Р Е П У Б Л И К А Б Ъ Л Г А Р И Я
МИНИСТЕРСТВО НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ

ОТЧЕТ ЗА СЪСТОЯНИЕТО И ГОДИШЕН ПЛАН ЗА РАЗВИТИЕ И ОБНОВЯВАНЕ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ В АДМИНИСТРАЦИЯТА И ИНФОРМАЦИОННИТЕ РЕСУРСИ НА ЕДИННАТА ЕЛЕКТРОННА СЪОБЩИТЕЛНА МРЕЖА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ И ЗА НУЖДИТЕ НА НАЦИОНАЛНАТА СИГУРНОСТ

март 2022 г.

СЪДЪРЖАНИЕ

СЪКРАЩЕНИЯ

CERT	Национален център за действие при инциденти в информационната сигурност
ENISA	Агенцията на Европейския съюз за мрежова и информационна сигурност
SSO	Single sign on
АИС	Автоматизирана информационна система
АОП	Агенция по обществени поръчки
АР	Административен регистър (поддържан от ИИСДА)
ВСС	Висш съдебен съвет
ГКПП	Граничен контролно-пропускателен пункт
ДАБДП	Държавна агенция „Безопасност на движението по пътищата“
ДАЕУ	Държавна агенция „Електронно управление“
ДАНИИ	Държавна агенция за научни изследвания и иновации
ДХЧО	Държавен хибриден частен облак
ЕАУ	Електронни административни услуги
ЕЕСМ	Единна електронна съобщителна мрежа
ЕПДЕАУ	Единен портал за достъп до електронни административни услуги
ЕПИР	Единна политика за информационните ресурси на електронното управление на Република България
Е-управление	Електронно управление
ЗЕИ	Закон за електронната идентификация (ЗЕИ)
ЗЕУ	Закон за електронното управление
ЗКС	Закон за киберсигурност
ИАГ	Изпълнителна агенция по горите
ИАРА	Изпълнителна агенция по рибарство и аквакултури
ИИСДА	Интегрирана информационна система на държавната администрация (Административен регистър)
ИКТ	Информационни и комуникационни технологии
ИР	Информационни ресурси
ИСБК	Информационна система за извършване на предварителен, текущ и последващ контрол по целесъобразност в областта на електронното управление и използването на информационните и комуникационните технологии
ИСУН	Информационна система за управление и наблюдение на средствата от ЕС в България
КЕП	квалифициран електронен подпис
КИН	клиентски идентификационен номер
КПКОНПИ	Комисия за противодействие на корупцията и за отнемане на незаконно придобитото имущество
МЗ	Министерство на здравеопазването
МИС	мрежова и информационна сигурност
МРРБ	Министерство на регионалното развитие и благоустройството
МС	Министерски съвет
МТИТС	Министерство на транспорта, информационните технологии и съобщенията
МФ	Министерство на финансите

НАП	Националната агенция за приходите
НАЦИД	Национален център за информация и документация
НЗОК	Националната здравноосигурителна каса
НМИМИС	Наредба за минималните изисквания за мрежова и информационна сигурност
НОИ	Национален осигурителен институт
НОИИСРЕАУ	Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги
НПР	Национална програма за развитие
ОА	Областна администрация
ОЦД	Основен център за данни
ПИК	персонални идентификационни кодове
РМС	Решение на Министерски съвет
СЕОС	Среда за електронен обмен на съобщения
СОСП	Съобщителен обект със специално предназначение
ССЕВ	Система за сигурно електронно връчване
УКД	уникален код за достъп
ЦВПОС	Централен виртуален ПОС терминал

I. ВЪВЕДЕНИЕ

Настоящият отчет представя информация относно състоянието на информационните ресурси (ИР) в администрациите за периода 01.01.2021 – 31.12.2021 г. Този период съвпада с продължаващото действие на редица мерки и ограничения, породени от пандемията от COVID-19. През 2021 г. трайно се установи практиката за взаимодействие в дистанционна среда и за работа от разстояние, което доведе до нарастване на очакванията и изискванията на гражданите и бизнеса за устойчиво и надеждно е-управление, гарантиращо им ефективни електронни услуги (е-услуги) и защита на техните данни и трансакции в електронна среда. В тази връзка, състоянието на ИР в държавната администрация, както и гарантирането на оптималното функциониране на ключови системи и ИТ-инфраструктурата, които да издържат на критично натоварване, е по-важно от всякога.

Към администрациите са поставени високи изисквания за осигуряване на административното обслужване в електронна среда и за ефективен достъп и защитен обмен на данни и информация при гарантиране на откритост, прозрачност и достъпност. Развитието на информационните технологии и ускоряването на цифровата трансформация следва да се осъществява при минимизиране на рисковете и оптимизиране на разходите, което поражда и редица предизвикателства – както нормативни, така и свързани с текущото състояние на ключови системи и услуги, и тяхната защита.

Същевременно политиката по отношение на ИР следва да се развива като обхване актуалните тенденции и насоки в е-управлението, цифровизацията на данни и процеси, информационните технологии и като цяло дигитализацията на публичния сектор, където акцентът се поставя върху три основни плоскости:

1. Потребителят е в центъра на процесите и с основен фокус при дизайна на услугите.

2. Нарастване на ролята на новите технологии в управлението, включително облачни и базирани на изкуствен интелект и поставяне на фокус върху данните като ключов капитал.

3. Киберсигурността, включително сигурността и защитата на системите и мрежите в публичния сектор.

II. СТРАТЕГИЧЕСКА РАМКА ЗА РАЗВИТИЕ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ

1. Стратегия за развитие на електронното управление в Република България 2019 – 2025 г.

Стратегията за развитие на електронното управление в Република България 2019 – 2025 г. (приета с Решение № 298 на МС от 2 април 2021 г.) очертава визията за развитие на електронното управление в Република България за постигане на необратима цифрова трансформация в публичния сектор, основана на:

- трансформация на модела на предоставяне на електронни административни услуги (ЕАУ), ориентирани към потребителя чрез промяна на технологичните и административни процеси, които стоят зад тях, с резултат намаляване на административната тежест за гражданите и за бизнеса;
- цифрова трансформация на публичния сектор, основана на данни;
- изграждане на модерна цифрова администрация, включително внедряване на онлайн инструменти за гражданско участие;
- високо ниво на мрежова и информационна сигурност (МИС);
- високо качество на поддръжка на споделените ресурси на е-управлението.

Визията и инициативите на европейско ниво определят нов цялостен подход към „икономика на данни“, който има за цел да увеличи търсенето и използването на цифрови данни и базираните на тях услуги, продукти и процеси в рамките на Единния европейски пазар. Съгласно Европейската стратегия за данните[1], с хоризонт до 2025 г., се предвижда създаването на Единно европейско пространство на данните и прилагането на нови модели за събиране, обработка, използване и повторни използване, съхранение и сигурност на данните.

В унисон с новите международни тенденции, в рамките на отчетния период, през месец март 2021 г. Стратегията за развитие на електронното управление е актуализирана с времеви хоризонт до 2025 г.[2], отчитайки целите и принципите, заложени в редица новоприети стратегически документи на национално и европейско ниво от значение за развитието на електронното управление и в частност ИР.

През месеците август-декември 2021 г. е извършена независима междинна оценка на изпълнението на Стратегия за развитие на електронното управление в Република България. В резултат на оценката, като ключова препоръка е очертано изготвянето на нов стратегически документ за развитие на електронното управление, информационните технологии и информационното общество с хоризонт на действие 2030 г. и включването на нови механизми за наблюдение и оценка на изпълнението на целите и дейностите в него.

2. Архитектура на електронното управление

Планирането, поддържането и развитието на ИР в администрациите, като градивен елемент и основен технологичен компонент на е-управлението, следва национална Архитектура на електронното управление (Архитектурата), която е ключова част от изпълнението на политиката за е-управление и предоставя общата рамка на взаимодействие между участниците в е-управлението.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066
[2] Решение № 298 на Министерския съвет от 2 април 2021 г.

