашката.

- Машината **няма** интернет връзка или връзка с други потребители след инсталирането й в изборната секция.

5. Дизайн на бюлетината на екрана и процедура за избор:

5.1. Бюлетината на екрана ще изглежда по идентичен начин както хартиената бюлетина (законово изискване) за общински съветници за Столична община;

- Големината на квадратите и лентите предоставят достатъчно място за комфортен избор със сензорен екран;

- Лентите и квадратите са разположени по сходен начин в ляво - както на хартиената бюлетина;

- Използват се еднакви шрифтове и еднакво графично оформление на бюлетините за всички политически партии и коалиции - за да се избегнат протести, че не са коректно представени в електронната бюлетина.

- Метод за скролване при дълга бюлетина – няма да бъде използван „touch scroll" поради опасност от неволно избиране на грешна партия или коалиция. Скролването ще се извършва с два големи, ясно видими и обозначени бутона (по подобие на познатия на гражданите инерфейс на банкоматите);

5.2. Електронната бюлетината ще дава възможност да се гласува с „празна бюлетина", т.е. без да се прави избор.

5.3. При гласуване, след извършване на избора за партия, коалиция местна коалиция или независим кандидат за общински съветник, както и при преференциалното гласуване, на екрана ще се визуализира съобщение за потвърждение на направения избор. Съобщението за потвърждение ще съдържа името на избраната партия, коалиция, местна коалиция или независим кандидат, изобразено с голям шрифт, и под него в случаите, когато е избрана преференция, щесе визуализира името на избрания кандидат.

Избирателят ще има възможност за:
- потвърждаване на избора, след което ще се разпечата разписката;
- отказване на избора и връщане в предишното меню за корекция на избора.

Процедурата за избор е съобразена с описаната в т. 7 „процедура за активиране на машината за един глас", т.е. не се дава възможност на избирателя да гласува повече от веднъж.

6. Процедура за активиране на машината за един глас

Активирането на машината за единично гласуване ще се извършва след проверка на личната карта на избирателя по някой от следните начини:

- С бутон, натискан от член на СИК за активиране на един глас;

За да се гарантира невъзможността един и същ гласоподавател да подаде повече от един глас, машината за електронно гласуване /МЕГ/ ще се активира от определено лице /председател на секционната изборна комисия или друго подобно лице/ след валидирането на биографичната информация на гласоподавателя на базата на представяне на валидна лична карта и съответствие с утвърден избирателен списък и проверка дали новият гласоподавател не е гласувал вече. Председателят ще може да активира сесията по гласуването само когато МЕГ не е в активна сесия. Освен това, не е възможно да се поставят „в изчакване" на опашка активации с цел да се избегнат грешки от страна на членове на секционните комисии, които работят с бутона за дистанционно активиране.

Най-накрая МЕГ издава продължителен звуков сигнал за потвърждение и разпечатва бюлетината, давайки знак по този начин, че сесията по гласуване на предишния гласоподавател е приключила и председателят трябва да изчака, докато от тъмната стая, където е МЕГ, излезе последният гласоподавател, за да може да активира следващото гласуване.

След гласуването на избирател машината се деактивира и впоследствие се активира при гласуване на следващ избирател.

7. Процедура по гарантиране анонимността на вота при събирането на разписките от гласуването

Ще бъде приложен един от двата възможни варианта за събиране на разписките, а именно:

- Разписката от гласуването попада в ръцете на избирателя, след което тя се пуска в специална изборна кутия, пред комисията;

Разписката се отпечатва директно от машината, на непрозрачна хартия, след което се сгъва на две, като отпечатаният текст остава от вътрешната страна и остава невидим за останалите, с което се гарантира анонимността на вота.

Предлаганата процедура осигурява гаранции за спазване на анонимност на вота при изпълнение на действията по събиране на разписките от гласуването.

8. Мерки и процедури за гарантиране на тайната на вота:

8.1.Машината гарантира пълна анонимност на подадения вот.

„Сиела Норма“ АД представя описание на предвидените в предлаганото решение мерки за постигане на тази цел.

