СЪЮЗ НА СЪДИИТЕ В БЪЛГАРИЯ

Член на Международната асоциация на съдиите (МАС)
Член на Европейската асоциация на съдиите (ЕАС)
Член на Европейски магистрати за демокрация и свободи (МЕДЕЛ)
София 1000, ул. Пиротска 7, ет.5, тел 0879686841
e:mail: office@judgesbg.org
web: http://www.judgesbg.org

До
Членовете на Съдийската колегия на
Висшия съдебен съвет (ВСС)

Уважаеми членове на Съдийската

колегия на Висшия съдебен съвет,

След въвеждането на Единната информационна система на съдилищата (ЕИСС) и запознаване с основните ѝ функции, съдиите, които работят с нея, откриват не само недостатъци в средата на работа (интерфейса) на системата, но и забелязват някои проблеми, които е възможно да се отразяват на сигурността ѝ. Разбира се, проверката за това не е от компетентността на юристи, а на програмисти и специалисти по киберсигурност. Въпреки това фактът, че в ЕИСС ще се обработват всички съдебни дела, някои от които засягат и въпроси за държавна тайна, а всички се отнасят в крайна сметка до правата на гражданите, е необходимо да се гарантира опазване на сигурността на данните – както липсата на недобронамерен или неоторизиран достъп до тях, така и с цел обезпечаване на работата на съдилищата.

Поради това е необходимо според нас да се извършват проверки на системата за сигурност, както вътрешно, така и от външни, независими специалисти, които да дадат още преди пълното въвеждане на системата, но и в хода на работата ѝ, оценка на рисковете, и да предложат насоки за повишаване на сигурността. Възприемаме като правилна стъпка това, че в чл. 14 от Договор за обществена поръчка № ВСС-495/16.01.2019 г. за въвеждане на системата е създадено задължение за работа с отворен код – т.е. за достъп до изходния код на програмата от широката общественост с цел анализ на недостатъците ѝ, както и това, че базата данни ще остане собственост на Висшия съдебен съвет. С това ще се избегнат спорове във

връзка с поддръжката на използвани в съдебната власт технологични продукти, каквито са възниквали в миналото, и са водели до необходимост от полагане на големи обеми труд за ръчна обработка на информация. Още повече, с оглед визията за електронно правосъдие, в бъдеще извън информационната система по някои дела няма да се поддържат архивни документи на хартия.

Въпреки тези положителни стъпки при възлагането на изработването на ЕИСС обаче възникват и някои въпроси, свързани с видимата част от компонентите на системата, с която съдиите и съдебните служители работят:

1. Използване на софтуерен код на трети лица

При работа с ЕИСС се установява, че документите се въвеждат в текстови редактор, който не е разработен от изпълнителя на договора за обществена поръчка за изработване на ЕИСС – „Информационно обслужване“ АД, а от друго лице. При работа с текст в системата ясно се показва, че текстообработването се извършва с помощта на програмата “Tiny” (https://www.tiny.cloud), която се разработва и поддържа от дружеството Tiny Technologies, Inc. със седалище в Калифорния, САЩ. Съгласно посоченото в страницата в интернет по-горе, софтуерът е лицензиран с отворен код, т.е. може да бъде използван и преработван и от други лица, вкл. „Информационно обслужване“ АД, но не става ясно как програмата е интегрирана в програмния код на системата ЕИСС и дали същата е изцяло под контрола на изпълнителя на договора за изработка на системата и дали изпраща данни на доставчика на външен софтуер. Последното може да се окаже проблемно с оглед чувствителността на информацията, с която се работи. Поради това тези въпроси също се нуждаят от проверка от независимо лице, което да установи дали не е възможно компрометиране на сигурността на ЕИСС.

2. Работа с електронни подписи

При работа със системата прави впечатление, че модулът за електронно подписване не работи с необходимата надеждност и се налага да се рестартира по няколко пъти на ден. Това освен притеснения за изгубеното време на съдиите води и до въпроси за надеждността на избраните средства за електронно подписване, което според нас също

следва да се провери преди пълното стартиране на ЕИСС във всички съдилища.

Съдии в страната освен това ни сигнализираха, че системата работи с квалифицирани електронни удостоверения за генериране на подпис, които освен данни на съда съдържат и чувствителни лични данни като единния граждански номер (ЕГН) на съдията. В този смисъл идентифицираме два проблема в нормативната база:

На първо място издадените на съдиите сертификати за електронен подпис не са ограничени до работата на съдилищата и законът им придава правно значение при подписване на всякакви документи (вкл. например частноправни договори на магистратите). С оглед необходимостта от многократно подписване на множество съдебни актове всеки ден нараства възможността за неправомерен достъп до частния ключ на сертификата, който генерира електронния подпис, и оттам – до възможност да се правят нерегламентирани изявления от името на съдията, които после не могат да бъдат оспорени при определени условия (чл. 18а, ал. 3 ЗЕДЕУУ). Поради това следва да се предприемат стъпки за това при създаване на служебни документи в законодателството да се предвиди въвеждане на електронен подпис, валиден само в служебно качество.