Архитектурата определя елементите на е-управление от функционална, системна и технологична гледна точка. По отношение на ИР реализацията на Архитектурата е подчинена на подхода за:

- прилагане на единен модел за заявяване, заплащане и предоставяне на електронни административни услуги (ЕАУ), който стои зад всяка електронна административна услуга;
- преход от фрагментирани и затворени към цялостни и технологично независими решения;
- поетапна промяна на модела на съхранение на данните от децентрализиран към централизиран такъв, като се започва с най-критичните за електронното управление масиви от данни;
- изграждане и развитие на споделени информационни ресурси и предоставянето им за децентрализирано управление и използване.

Към момента Архитектурата е фокусирана основно по отношение на унифициране и подобряване на качеството на предоставяните ЕАУ от администрациите. Поради различни причини се забавят мерките, свързани с изграждането на цялостни и технологично независими решения, с промяна на модела на съхранение на данните и с надграждането на споделените информационни ресурси, които мерки съвкупно ще доведат до пълното дигитализиране и изграждане на процесите в администрацията и публичния сектор, като цяло.

В допълнение Архитектурата на електронното управление е във версия от 2019 г. Предвид динамиката в развитието на технологиите и процесите, особено видна след настъпването на пандемията от COVID-19, както и актуализираната стратегическа и нормативна рамка, е наложително Архитектурата да бъде своевременно актуализирана и разширена.

Друг съществен проблем е, че са изминали почти три години от одобряването на националната Архитектура и все още липсват разработени и приети архитектури по области на политики, които да описват функционалните, системни и технологични елементи на е-управлението в съответните сектори и взаимовръзките с останалите сектори на държавно управление. Този дефицит е необходимо да бъде адекватно адресиран през 2022 г.

3. Единна политика за информационните ресурси

С РМС № 296/02.04.2021 е приета Единна политика за информационните ресурси на електронното управление на Република България (ЕПИР), разработена на основание чл. 7в, т. 5 от Закона за електронното управление (ЗЕУ)[3].

Документът описва принципи, общи насоки, мерки и действия за разработването на единна политика за развитие на ИР, като информационна и технологична екосистема, която да се характеризира с балансираност, самостоятелност, разширяемост и устойчивост.

Изключителната динамика в развитието на ИКТ, институционализирането на политиката за е-управление, информационни технологии и информационно общество, както и напредъкът по приоритетите и инициативите за цифрова трансформация в национален и международен план налагат разработването на самата политика за развитие на информационните ресурси. Тя следва да бъде съобразена и допълнена със съответните правила, стандарти и процедури за развитие и управление на ИР, както и да бъдат разработени методически указания към администрациите по изпълнението ѝ.

[3] Публикувана на адрес https://e-gov.bg/wps/portal/agency/strategies-policies/e-management/strategic-documents/strategic-documents

4. Основни източници на информация за състоянието на информационните ресурси

За целите на този отчет, освен наличните данни за функционирането на хоризонталните и централизирани системи на е-управление, е използвана информация и от Интегрираната информационна система на държавната администрация (ИИСДА), Регистъра на информационните ресурси (РИР) и въпросници, публикувани на уеб страницата на Държавна агенция „Електронно управление“ (ДАЕУ)[4].

Основното предназначение на ИИСДА е да предоставя стандартизирана информация, която трябва да е проследима във времето, лесно модифицируема и в съответствие с провежданите политики и промените в нормативната уредба. ИИСДА е единен източник на информация за ръководителите на администрации и техните функции, организацията на работа, предоставяните административни услуги, човешките ресурси и състоянието на държавната администрация.

РИР се води и поддържа съгласно ЗЕУ и съдържа информация за:

- информационните ресурси, с които разполагат административните органи, с изключение на тези, чието предназначение е за работа и съхранение на класифицирана информация;
- информационните ресурси на Единната електронна съобщителна мрежа (ЕЕСМ) на държавната администрация и за нуждите на националната сигурност;
- годишни планове за обновяване на ИР на администрациите.

Регистърът се поддържа като електронна информационна система, в която служители, определени от административния орган, вписват информацията. Служителите отговарят за достоверността на въвежданата информация, както и за навременното ѝ въвеждане.

За целите на този отчет са подготвени и въпросници, които бяха попълнени от администрациите с цел получаването на допълнителна информация, която би допълнила другите източници[5] с оглед установени пропуски и трудности при валидиране достоверността на данните.

[5] Въпросниците са публикувани в секция „Открито управление“ на уеб сайта на ДАЕУ: https://e-gov.bg/wps/portal/agency/about-us/open-management

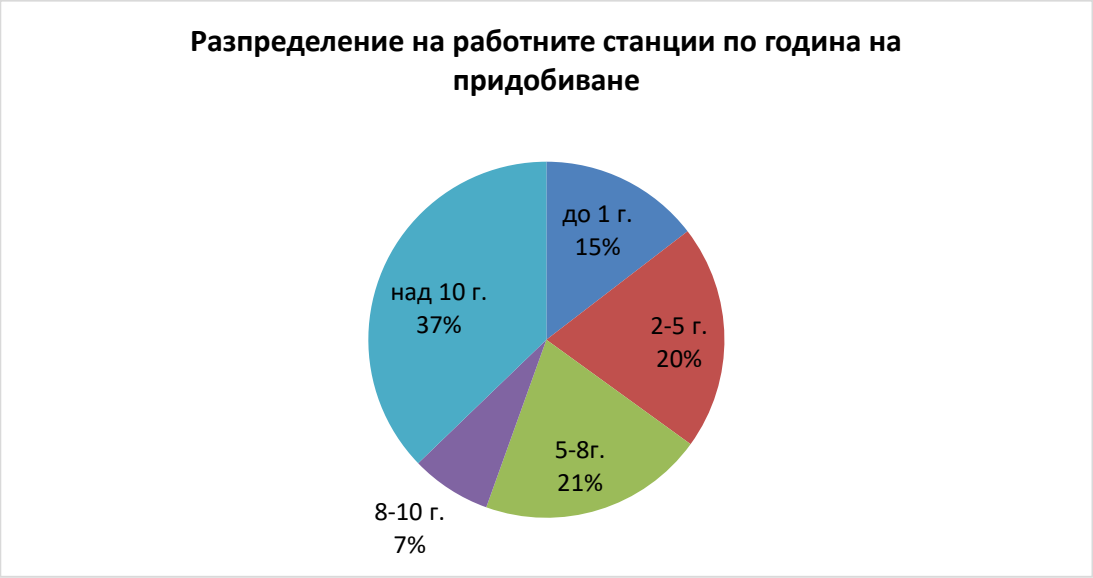
III. СЪСТОЯНИЕ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ В АДМИНИСТРАЦИЯТА

Съгласно чл. 55, ал. 1 от Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги (НОИИСРЕАУ), информационни ресурси са:

- хардуер, в т.ч. сървъри, настолни и мобилни компютри и устройства;
- мрежово оборудване;
- софтуер;
- софтуерни лицензи.

1. Обезпеченост на администрациите с хардуер

Към 31.12.2021 г. администрациите разполагат със 108 382 бр. работни станции, (спрямо 93 358 бр. към 31.12 2020 г.), като от тях 65% са в централната администрация и 35% - в териториалната администрация. Данните в РИР показват, че 37% от работните станции са придобити преди повече от 10 г., а 21% са на възраст между 5 и 8 г. Тоест, повече от половината от работните станции в администрацията са на възраст над 5 години, като е отчетено минимално намаление спрямо предходната година. Това създава сериозни рискове пред ефективността на администрацията, както и затруднява работните процеси и работата с информационните системи в нея. Административните органи следва да планират ресурс за поетапното обновяване на работните станции след пълната им амортизация и извеждане от експлоатация, приоритетно на тези, които са над 10 г.