По което и да е време е невъзможно да се разбере съответствието между хартиените бележки от гласуването в кутията за гласуване с гласоподавателя, който ги е пуснал там. Между защитите, които помагат да се осигури анонимност на вота, с решението, осигурявано от „Сиела Норма“ АД, ние можем да изброим следното:

- ✓ Не се обменя лична информация между дистанционния бутон за активиране и машината за гласуване.
- ✓ Машината за гласуване стои в кабината за гласуване само за оторизирани гласоподаватели. Гласоподавателят влиза сам в кабината за гласуване и машината се активира само след като гласоподавателят е готов да гласува и председателят се увери, че той/ тя е сам/а.
- ✓ Дигиталното представяне на гласа не се записва в последователност в машината за гласуване.
- ✓ Подобно на ръчното гласуване, пускането на хартиената бележка от вота в кутията за гласуване не може да определи последователността на вота в кутията за гласуване когато се отвори.
- ✓ Само валидна памет със сертифицирано приложение от гласуването в сертифицирана оперативна система може да протича в машината за гласуване през изборния ден.
- ✓ По време на гласуването паметта е защитена от физически достъп, за да се предотврати манипулиране от неоторизирани потребители.
- ✓ Кутията за гласуване се проверява дали е празна преди началото на процеса на гласуване след това кутията се затваря със защитни средства и се държи на открито място по време на целия изборен ден.

По отношение на гласовете, съхранявани дигитално в машината за гласуване, гласовете се съхраняват в специално генерирана секция от паметта със следните качества:

- Всеки вот е отделен файл в системата с файлове
- Името на всеки файл е уникално и се генерира на случаен принцип
- Вотът се съхранява в позиция, случайно избрана в паметта, което означава, че вотовете не се съхраняват в последователност в системата от файлове.

9. Допълнителни процедури за сигурност:

- Машината не стартира процедура за гласуване, без да са включени и двете памети - основна и резервна;

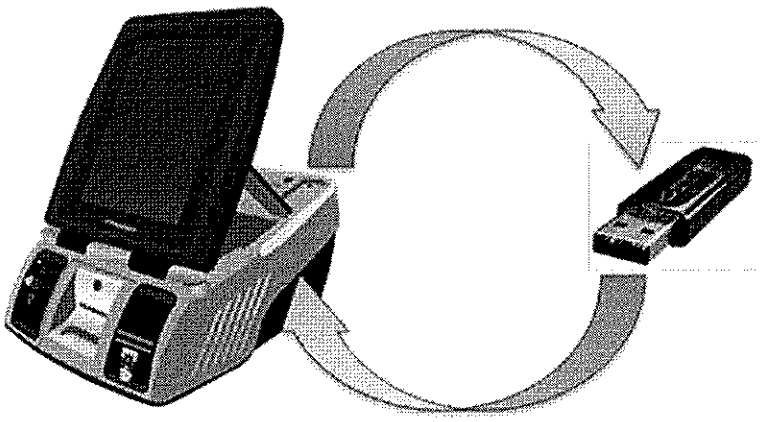
- Не се допуска принтиране на разписката с вота преди извършване на изрична проверка от машината, че вотът е вече съхранен успешно и на двете памети.
- Има предвидена процедура за защита на операционната система от неоторизиран достъп и нежелани модификации в случаите, когато паметта, съдържаща операционната система, се съхранява в СИК преди изборния ден.

„Сиела Норма“ АД осъзнава и оценява аспектите на допълнителната сигурност, които трябва да се заложат в нашето решение и ние бихме гарантирали, че нашето решение покрива всички технически и функционални аспекти и аспектите на сигурността съгласно изискванията на Министерския съвет на Република България. В този раздел е обяснено какво се предвижда с оглед допълнителните компоненти на сигурността и процедурните аспекти на нашето решение.

А. <u>Вотът трябва да се запази на две отделни физически устройства-памет /мемори стик/ /на които е инсталирана операционна система и едно допълнително копие на второ устройство-памет/.</u>

„Сиела Норма“ АД гарантира непрекъснатост на дейността чрез прилагане на процес на резервиране на данните през целия изборен процес с използване на машини за електронно гласуване. Машината използва две устройства-памет: вътрешна и външна, като и двете памети са физически защитени, за да се елиминира възможността външни потребители да могат да ги свалят.