На второ място обстоятелството, че всеки съдебен акт се подписва с електронен подпис, съдържащ ЕГН на съдията, означава, че тези данни потенциално се разкриват на широк кръг лица. Затова искаме да се гарантира, че актовете, подписани с електронен подпис с ЕГН ще останат видими само за потребителите с достъп до системата, и то в рамките на един съд, а на гражданите ще се връчват удостоверени с положен автоматично в рамките на ЕИСС подпис, който удостоверява автентичността на получения от страната или институцията акт, но не съдържа чувствителни данни за издалия го съдия или съдебен служител (т.нар. „сървърен“ електронен подпис). Настояваме и с бързи изменения в нормативната уредба да се създаде възможност за удостоверяване на изявленията на съдиите по друг начин, който да не съдържа лични данни извън трите имена на съдията в публичната версия на подписания акт.

3. Информация за физическата сигурност на данните и позволяване на локално копиране на базата данни

Информацията, съхранявана от ЕИСС, макар и електронна, се пази във физическо хранилище (сървър). Настояваме да бъде посочено публично какви са процедурите за архивиране на тази информация през подходящи периоди от време при спазване на изискванията за опазване на защитената от закона тайна. Смятаме, че последната не би се нарушила, ако се съобщи колко копия на базата данни съществуват и под контрола на кои лица ще се пазят те, както и дали става въпрос за копия, достъпни онлайн, или такива, които периодично ще се съхраняват на изолирани от интернет устройства.

Смятаме за правилна стъпка частите от базата данни, които се отнасят до делата на един отделен съд да се копират периодично и на локален сървър на съда, където такъв е наличен, за да може работата на съда да не бъде затормозявана при евентуален срив на системата на друго място. Освен това смятаме за естествено всеки орган на съдебната власт да поддържа при себе си локално пълна база с данни за водените пред него или приключили наскоро дела.

4. Информационен одит

Намираме, че с оглед на това, че за пръв път в България се разработва и внедрява наведнъж система, която да работи с чувствителни данни за цял отрасъл на държавната власт, какъвто е правосъдието, следва да се проведе пълен независим одит на кода на ЕИСС от определени от ВСС външни специалисти, които да дадат отговор на поставените по-горе въпроси, а също така и:

– налице ли са при проверка на софтуерния код, работещ с базата данни, уязвимости, които сериозно компрометират сигурността;

– наблюдават ли се такива уязвимости в модулите на ЕИСС, чрез които системата работи с други регистри или информационни системи, както и с разработки на трети лица;

– подходяща ли е физическата инфраструктура за надеждна работа на системата,

като тези поне две независими едно от друго лица с добра професионална репутация да дадат и евентуални препоръки от направения одит за сигурност.

Във връзка с всичко изложено излагаме исканията се за проверка за сигурността на ЕИСС и защита на данните на работещите с нея съдии и съдебни служители:

1. Да се извърши одит на системата чрез достъпния отворен програмен код и евентуално описание на мерките за физическа защита и съхранение от поне двама независими професионалисти, които да идентифицират проблеми в сигурността и да дадат препоръки за отстраняването им, ако има такива.

2. Да се провери дали се изпълнява задължението кодът на системата да е отворен и необременен с права на трети лица.

3. Да се гарантира, че данните от съдебните дела не се прехвърлят на компютърни системи на трети лица.

4. Всички публично достъпни електронни копия на съдебни актове да бъдат издавани от ЕИСС само по начин, че да не съдържат електронен подпис, съдържащ чувствителни лични данни на съдии или съдебни служители.

5. Да се гарантира, че всеки съд ще има резервно копие от базата данни на всички водени пред него дела, за да може да я възстановява при нужда.

6. Да се посочат мерките за ефективно физическо съхраняване на базата данни, включително периодични копия на носители без достъп до интернет, за да се гарантира запазването на съдебните дела и актове.

Намираме, че изброените действия трябва да се извършат преди пълното въвеждане на ЕИСС в съдилищата в страната, за да се създаде у гражданите и магистратите доверие в сигурността на системата, с която ще се осъществява правосъдната дейност в цялата страна.

гр. София
2 октомври 2020 г.

Управителен съвет на
Съюза на съдиите в България