Фигура 1. Разпределение на работните станции по година на придобиване

Разпределението на останалите видове активи, въведени в РИР е следното:

Вид активи	Брой	Стойност на актива в лв. (към момента на придобиване)
Сървъри	4 589	61 407 796.98
Масиви за данни	1 030	1 635 722.72

Вид активи	Брой	Стойност на актива в лв. (към момента на придобиване)
Периферни устройства	12 1294	86 564 396.91
Запаметяващи устройства	1 135	7 785 448.32
Поддържащи системи	9 631	20 177 518.88
Шкафове	1 640	8 938 682.64
Мрежови устройства	13 549	37 633 278.97
Компютърни мрежи	787	117 612 917.61

Таблица 1. *Въведени активи в РИР*

За отчетния период, въведените в РИР данни показват промяна в обема на видовете хардуерни активи, като по-съществено увеличение се наблюдава при масивите за данни, мрежовите устройства и работните станции.

Продължава тенденцията при използваните от административните органи работни станции, сървъри и мрежови устройства да се наблюдава голямо разнообразие от производители. От друга страна, на този етап липсва общонационален стандарт за вид и тип хардуер, който следва да се използва за изпълнението на едни и същи функции и дейности в различните администрации. Това обстоятелство поражда риск от увеличаване на разходите за поддръжката им и намаляване на ефикасността. Основна причина за това е липсата на конкретно дефинирана политика за информационните ресурси.

2. Обезпеченост на администрациите със софтуер и лицензи

От наличните в РИР данни за операционни системи на работни станции е видно, че над 30% от тях са с остарели версии, които вече не се поддържат от основния доставчик Microsoft, като се наблюдава леко понижение на тази стойност в сравнение с миналия отчетен период – 36,78% .

Неподдържаните версии на софтуер крият сериозен риск за информационната сигурност. От подобен дефицит страдат най-вече общините, които разполагат с ограничен финансов ресурс.

Според данните от РИР в администрациите се използват различни по вид системи за управление на бази данни. Поради липса на задължително поле за посочване на предназначение на софтуера, не може да бъде извлечена справка, която да даде достоверни данни за използваните системи за управление на база данни (СУБД) в администрацията.

От инсталираните на сървърите в администрациите операционни системи преобладават различни версии на MS Windows Server и MS Exchange Server.

По отношение на антивирусния софтуер, към момента на разработването на отчета в РИР липсва задължително поле за посочване на предназначение на софтуера, поради което не може да бъде извлечена справка, която да даде достоверни данни за използвания антивирусен софтуер в администрацията. Предвид това, данните относно използвания антивирусен софтуер се базират само на отговорите от разпратените до административните

органи въпросници. Според наличната информация, най-използвани от администрациите са антивирусните решения на ЕСЕТ, както и безплатен софтуер.

ESET Antivirus	Panda Antivirus	F-Secure Business	Kaspersky Antivirus	Symantec Antivirus	Друг платен антивирусен софтуер	Безплатен антивирусен софтуер
37,52%	7,47%	6,36%	5,72%	4,77%	6,84%	31,32%
236	**47**	**40**	**36**	**30**	**43**	**197**

Таблица 2. *Разпределение на антивирусния софтуер*

Аналогично, данните относно платформите за виртуализация не могат да бъдат извлечени от РИР, поради което отново се базират само на отговорите във въпросниците.

Платформи за виртуализация	Териториална администрация	Централна администрация
Microsoft Hyper-V %	45.69	42.86
VM Ware %	32.59	45.26
Друга платформа %	21.73	11.88

Таблица 3. *Платформи за виртуализация, по вид администрации*

	Microsoft Hyper-V	VM Ware	Друга платформа	Общо
брой	429	409	148	986
%	43.51	41.48	15.01	

Таблица 4. *Платформи за виртуализация, общо*

Данните от попълнените въпросници потвърждават, че преобладаващата платформа за виртуализация, използвана в администрациите към 31.12.2021 г., е Microsoft Hyper –V. Следва да се отчете, че по-голяма част от централната администрация използва решения на VM Ware.

3. Информационни системи

От гледна точка на ресурсите на е-управление информационните системи са: системи на е-управление – хоризонтални и централизирани - и системи на администрациите.

За отчетния период продължава процесът по интегрирането на информационните системи на администрациите с хоризонталните и централизираните системи на електронното управление.

3.1. Хоризонтални системи на електронното управление

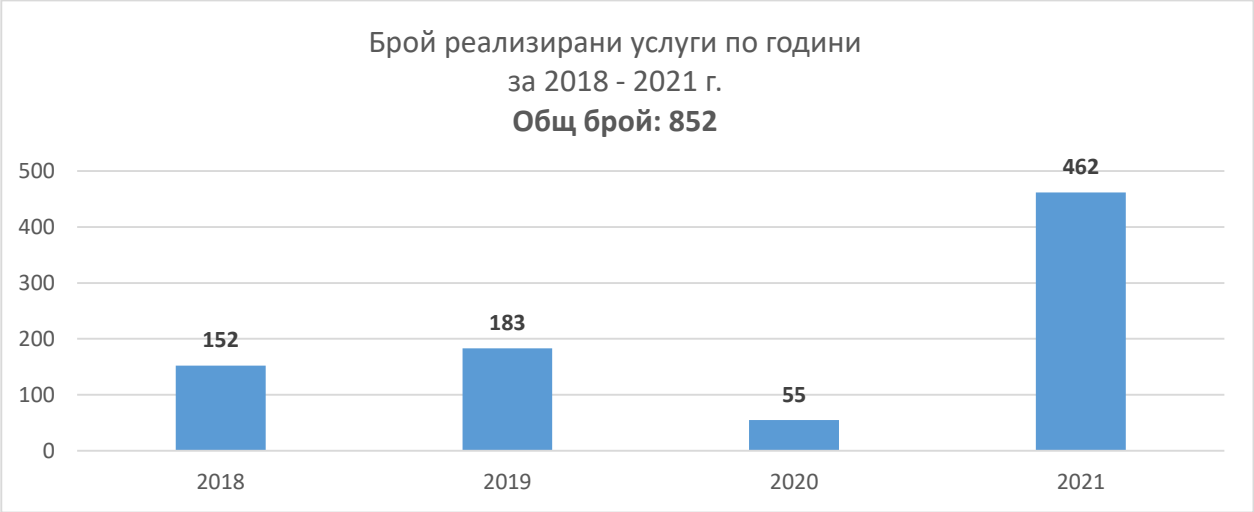
Следните хоризонтални системи са основните градивни елементи на е-управление:

- **Единен портал за достъп до електронни административни услуги (ЕПДЕАУ, egov.bg)**

Единният портал е реализиран като единна точка за достъп до ЕАУ. Към 31.12.2021 г. е публикувана информация за 1 329 услуги, от тях 852 ЕАУ са реализирани чрез централизирано и унифицирано заявяване. За заявяването им са разработени над 1 100 електронни форми на услугите и съпътстващите документи.

През 2021 година са реализирани 462 нови ЕАУ за централизирано заявяване – над 8 пъти повече, в сравнение с 2020 г. Към момента на изготвянето на отчета услугите се предоставят централизирано от 480 администрации, от които 33 са централни, 300 на общинско ниво (общини и техните райони), 28 областни и 120 специализирани териториални структури.

През 2021 година е публикувана информация за 477 ЕАУ, предоставяни децентрализирано от Министерство на вътрешните работи (МВР), Национален осигурителен институт (НОИ), Агенция по геодезия, картография и кадастър (АГКК), Агенция Митници, Национален център за информация и документация (НАЦИД) и др. чрез разработени портали на администрациите.



Фигура 2. *Брой разработени услуги по години*

За отчетния период присъединените административни структури към Единния модел на заявяване са над 2 пъти повече в сравнение с предходната година - 297, от които 163 са на общинско ниво, 14 са централни и 120 са специализирани териториални администрации.