Във всеки един момент всеки файл, който е необходим за работата на машината, се поддържа синхронизиран между двете памети. С други думи, всяка памет е огледало на съответната ответна част. Машината за електронно гласуване не позволява работата да продължи, ако възникне неочаквана промяна в информацията, запазена на една от паметите, което добавя допълнително ниво на сигурност и надеждност.



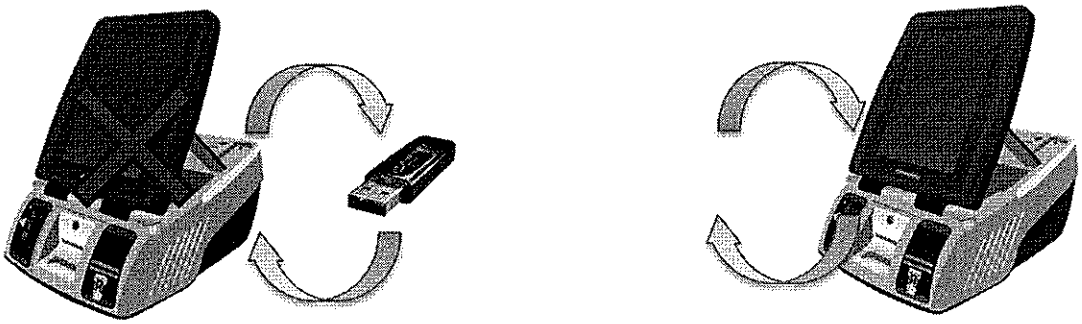
Фигура: Гарантиране на непрекъснатост на дейността чрез използване на 2 различни информационни носителя

чл. 2 от ЗЗЛД

Правилното продължаване на процеса на гласуване се гарантира дори и в случаите, когато машината спре работа поради неочаквана причина /например повреда на една от физическите памети/; изборното приложение има механизъм за възстановяване, който се базира на възстановяване, което позволява непрекъснатост на работата. В зависимост от коренната причина за проблема, възстановяването ще се фокусира върху машината или върху външната памет.

Механизъм за „Възстановяване на машината“:

Този механизъм се състои в намиране на нова машина, която е предварително конфигурирана като резервна машина за смяна и се изтегли информацията от външната памет върху вградената памет на новата машина.



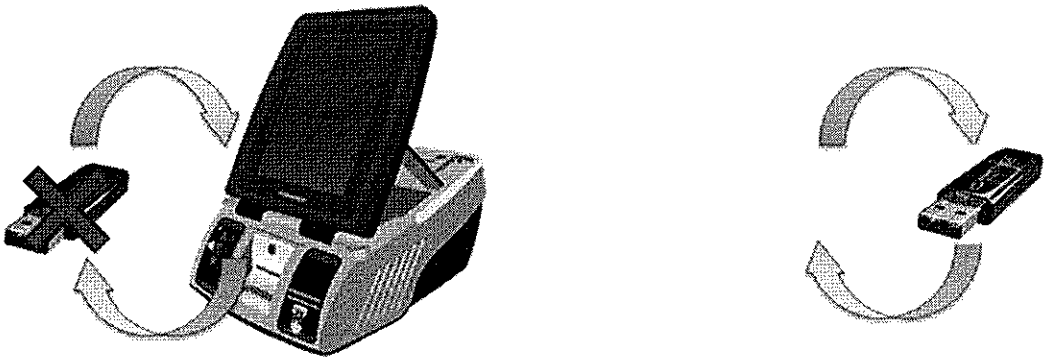
Фигура: Смяна на машината с изтегляне на информацията от външната памет върху вградената памет на новата машина

Резервните машини за смяна идват със същото защитено приложение, както при основните машини. Резервните машини ще имат специален ключ, който позволява на машината да отваря файловете на външната памет, които първоначално са били криптирани с помощта на уникалния ключ на основната машина.

Механизъм за „Възстановяване на паметта“:

Приложението има друг механизъм за възстановяване, познат като **„Заместваща памет“,** който позволява работата да продължи в случай, че външната памет, използвана за резервиране на данните, се повреди или не е съгласувана. Този механизъм включва смяна на паметта, използвана в момента, с нова сертифицирана памет, която ще се използва за смяна. Заменящата памет е сертифицирана с криптиран файл, което предотвратява възможността произволна памет да бъде използвана като заместваща памет. Машините са свързани с външната памет по време на работата на машините, което позволява машините да работят, като използват обикновена външна памет. Процесът на смяна на паметите осигурява синхронизация на данните от вградената памет и от външната памет, като се създава връзка между машината и новата памет.

