**ПЛАН**

за провеждане на избори с използване на машинно гласуване

в изпълнение на чл. 213б от Изборния кодекс

Действия и мерки за сигурност, предприети от участниците в процеса на осигуряване на машинното гласуване

I. **Управление на криптографски ключове**:

1. Хеш код на системния софтуер – предоставя се от изпълнителя и се удостоверява от МЕУ.

2. Хеш код на приложния софтуер – предоставя се от изпълнителя и се удостоверява от МЕУ.

3. Хеш код, получен като резултат от довереното изграждане на изходния код, който се инсталира на СУЕМГ – съхранява се в ЦИК, като се генерира съвместно при довереното изграждане с участие на изпълнителя на дейностите за техническо осигуряване на машинното гласуване и представители на ЦИК, при използване на материалите от т. 1 и т. 2.

Хеш код на инсталирана СУЕМГ – видим е след инсталацията на СУЕМГ, посредством хеш екстрактор.

Размяната на криптографски ключове на програмния код се извършва на два етапа, като всеки от ключовете се предоставя от страните, които ги генерират, в запечатан плик.

**ІІ. Изграждане и инсталиране на системен и приложен софтуер на СУЕМГ**

Извършва се на три етапа, както следва:

1. Осъществяването на процедурата по доверено изграждане на изходния код при спазване на раздел I се извършва от изпълнителя под контрол на представители на ЦИК, в защитена среда, осигурена от МЕУ. Като резултат от довереното изграждане се генерират три пълни комплекта от изпълнимия софтуер, всеки от които се състои от четири флаш памети – за инсталиране, отключване, лог екстрактор и хеш екстрактор. Пълните комплекти се съхраняват от ЦИК.

2. След приключване на този процес изпълнителят получава инсталационни флаш памети. Инсталирането на генерирания при изпълнение на т. 1 инсталационен софтуер върху СУЕМГ се осъществява в съответствие с договора между ЦИК и изпълнителя.

3. Провизиране на СУЕМГ – извършва се от изпълнителя, като се осъществява предварителен и текущ контрол от страна на ЦИК.

**ІІІ. Зареждане на данни за съответния избор в СУЕМГ**

Централната избирателна комисия възлага на „Информационно обслужване“ АД издаването на цифрови сертификати за използване в СУЕМГ върху смарт карти, предоставени от ЦИК.

Смарт картите се предават от ЦИК на изпълнителя за параметризация на СУЕМГ, която се извършва от изпълнителя на дейностите за машинно гласуване.

**ІV. Съхранение и транспорт на СУЕМГ**

Специализираните устройства за електронно машинно гласуване се съхраняват в склад, чийто външен периметър се охранява денонощно от ГД „Жандармерия, специални операции и борба с тероризма“. С решения № 775 от 2021 г. и № 694 от 2022 г. на Министерския съвет на МВР е възложено да осъществява външната охрана на помещенията, в които се съхраняват СУЕМГ.

В склада има инсталирана алармена система и система за видеонаблюдение и запис.

Достъпът на лица в склада е възможен само след изрично писмено разпореждане на Централната избирателна комисия до ГД „Жандармерия, специални операции и борба с тероризма“. В склада се допускат само лица, за които е извършена съответната предварителна проверка от органите на МВР и ДАНС.

Относно транспортирането на СУЕМГ е създадена организация за непрекъснат съпровод и охрана от полицейски служители по време на:

- транспортиране на СУЕМГ от склада до определените места в областните центрове;

- претоварването в областните центрове и транспортирането на СУЕМГ до всяка избирателна секция;

- съхранението на СУЕМГ в СИК от момента на пристигане до тяхното предаване за обратно транспортиране;

- транспортиране на СУЕМГ от СИК до определените места в областните центрове;

- претоварването на СУЕМГ в областните центрове и транспортирането им до склада.