Фигура 3. *Брой присъединени към Единния модел администрации по години*

Към края на 2021 г. са присъединени всички областни администрации, като централизирано се предоставят 21 техни услуги, както и всички общински администрации, като централизирано се предоставят всички техни услуги.

През 2021 г. са реализирани федерирани портали за 25 администрации – НАП, Изпълнителна агенция по рибарство и аквакултури (ИАРА), 5 областни администрации – Кюстендил, Монтана, Добрич, Русе и Шумен и 18 общини.

- **Система за електронна автентикация (е-Автентикация)**

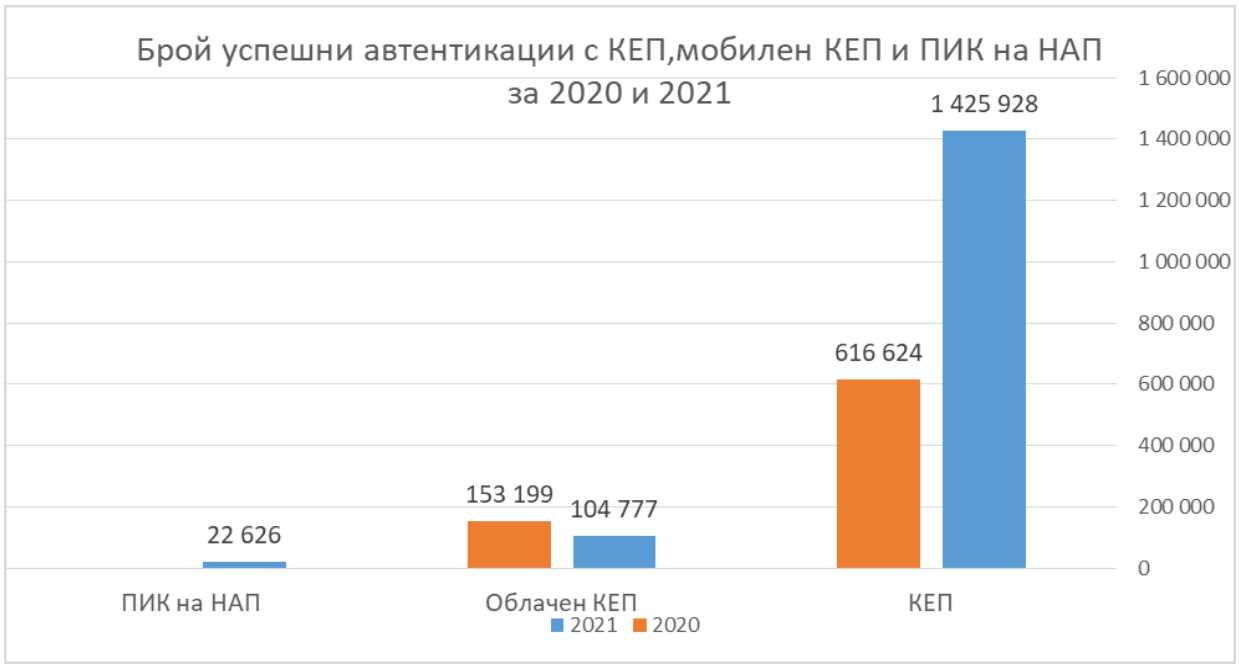
Системата за е-Автентикация (във версия еАвт 2.0) реализира процеса, свързан с еднократната идентификация и автентикация (удостоверяване на самоличността) на потребители пред системи, които го изискват. Тя предоставя унифициран интерфейс за интеграция на доставчици на електронна идентификация, стандартизиран в документ „Модел на интеграция с хоризонтална система за е-Автентикация“[6].

С еднократна интеграция на система е възможно потребител да се автентикира с всяко средство за идентификация, предоставяно от интегрираните с еАвт 2.0 доставчици на идентификация, както и обратното, при интеграция на доставчик на идентификация чрез предоставяното от него средство могат да се автентикират потребители пред всички интегрирани с еАвт 2.0 системи.

Общият брой успешни автентикации за 2021 г. през системата еАвт е: 1 553 331 бр. (за еАвт версия 1.0 – 447 038 бр., за еАвт версия 2.0 – 1 106 293 бр.).

През 2021 г. само за еАвт 2.0 регистрираните успешни автентикации чрез КЕП са 1 035 045 бр., с мобилен КЕП – 48 622 бр. и чрез ПИК на НАП - 22 626 бр., от които 980 875 са нови уникални потребители. За сравнение с предходния отчетен период – автентикациите чрез КЕП са 616 624 бр., а с мобилен – 153 199 бр.

[6] Моделът за интеграция с хоризонтална система за електронна автентикация е публикуван на сайта на агенцията на следния електронен адрес: https://e-gov.bg/wps/portal/agency/systems/info-systems/e-authentication



Фигура 4. *Статистика за успешно автентикирани потребители със средства, поддържани от системата*

Посредством системата е реализиран методът Single sign on (SSO) или еднократна идентификация за удостоверяване, който позволява на потребителите сигурно да се удостоверяват пред множество приложения и уебсайтове, като използват само един набор от идентификационни данни, предоставяни от еАвт 2.0.

През годината са разработени модели за използване на двуфакторна автентикация към всяко от интегрираните средства за идентификация (КЕП+двуфакторна автентикация, ПИК+двуфакторна автентикация).

На фигурата по-долу са представени администрациите, чиито информационни системи и портали са интегрирани към еАвт 2.0 и техния дял при формиране на потребителски сесии.

Фигура 5. *Интегрирани системи на доставчици на услуги към системата еАвт 2.0*

- **Система за електронно плащане (е-Плащане)**

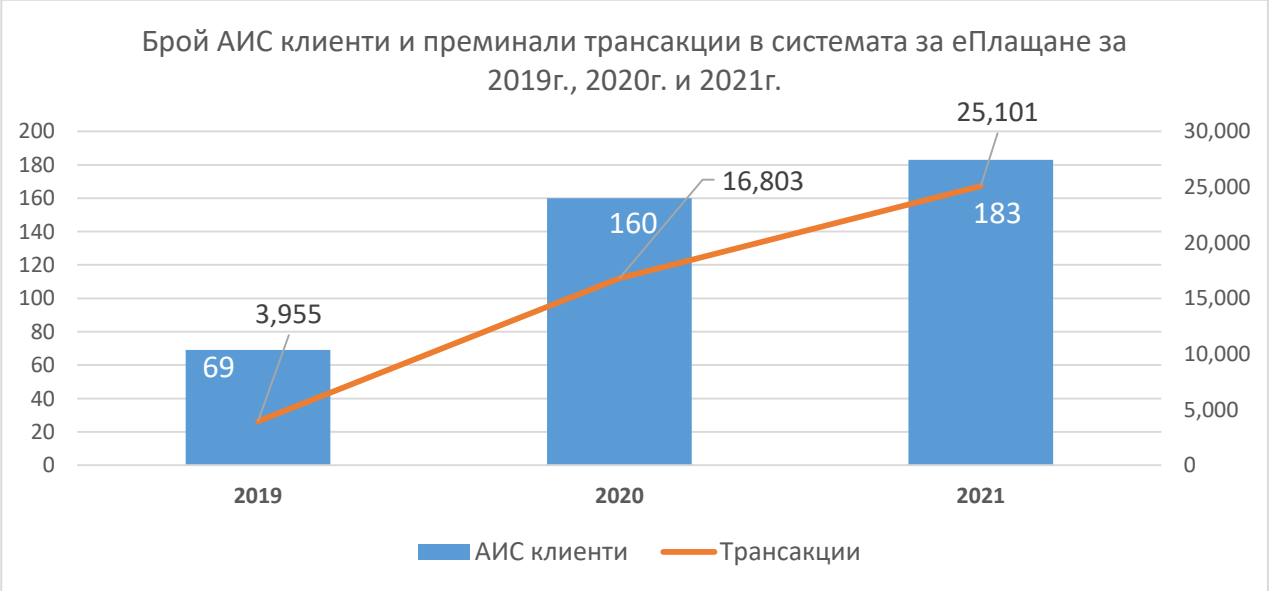
Системата предоставя възможност на задължените лица да заплатят своите задължения чрез кредитна или дебитна карта, чрез ePay или на гише в банков клон с платежно нареждане,

както и с предоставен код за достъп. С надградените нови функционалности на системата през 2021 г. се предоставя още един канал за плащане - т. нар. Централен виртуален ПОС (ЦВПОС) терминал. При този метод на плащане могат да се заплатят едно или няколко задължения с една трансакция, като не се дължат преводни такси и комисионни от гражданите.