Ч.2 от 331Д



Фигура: Смяна на паметта с нова сертифицирана памет

B. <u>Нежелателно използване на "местене чрез докосване", което създава опасност от това да бъде избрана грешна партия или коалиция необратимо. Препоръчва се местенето да се прави с двата големи, ясно виждащи се и маркирани бутони /подобни на познатите такива от банкоматите – АТМ машини/.</u>

При гласуването трябва да се предотврати използването на местене във всяка точка на екрана на машината за гласуване. Само на списъка за избор на кандидати и само ако списъка с кандидати, включващ партии, коалиции и независими кандидати, е прекалено дълъг и не се вмества на една страница, може да се използва метода за местене по страници, за да се постигне съответствие с вида и усещането при хартиената бюлетина, като по този начин се избягва евентуално объркване по време на избора на опция.

C. <u>Имената за преференциален избор не се показват на самата електронна бюлетина, но изборът на преференция трябва да се покаже на екрана, за да потвърдите своя избор и той съответно да се разпечата върху бюлетината.</u>

Върху основната електронна бюлетина с избор на кандидати имената на преференциите не се виждат; появява се само номерът, който представлява преференцията. Името на избраната преференция се вижда на страницата за преглед непосредствено преди гласоподавателят да потвърди, че пуска гласа си.

D. <u>Решение, което да гарантира невъзможност един и същ гласоподавател да подаде повече от един глас</u>

За да се гарантира невъзможността един и същ гласоподавател да подаде

чл. 2 от ЗЗЛД

повече от един глас, машината за електронно гласуване /МЕГ/ трябва да се активира от определено лице /председател на секционната изборна комисия или друго подобно лице/ след валидирането на биографичната информация на гласоподавателя на базата на представяне на валидна лична карта и съответствие с утвърден избирателен списък и проверка дали новият гласоподавател не е гласувал вече. Председателят ще може да активира сесията по гласуването само когато МЕГ не е в активна сесия. Освен това, не е възможно да се поставят „в изчакване“ на опашка активации с цел да се избегнат грешки от страна на членове на секционните комисии, които работят с бутона за дистанционно активиране.

Най-накрая МЕГ издава продължителен звуков сигнал за потвърждение и разпечатва бюлетината, давайки знак по този начин, че сесията по гласуване на предишния гласоподавател е приключила и председателят трябва да изчака, докато от тъмната стая, където е МЕГ, излезе последният гласоподавател, за да може да активира следващото гласуване.

E. Когато бюлетината е в ръцете на гласоподавателя - процедурата за сгъване на бюлетината, преди да я пусне в урната, или как ще се гарантира анонимността на гласуването.

Бюлетината се разпечатва така, че цялата информация за гласуването е ориентирана нагоре, като тя е предварително срязана, за да може гласоподавателят да си я вземе. Същият трябва да вземе бюлетината и след като провери отпечатаната информация, трябва да я сгъне през средата, като изборната информация остане вътре, след което да я пусне в изборната урна.

F. Процедура за предотвратяване на възможността за разкриване на вотовете чрез анализиране на електронните журнали

Електронните журнали съдържат всички транзакции, извършени по време на целия изборен процес от машините за гласуване. При подаването на вотове транзакциите, записани в електронните журнали, са транзакции за запаметяване и транзакции за разпечатване на всеки вот и няма начин тази транзакция да е свързана с вота, който ги е генерирал. Гласовете се запаметяват в специално създаден отдел на паметта и имат следните характеристики:

- ✓ Всеки вот е един единствен файл в системата от файлове;
- ✓ Името на всеки файл е уникален и случайно генериран;
- ✓ Вотът се запазва на случайно място в паметта, което означава, че гласовете не се запаметяват в последователен ред в системата от файлове.

Всички вотове се запаметяват с датата и часа на начало на избора с цел да

се предотвратят опитите да се разбие тайната на гласуването чрез обвързване на датата и часа на гласуването с датата и часа, когато дадено лице е упражнило своето право на глас. Създаването на временни файлове помага да се избегне това гласовете да бъдат запаметявани в открит последователен ред в системата от файлове.

G. Да не се позволява разпечатване на бюлетините преди изрична проверка на машината, че вотът вече е успешно запазен и на двете памети

Работата на машината по време на генерирането на всеки вот става чрез осъществяване на транзакция, което означава, че само когато една транзакция действително е приключила, подаденият глас се запаметява и се разпечатва хартиена бюлетина и едва тогава може да се извърши следващата транзакция.

Машината за гласуване осигурява разпечатване на бюлетин, тъй като процесът на запаметяване на бюлетината се извършва чрез осъществяване на транзакция и разпечатването на бюлетината се извършва едва след като е приключила успешно транзакцията по гласуване. След като вотът е успешно запаметен на наметите, се изпълнява процесът на разпечатване на хартиена бюлетина.

H. Процедура за защита на операционната система от външно влизане и нежелателни промени, когато операционната система е запаметена в ПЕК преди изборния ден.

За да се гарантира легитимността и надеждността на изборния софтуер, външните приложения и операционната система, „Сиела Норма“ АД предлага няколко процеса:

Процес на защита на приложението:

Този процес включва сертификация на кода на приложението, което ще работи през изборния ден на машините за електронно гласуване. Процесът на защита сработва по време на официална церемония, където ресурсният код на изборния софтуер се проверява, сертифицира и след това се защитава. По време на тази церемония се генерира тайна парола, която е известна само на приложенията, които са защитени по време на тази церемония. Този процес обвързва всички приложения и опитът да се промени или замести някое от тях ще разруши веригата от сертификати и приложението ще бъде отхвърлено. Много малко вероятно е генерираната парола да бъде открита, тъй като кодът на приложенията ще бъде криптиран и объркан, още повече че изборното приложение не извършва операции с тази секретна парола през RAM паметта в нито един момент по време на изборите.

Чл. 2 от ЗЗЛД

Процес на проверка:

Този процес се състои във валидиране на изборния софтуер на машината за гласуване във всеки един момент. Всяка МЕГ има уникален идентификатор, който се генерира от тях на базата на уникалните софтуерни и хардуерни компоненти. Уникалният код за софтуера и хардуера заедно с тайната парола и динамично генерирания сийд, може да се генерира код /уникален идентификатор, за да се провери дали изборното приложение, което работи в системата, са истински. Тази проверка може да се направи по няколко начина:

- Въвеждане на сийд в МЕГ, като се обърне внимание на генерирания код, след което се изисква от външното приложение кода, който използва като изходна информация идентификатора на ЕМГ /публичен/ и използвания операторски сийд /публичен/. Ако кодовете съвпадат, приложението е автентично.
- Автоматизиран процес в МЕГ, който при откриването на изборите иска уникален код за валидиране. Членът на секционната комисия трябва да поиска кода за външното приложение, който използва като изходна информация идентификатора на ЕМГ /публичен/, след което да въведе кода в МЕГ. След това машината валидира кода, като го сверява с този, който е генерирала тайно и ако те съвпадат, приложението е автентично.

Процес на валидиране на операционната система:

Този процес се състои в генериране на уникален идентификатор за операционната система, който се базира на ключове за регистрация, команден процесор и структура в момента на създаването. Когато изборният софтуер, който вече е инсталиран на място, влезе в процеса на проверка, този код ще се види и той може да се провери от члена на секционната избирателна комисия. Ако кодовете съвпадат, операционната система е автентична.

16. Възможно ли е изпълнителят да предостави на възложителя процедура за ревизия на инсталирания софтуер и хардуер за наличие на неоторизиран такъв?

Да. В мерките за софтуерна сигурност, които се изпълняват на всяка машина за гласуване, се включва генерирането на OS воден знак, който съответства на хеш на хешове изчислявани от няколко компонента в операционната система, включително:

- Framework конфигурационни файлове
- Частни програмни мениджъри и изпълними файлове

• Регистратура, специално обвързана с Операционната система, приложения стартиращи се при старт на системата (изпълними веднъж и продължаващи), конфигурация на модифицирания shell. (отговаря за изпълнението и удостоверяване на основното приложение)

Водният знак ОС гарантира, че всяка промяна върху някой от елементите по-рано, изброени, които биха могли да доведат до изпълнение на неразрешено или злонамерено приложение, заедно с основното приложение, ще бъде автоматично открити.