През 2021 г. са присъединени 183 АИС клиента, вкл. 172 са присъединени към ЦВПОС Общият брой на присъединените АИС клиенти е 432.

Фигура 6. *Брой АИС клиенти в системата за е-Плащане*

Извършените трансакции за 2021 г. са 25 101 бр., като същите данни за 2020 г. са съответно 160 присъединени АИС клиенти и 16 803 трансакции (съгласно фиг. 7).



Фигура 7. *Статистика за присъединени АИС клиенти на администрации и преминали трансакции в системата за е-Плащане*

През 2021 г. се констатира увеличаване на броя на присъединените администрации спрямо предходната година. Към системата са новоприсъединени общо 386 броя администрации – 30 централни администрации, 243 общини и районни администрации и 113

териториални администрации. Най- висок е делът на присъединени участници- общински администрации – 81%. Една администрация може да има повече от един АИС клиент, присъединен към системата за е-Плащане.

През следващата година усилията ще бъдат насочени към присъединяване на структури на централната администрация, с акцент върху доставчици на ЕАУ от ниво 4, както и към присъединяване към системата на останалите банки – доставчици за платежни услуги.

- **Система за проверка валидността на персонален цифров сертификат (е-Валидиране)**

Системата е средство за проверка и потвърждаване на валидността на квалифициран електронен подпис, удостоверение за време (time stamp), електронно подписан документ в реално време, както и възможност за разпечатване на електронен документ, преобразуване на съдържанието на документ на хартиен носител в електронна форма.

Към системата са добавени 710 удостоверителни (Root) сертификата от доверителния списък, администриран от Европейската комисия относно валидиране на електронен подпис.

Системата е интегрирана със Системата за сигурно електронно връчване, като за отчетния период е проверена валидността на 8 420 персонални цифрови сертификата.

- **Система за управление на електронни форми (е-Форми)**

Системата за управление на електронни форми (е-Форми) предоставя възможност за избор на услуга и автоматизиране на последващите процеси на взаимодействие между заявител и доставчик при предоставяне на заявената услуга. Системата позволява достъп на автентикирани вече потребители до списък от ЕАУ и попълване на съответната електронна форма, и подаване към административния орган, изпълнител на услугата.

През прототипа на системата за електронни форми се предоставят за централизирано заявяване 835 ЕАУ. Формите са разработени по стандарт с цел унифициране на формуляри. От създаването на прототипа на системата в края на 2018 г. статистика на заявените ЕАУ по години е представена на фиг. 8.

Фигура 8. *Брой заявявания на ЕАУ по години*

- **Система за сигурно електронно връчване (ССЕВ, е-Връчване)**

През 2021 г. чрез надграждане на системата са осигурени:

- сигурност на съобщения и документи – всяко съобщение и документ се криптират с уникален симетричен ключ, като се генерира и асоциира и уникален асиметричен ключ за всеки потребител на системата; нови механизми за сигурно генериране, съхранение и контрол на достъп до ключове с поддръжка на HSM; интеграция със системата за проверка против наличие на зловреден код;

- шаблони на съобщения – възможност за създаване на шаблони на съобщения, включително фиксиране на задължителни полета и формат на съдържащата се в тях информация, асоцииране на метаданни и определяне на видове документи, прилагани към шаблона; във всеки шаблон е заложена възможност за автоматично извличане и визуализиране в полета от шаблона на информация от официални регистри и бази данни;

- хранилище за документи – оптимизирано и сигурно съхранение (чрез използване на криптографски методи) на документи; интуитивни потребителски интерфейси за управление на документите;

- управление на групи и права;

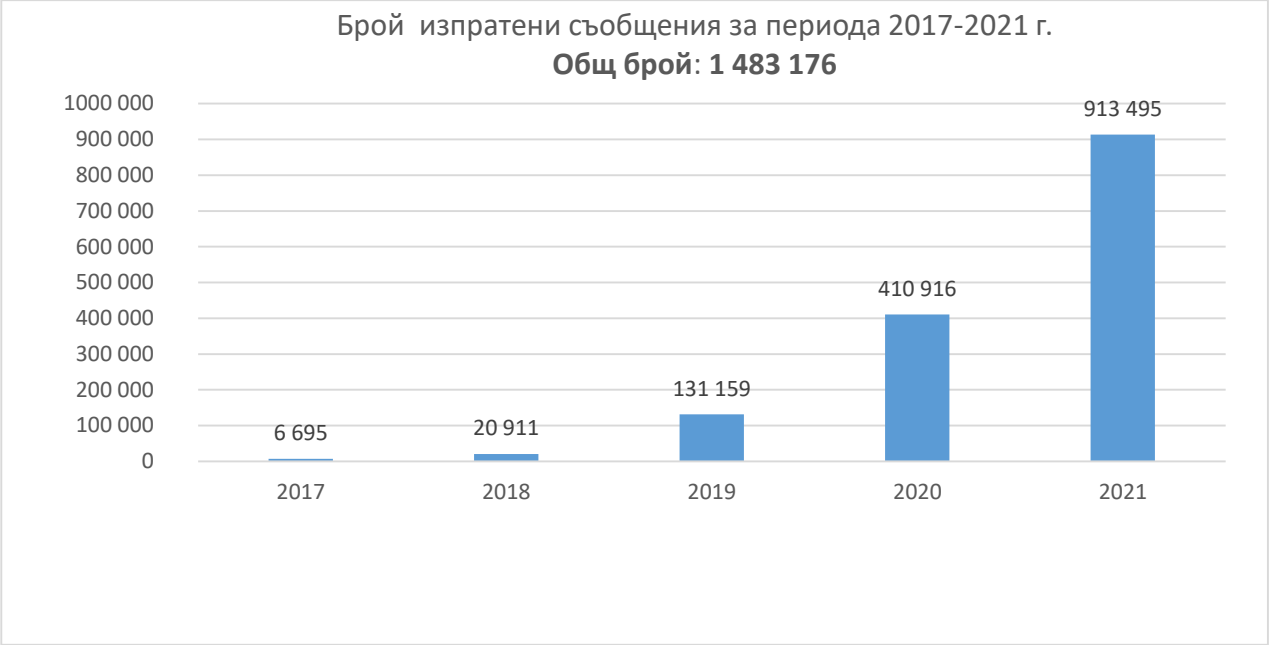
- нова версия на протокола за Системата за електронен обмен на съобщения (СЕОС), използваща международно утвърдения AS4 протокол като транспортен протокол за обмен на съобщенията.

С цел повишаване на сигурността и отказоустойчивостта на системата бяха надградени хардуерните и мрежови компоненти от инфраструктурата на Държавния хибриден частен облак (ДХЧО), на която е разположен ССЕВ.

Към 31.12.2021 г. в ССЕВ регистрираните потребители са 162 302 броя, от които 2 067 административни органи; 8 183 лица, предоставящи обществени услуги и изпълняващи публични функции; 144 253 са физически лица както и 7 809 юридически лица. Справка за броя на новорегистрирани потребители в ССЕВ по години е представена на графиката.