Възможно е да се предостави на възложителя с процедура, и да се провери, че операционната система и воден знак се поддържа през различни етапи от процеса. В зависимост от договорената процедурата, това може да изисква допълнителна разработка за предоставяне на договореното, и, по този начин, времето ще трябва да бъдат отчетено при обсъждането на процедурта.

От гледна точка на хардуер, всяка машина има врата с ключалки, които възпрепятстват достъпа до основни компоненти. Нещо повече, на изборния процес, при конфигурация на машините, се добавят ремъци номерирани сигурност (невъзможност за премахване или замяна, без да остави следа), за да се повиши сигурността на машината.

17.Възможно ли е изпълнителят да предостави на възложителя описание на всички настройки на операционната система, свързани със сигурностга на КСМГ?

Да. Операционната система (ОС), използвана в машините за гласуане е персонализирана версия на Windows, това се прави с цел да се избегнат потенциални заплахи за сигурността и деактивиране на компонентите, които не се използват по време на събитието (вкл. Wi-Fi, Bluetooth). Тази ОС ще има воден знак, изчислен от вътрешни файлове и регистри и всяка машина ще бъде в състояние да го покажете във всеки необходим момент, така че може да бъде проверен.

18.Възможно ли е изпълнителят да предостави доказателства на възложителя за това. че всички настройки на реално конфигурираните на КСМГ в момента на въвеждане и извеждане на КСМГ са еднакви?

Да. Всички конфигурируеми параметри на приложението за изборите се манипулират чрез един конфигурационен XML файл. Възможно е да се въведе процедура за сравнение хеша на този файл с версията на файла, инсталиран на всяка машина, по всяко време на изобирите.

Освен това, за да се гарантира, че инсталираните машини изпълняват автентичен софтуер, по време на изборите, по всяко време на процеса, предедателя на СИК може да изпълни процедура, която да генерира ключ, който да се сръвни и така да се гарантира, че софтуерът е автентичен.

кл. 2 от 33 АД

19.Възможно ли е изпълнителят да предостави на възложителя процедура за преглед на настройките на операционната система, свързани със сигурността?

Да. Възможно е да се постигне съгласие в рамките на процедура за възложителя да прегледате настройките на операционната система на машините..

20.Възможно ли е изпълнителят да предостави доказателства на възложителя за реализиран контрол на достъпа до ресурсите на операционната система, в съответствие с принципа на „необходимост да се знае"?

Да. Персонализираната ОС е конфигурирана по такъв начин, че обвивката на операционната система е контролирано приложение, което работи само за прилагането на изборите и изпълнява:

- Предоставяне на достатъчно време, за да основното приложение за да започне след операционната система и нейните услуги са заредени напълно
- Валидиране на автентичността на основното приложение работи в машината за гласуване. Основното приложение на машината за гласуване е цифрово подписан с цифров сертификат (X.509), който се издава от root CA (също X.509) вече инсталирани в операционната система.

21.Възможно ли е изпълнителят да предостави на възложителя процедура за създаване, забраняване и управляване на потребителски акаунт в КСМГ?

Да. Тъй като се използва персонализирана ОС възможни компоненти, които могат да бъдат атакувани се намаляват, в сравнение с пълната версия на операционната система. Само необходими от обвивката и изборните приложения средствата са оставени в операционната система, това означава, че потребителите се управляват от конфигурационните файлове на приложението на изборите.

22.Възможно ли е изпълнителят да предостави на възложителя процедура за управление на паролите за КСМГ?

Да. Паролите използвани във всяка машина могат да бъдат дефинирани

23.Възможно ли е изпълнителят да предостави на възложителя парола за достъп до настройките на BIOS на КСМГ?

Да, възможно е.

24.Възможно ли е изпълнителят да предостави доказателства па възложителя за това, че паролата на BIOS защитава от възможността за зареждане (boot) от други устройства, различни от твърдия диск на системата?

Да. Възможно е да се докаже, че BIOS включва конфигурация за сигурност, за да се предотврати промяна на реда зареждане. Машината винаги ще зарежда от вътрешния твърд диск, който е разположен във вътрешността в недостъпно техническо отделение, обезпечено с касова брава.