Фигура 9. *Брой регистрираните потребители в ССЕВ по години*

Обменените съобщения чрез ССЕВ към момента на изготвянето на отчета са общо 1 483 176. Справка за обменените съобщения по години е представена на следващата графика.



Фигура 10. *Справка за обменените съобщения по години*

От стартирането на системата през 2017 година, интегрираните със ССЕВ информационни системи на административни структури са общо 265, от които за 2021 в продукционна среда са 72 – 59 на администрации, 10 на лица по чл.1 ал. 2 и 3 на юридически лица).

3.2. Централизирани системи за е-управление

Централизираните системи са предназначени да подпомагат администрациите в процеса по подобряване на качеството на обслужването на гражданите и бизнеса. В голямата си част те позволяват с една инсталация на системата да работят множество администрации (multi-tenant решения). На този етап функционират следните централизирани системи:

- **Среда за междурегистров обмен на данни RegiX**

През 2021 година продължават усилията за разширяване на възможностите за служебен обмен на данни чрез вътрешни електронни административни услуги (ВЕАУ) между административните органи чрез RegiX. Общият брой консуматори на справки е над 950, като за 2021 г. са обработени 305 заявления за достъп до данни и са присъединени нови 243 консуматора.

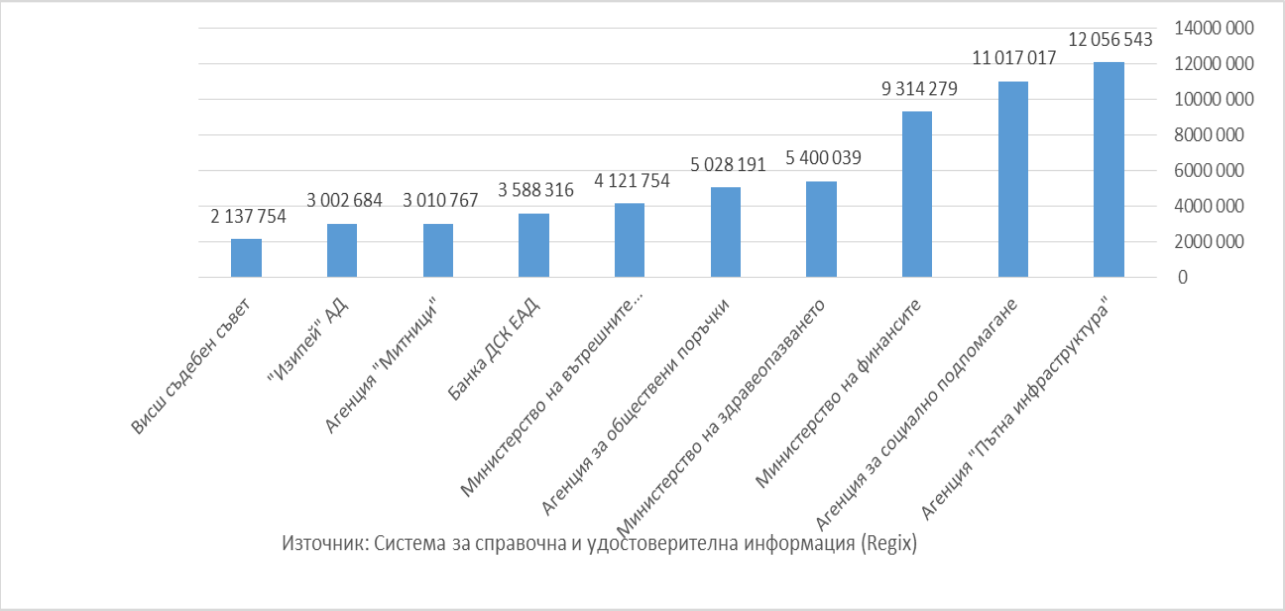
Данните от системата за 2021 г. са както следва:

- общият брой извършени справки през системата за 2021г. възлиза на 72 317 873 бр.;

- най-голям брой справки са регистрирани към регистри на Министерство на регионалното развитие и благоустройството – 17 857 473 бр., Агенция по вписванията – 17 432 714 бр. и Министерство на вътрешните работи – 13 950 362 бр.;

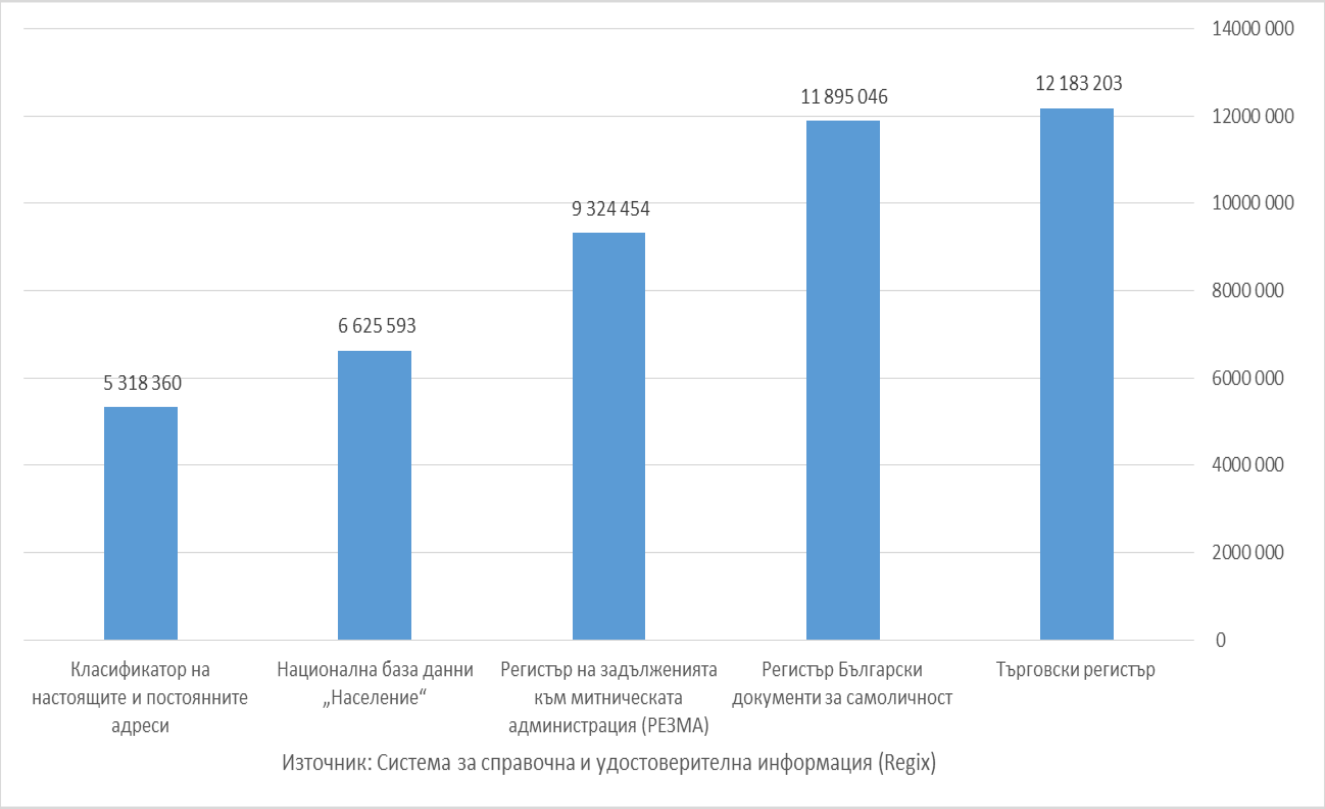
- потребител с най-голям брой заявки е Агенция „Пътна инфраструктура“ – ; 12 056 543 бр.;

- най-голям брой справки са извършвани от Търговския регистър – 12 183 203 бр.



Фигура 11. Топ 10 „Консуматор“ на справки

Фигура 12. Топ 10 посещавани администрации



***Фигура 13**. Справки и посетени регистри за 2021 г.*

За периода са присъединени 11 регистъра с 13 справки и операции за достъп на Комисията за регулиране на съобщенията (КРС).

В новото информационно приложение, на електронен адрес: https://info-regix.egov.bg/main се публикуват данните за присъединените регистри и операциите за достъп до тях, както и статистическа и справочна информация за използването на системата.

Активно се ползва разработеното и внедрено ново административно приложение, на електронен адрес: https://admin-regix.egov.bg/main и ново клиентско приложение: https://client-regix.egov.bg/main.

На фигурата по-долу е представена статистика, свързана с отчетения общ брой справки, генерирани през средата, разпределени по години.

***Фигура 14.**: Брой справки генерирани през средата, разпределени по години*

Към 31.12.2021 г. към RegiX са интегрирани 310 информационни системи на лицата по чл. 1, ал. 1и 2 от ЗЕУ.

През последната година към RegiX са присъединени всички общински администрации. Засиленото използване на системата RegiX се дължи както на популяризирането ѝ сред консуматорите, така и на законовите изисквания, задължаващи административните органи и лицата по чл. 1, ал. 1 и 2 от ЗЕУ да предоставят ВЕАУ с цел намаляване на административната тежест за гражданите и бизнеса.

3.3. Информационни системи в администрациите

Информационните системи в държавната администрация се явяват важна предпоставка за автоматизиране на вътрешно-административните процеси и за изпълнение на оперативните дейности. Данните в ИИСДА показват спад в броя на администрациите, които нямат внедрени информационни системи във всички категории, като най-значително е намалението при АИС за комплексно административно обслужване (близо 3%).

Администрации, които НЯМАТ внедрени информационни системи	**2019 г. %**	**2020 г. %**	**2021 %**
Административни информационни системи/ Система за документооборот	6.13	5.79	5.45
Система за управление на човешките ресурси	30.49	26.75	23.51
Система за труд и работна заплата	4.09	2.90	2.73
Система за счетоводство	4.60	1.70	1.36

***Таблица 5.** Администрации, които нямат внедрени информационни системи*

Система за управление на база данни	48.21	46.17	45.83
Системи за управление на документи, потоци и съдържание през WEB	54.36	46.85	44.46
АИС за комплексно административно обслужване	76.66	72.06	69.34
Система за правно-информационни услуги	-	17.04	16.87

През отчетния период, само в Агенция „Митници“ е стартирало изграждане и надграждане на 10 информационни системи в облачна архитектура (Red Hat OpenShift), изградена в ИТ инфраструктурата на агенцията.

4. Електронна идентификация

Действащата нормативна уредба в Република България предвижда, че лицата по чл. 1, ал. 1 и 2 от ЗЕУ са длъжни да осигурят възможност на гражданите и организациите при заявяването на ЕАУ да се идентифицират по реда на Закона за електронната идентификация (ЗЕИ) или чрез средства за електронна идентификация, определени с решение на Министерския съвет, издавани и поддържани от административни органи.

През отчетния период няма промяна по отношение на нормативно определените средства за електронна идентификация – КЕП, ПИК, издавани от НАП и НОИ, както и уникален код за достъп (УКД), издаван от Националната здравноосигурителна каса (НЗОК). Посочените средства са временно решение, обусловено от липсата на Национална схема за електронна идентификация по ЗЕИ. Тяхното използване е регламентирано в параграф 5 от Преходните и заключителни разпоредби на НОИИСРЕАУ.

4.1. Електронна идентификация за нуждите на заявяване на ЕАУ

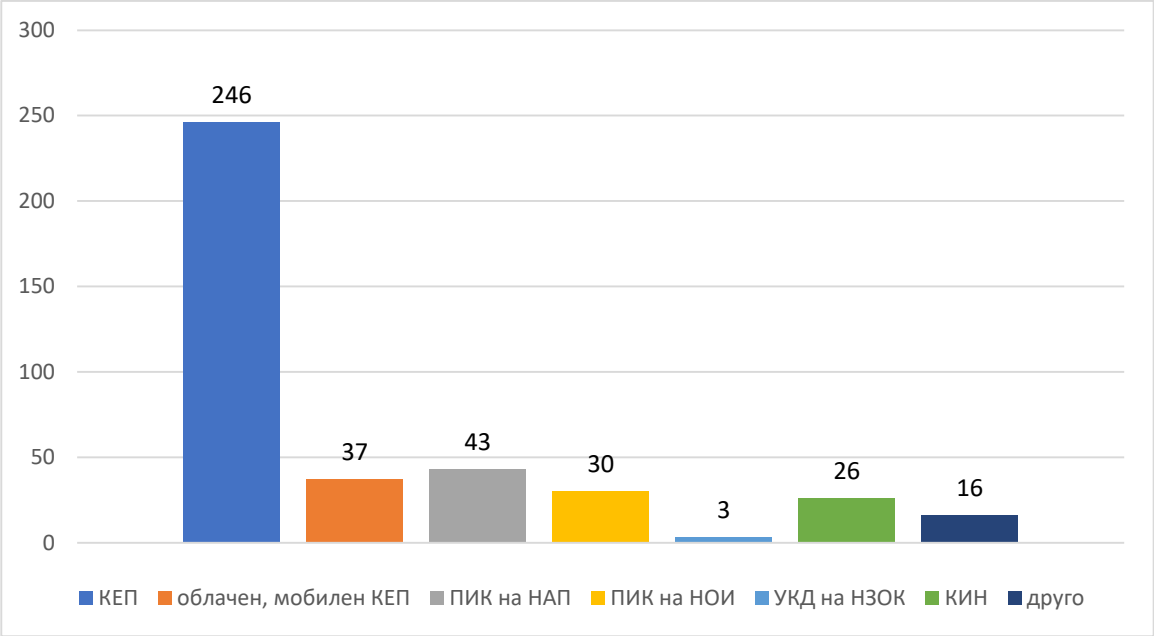
Анализът по отношение на електронната идентификация е направен на базата на данни, предоставени от административните органи в резултат на попълнени въпросници. Информация е изпратена от 367 администрации. При изготвяне на анализа е използвана и информация, съдържаща се в ИИСДА, събрана за нуждите на Годишния доклад за състоянието на администрацията за 2021 г. Не е налице възможност структурирано събиране и последващ анализ на данни в тази сфера.

През отчетния период остава значителен процентът на административните органи, посочили, че не предоставят ЕАУ, за които е необходима електронна идентификация на заявителя – около 33%[7]. Тук следва да се отбележи, че за настоящия анализ полетата от въпросника, оставени от администрациите празни, са отчетени със стойност „нула“. В резултат на посоченото, данните отразяват по-скоро тенденции по отношение на наблюдаваните параметри и не следва да се разглеждат като абсолютни стойности. Данните не могат да бъдат кредитирани като изчерпателни или достоверни.

През отчетния период се запазва тенденцията за преобладаващ брой административни органи, които предоставят ЕАУ след идентификация на потребителите с КЕП (*Фигура 15*). Броят на администрациите, които предоставят ЕАУ с някое от останалите нормативно определени средства за електронна идентификация е следният: От общо 367 администрации, предоставили отговор на изпратените въпросници, около 10 % са декларирали, че предоставят услуги, за които гражданите могат да се идентифицират с облачен, мобилен КЕП, около 12 % - с ПИК на НАП и около 8 % - с ПИК на НОИ. Запазва се тенденцията на

[7] *Анализът е направен на базата на получена информация от 367 административни органа*

изключително малък брой административни органи, които предоставят ЕАУ, които могат да се заявят с УКД на НЗОК – под 1 %.



Фигура 15. *Брой на административните органи, които предоставят ЕАУ с различни средства за електронна идентификация*

Независимо от продължаващата тенденция на слабо нарастване при предоставянето на ЕАУ, за които е необходима електронна идентификация на заявителя с облачен, мобилен КЕП, разликата с традиционния КЕП остава съществена. Както е посочено по-горе, около 10% от предоставилите информация административни органи са заявили, че предоставят ЕАУ, за които е необходима електронна идентификация на заявителя с облачен, мобилен КЕП при средно 8% за 2020 г.