25.Възможно ли е изпълнителят да предостави на възложителя процедура за съхранение на одитните записи на операционната система в КСМГ?

Да. Дневникът на одит на машината включва всяко действие, което се извършва и е възможно да се експортне тази информация за целите на одита.

26.Възможно ли е изпълнителят да предостави на възложителя списък на събитията (одитни записи), които ще се генерират в КСМГ с цел последващ одит?

Да, Възможно е да се изпрати списък с всяко действие, който се съдържа в дневникът за одит.

27.Отговарят ли описаните в документите настройки, касаещи одитните записи на тези, които са конфигурирани в КСМГ?

Кои записи ще бъдат конфигурирани във машината преди началото на изборите, могат да бъдат съгласувани с възложителя.

28. Забранено ли е автоматичното презаписване на дневниците, съдържащи одntни записи?

Да. Забранено е да се презаписват лог файловете и върху тях никога не се записва.

29. Възможно ли е изпълнителят да предостави на възложителя процедура за проверка на одитните записи?

Да. Одитините логове могат да се проверят през КСМГ от потребител с необходимите оторизации. Може да се съгласува допълнителна процедура, съгласувано с възложителя, ако е необходимо.
30. Как се документира всяко нарушение на сигурността?

Всяко изменение на работещата операционна система и настройките на приложенията ще бъде маркирано от приложението за гласуване. Освен това, всеки опит да се променя всеки конфигурационен файл ще бъде невъзможно без притежаването на коректен декриптиращ ключ и сертификати за подписване.

31. Изготвя ли се одит на всички събития, свързани със специфичното софтуерно осигуряване?

Да. Лог-файла на КСМГ включва събития, които могат да засегнат сигурността на извършването на изборите.

32. Възможно ли е изпълнителят да предостави на възложителя процедура за защита от вредни програмни средства?

Да. Както е обяснено по-горе, софтуерът е защитен чрез наличието на персонализирана операционна система, с пълно контролиране на приложенията, работещи в кастамизирано обкръжение, даващо идентификация за жизнеността на операционната система и приложението за изборите, и BIOS е заключен, за да се предотврати промяна на неговото конфигуриране. Освен това, както също е обяснено по-горе, както и жизненоважните компоненти на хардуера на КСМГ са заключени, използват се ленти за сигурност, както и достъпа до машините се охранява.

КОНФИГУРАЦИОНЕН КОНТРОЛ

33. Възможно ли е изпълнителят да предостави на възложителя процедура за отразяване на актуалното състояние на конфигурациите на КСМГ, съобразена с добрите практики в областта?

Да. Възможно е да се предостави на възложителя доклад с конфигурацията на КСМГ. Важно е да се отбележи, че наборът от ISO сертификати на Smartmatic включва най-новата сертификация по ISO 27001 за управление на информационната сигурност, предвидена е специална сертификация „Осигуряване на хардуерни и софтуерни решения и напълно комплектувани услуги, улесняващи процеса на гласуване за свързани с правителството избори и общонационални, критични събития като регистрация на граждани и идентификация на граждани, електронно гласуване ". ISO одити на Smartmatic се извършват от DNV-GL, един от най-уважаваните сертифициращите органи по целия свят, със седалище в Норвегия.

34. Възможно ли е да бъде предоставен софтуерен инструмент от фирмата разработчик на софтуера, позволяващ да се генерират различни по своя обем и разпределение данни, доказващи коректността на изведените от КСМГ крайни резултати?

Възможно е да се предостави софтуерен инструмент за генериране на различни по обем и разпределение данни, за доказване на коректността на крайните резултати. Може да се ползват и отпечатаните гласувания. За да се генерира специален софтуер, ние ще трябва да имаме предвид наличното време за подготовката на изборния софтуер

За този и следващите отговори, ние може да включим по-подробни детайли, ако е необходимо и ако имаме достатъчно време.

ДЕЙСТВИЯ ПРИ КРИТИЧНИ СИТУАЦИИ

35. Възможно ли е изпълнителят да предостави на възложителя разработени в цялост процедури за действия в критични ситуации, в които в частност да са включени:

а/ процедура за архивиране на информацията и състоянието на КСМГ?

б/ процедура за реакция при хардуерен/софтуерен срив на КСМГ?

в/ процедура при наличие на компютърни вируси КСМГ?

При случай на инцидент, в който "машината за гласуване" спре да работи и има нужда от подмяна по всяко време от етапа на гласуване, цялата информация се прехвърля върху нова защитена и валидна "машина" предеарително заделена за целта.
USB устройството от машината имаща нужда от подмяна се прехвърля на новата доставена машина. Ще протече процес на кръстосана валидация използващ цифровите подписи на 2те устройства и ако те са валидни ще стартира репликация на данните и статуса от предишната машина.
Тази процедура протича минути и на края новата машина ще бъде точно копие на предишната, но включвайки

- Нов хардуерен номер (хардуерните номера са уникални за всяко устройство)
- Файл с лог, който записва събитието с репликацията между предишния и новия хардуерен номер на машините

Замяна на Памет:
Подобно на предишната процедура, ако USB паметта е повредена в някой момент от процеса, машината за гласуване ще покаже съобщение и ще се поиска стартиране на процедура за подмяна.

Нова USB памет, сертифицирана от доставчика и с валиден сертификат се вкарва в машината. След проверка по сигурността, информацията ще се дублира върху новата памет, осигурявайки по този начин че информацията и текущия статус на машината и външната памет са едни и същи
Както и при предишната процедура това събитие ще бъде отчетено в лог и хардуерния номер на USB паметта ще записан във лог файла и в пакета за прехвърляне
Тези процедури са базирани на сходството на информация между вътрешната и външната памет. Машината пази системни файлове с които доставя информация относно статуса, състоянието и данните и тези файлове се използват за възстановяване на същото състояние и условия на новата машина.

Ул. 2 от 53АД

ПРОЦЕДУРИ, ПОЗВОЛЯВАЩИ ЧАСТИЧНА ВЕРИФИКАЦИЯ НА ПРОЦЕСА НА ИЗПОЛЗВАНЕ НА КСМГ

36. Възможно ли е изпълнителят да предостави на възложителя процедура по изготвяне иа хеш подпис на твърдия диск на КСМГ и копие на твърдия диск при завършване на конфигурационните настройки, непосредствено преди експортиране към изборните райони?

Да. Имайте предвид, че на твърдия диск ще се съдържа хеш-таблица с всички критични файлове налични на твърдия диск. Тази таблица може да се експортира, но текущото приложение не включва тази функционалност, за да се облекчи процедурата. За да се генерира специален софтуер, ние ще трябва да имаме предвид наличното време за подготовката на изборния софтуер.

37. Възможно ли е изпълнителят да предостави иа възложителя процедура по изготвяне на хеш подпис на твърдия диск на КСМГ и копие на твърдия диск след приключване на изборния ден за всяка машина.

Да. Имайте предвид, че драйвера ще съдържа хеш-таблица с всички критични файлове налични на твърдия диск. Тази таблица може да се експортира, но текущото приложение не включва тази функционалност, за да се облекчи процедурата. Копие от файловете с резултати, както и файлове от гласуването е налично и във вградения твърд диск и на външната памет, което означава, че автоматично копие на тези важни файлове винаги ще се съхранява и ще е на разположение за целите на проверката и одита. За да се генерира специален софтуер, ние ще трябва да имаме предвид наличното време за подготовката на изборния софтуер.

38. Възможно ли е изпълнителят да предостави на възложителя процедура, позволяваща зареждане във виртуална и в реална среда на получените копия на твърди дискове с цел проверка коректността на машинното гласуване?

Като се има предвид прилаганите всеобхватни мерки за сигурност, за нас не е лесно да осигурим операционната система и приложението, работещи във виртуална среда. По отношение на проверката на коректност в реални условия, ние предлагаме да се предоставят на възложителя няколко КСМГ, както и сценарий позволяващ да се получат предвидими и следователно проверими резултати.

Чл. 2 от ЗЗЛД

39. Възможно ли е изпълнителят да предостави на възложителя процедура по предоставяне в ЦИК на копията на КСМГ и протоколите с изчислените хеш подписи?

Да, можем да предоставим на възложителя процедура по предоставяне в ЦИК на копията на КСМГ и протоколите с изчислените хеш подписи

Веселин Т... чл.2 от ЗЗЛД