Анализът на данните от попълнените въпросници показва, че се запазва слабият темп на намаляване на броя на администрациите, които използват клиентски идентификационен номер (КИН) като средство за електронна идентификация – около 7% при средно 9% към 31.12.2020 г. Тук следва да се отбележи, че употребата на КИН, като средство за идентификация, не е нормативно обусловено. Продължава използването и на други средства за електронна идентификация, които не са нормативно установени, но техният дял спрямо нормативно установените средства продължава да намалява. Такива средства се използват най-често от общинските администрации и се издават от тях самите във връзка с конкретни техни нужди. Тук се включват най-често КИН, различни персонални идентификационни кодове и номера (ПИК/ПИН) и по-рядко потребителско име и парола. Тези средства за електронна идентификация не способстват за защитата и сигурността на данните и е необходимо постепенно да отпаднат напълно.

Анализ по отношение на относителния общ брой ЕАУ, за които е необходима електронна идентификация на заявителя, е трудно да се направи на базата на подадената информация от административните органи. Запазва се положителната тенденция на увеличаване на броя им в резултат на продължаващия процес на интеграция на общинските администрации с хоризонталните системи на електронното управление, в частност с ЕПДЕАУ. Анализът на данните показва, че благодарение на тази интеграция се наблюдава постепенно намаляване на броя на административните органи (около 33%), които са заявили, че не предоставят ЕАУ, за които е необходима електронна идентификация на заявителя, при около 46% за предходния отчетен период. По този начин се предоставя възможност на

общините за достъп до разполагаем информационен ресурс в случаите, когато съответната община не разполага с достатъчно средства за цифровизация на услугите или изпитва недостиг на технически капацитет.

Независимо от положителната тенденция се запазва относително по-високия дял на териториалните администрации, в сравнение с централните, които не предоставят ЕАУ, за които е необходима електронна идентификация на заявителя (фиг. 14).

Фигура 16. *Брой на административните органи, които не предоставят ЕАУ, за които е електронна*

Данните показват, че намалява броят на административните органи, които са посочили, че през 2022 г. предвиждат внедряване на нови ЕАУ, за които е необходима електронна идентификация, по-специално с КЕП или облачен, мобилен КЕП. Те са около 26%, за разлика от предходния отчетен период, когато тенденцията е била нарастваща и те са били около 39%.

Във връзка с изпълнение на задължението, произтичащо от чл. 5, ал. 5 от ЗЕУ за вписване в Административния регистър на средствата за електронна идентификация, през 2021 г. беше утвърдена Методика за определяне от лицата по чл. 1, ал. 1 и 2 от Закона за електронното управление на средствата за електронна идентификация, които се използват при заявяване на ЕАУ и тяхното ниво на осигуреност. Методиката има за цел да подпомогне административните органи, лицата, осъществяващи публични функции и организациите, предоставящи обществени услуги в процеса по определяне на нивото на осигуреност на предоставяните от тях ЕАУ и средствата за електронна идентификация, с които тези услуги могат да се заявяват, както и нивото на осигуреност на тези средства. Методиката предоставя метод за определяне на нивото на осигуреност на средствата за електронна идентификация, който се основава на ключови критерии за оценка на риска при предоставяне на ЕАУ.

Около 60% от отговорилите на въпросника администрации са заявили, че са изпълнили изискването на чл. 5, ал. 5 от ЗЕУ, спазвайки Методиката. С това се наблюдава положителна тенденция на увеличаване на броя им в сравнение с предходния отчетен период, когато те са били около 42%. Около 20% са посочили, че все още не изпълняват изискването и около 20% - не са дали отговор на въпроса. Част от администрациите, които все още не изпълняват изискването, са заявили, че са в процес на актуализиране и въвеждане на данните или че този процес предстои. Сред основните причини за неизпълнение на законовата разпоредба, наред

с непредоставянето на ЕАУ, са липсата на административен капацитет, финансиране, както и липсата на специално поле в Административния регистър, в което да се нанася информацията за средствата за електронна идентификация и тяхното ниво на осигуреност.

След направена справка в ИИСДА, чрез извличане на данни, събрани във връзка с изготвянето на Годишния доклад за състоянието на администрацията за 2021 г., е установено, че 542 администрации са обявили средствата, с които по електронен път се идентифицират потребителите на ЕАУ. Съгласно тази информация 92% от администрациите изискват КЕП, 27% - ПИК и 23% - потребителско име и парола. Част от администрациите предоставят достъп до ЕАУ с повече от едно средство за електронна идентификация.

Видно от гореизложеното, налице е разминаване в подадените данни от административните органи в различните източници на информация. С оглед направения анализ е препоръчително през 2022 г. да бъдат извършени проверки от Министерството на електронното управление за установяване на фактическото положение. Необходимо е, също така, да се инициират промени в ИИСДА като се създаде специално поле в Административния регистър, в което да се нанася информацията за средствата за електронна идентификация и тяхното ниво на осигуреност.

4.2. Трансгранична електронна идентификация

С оглед задълженията на Република България, произтичащи от Регламент (ЕС) № 910/2014, да признава средствата за електронна идентификация, издадени в други държави членки на ЕС, през 2021 г. ДАЕУ изготви нова техническа спецификация за надграждане на българския eIDAS възел с най-новата версия, предоставена от ЕК.

През отчетния период остава почти непроменен броят на административните органи, които са заявили, че са предоставяли ЕАУ на граждани на държави – членки на ЕС – 4,6%. Повечето от тези администрации не са посочили кои са най-често заявяваните ЕАУ от чуждестранни граждани. Една от причините за този нисък резултат е, че администрациите не събират информация и не водят статистика за гражданството на заявителите на ЕАУ. Друга вероятна причина е, че информацията за ЕАУ, както и формулярите за заявяването им, не са налични на език, различен от българския. Някои администрации заявяват, че предоставят ЕАУ на чуждестранни граждани, които се идентифицират с КЕП, а други сочат, че за ЕАУ, които предоставят, е необходимо ЕГН за автентикация, което ги прави неприложими за чуждестранни граждани.

Над 95% от администрациите не предоставят ЕАУ на чуждестранни граждани. Наличната информация не може да послужи за задълбочен анализ, необходим за предприемането на целенасочени действия за предоставяне на конкретни трансгранични електронни услуги, към които има засилен интерес. Разбира се, трябва да се насърчава използването на ЕАУ от чуждестранни граждани, което изисква провеждането на целенасочена политика в тази сфера.

Във връзка с гореизложеното се оформят следните **изводи по отношение на електронната идентификация**:

- все още не е изградена националната схема за електронна идентификация, предвидена в Закона за електронната идентификация, което допринася за забавяне развитието на е-управлението и в определена степен ограничава достъпа на гражданите и бизнеса до ЕАУ, в т.ч. и трансгранични такива;

- към настоящия момент правно регламентираните средства за електронна идентификация са КЕП, ПИК на НАП/НОИ и УКД на НЗОК;

- използват се и средства за електронна идентификация, които не са правно регламентирани - КИН (клиентски идентификационен номер), ПИН (персонален

идентификационен номер). Гражданите се идентифицират чрез тях предимно пред общинската администрация;

- запазва се тенденцията ЕАУ да се заявяват след идентификация на потребителя с традиционен КЕП в сравнение с останалите средства за електронна идентификация, включително и с облачен/мобилен КЕП;

- общинската администрация предоставя ЕАУ основно чрез ЕПДЕАУ и потребителите на тези услуги се идентифицират чрез средствата, които изисква портала, а именно: КЕП, включително облачен/мобилен КЕП и ПИК на НАП/НОИ;

- не всички администрации са изпълнили изискването на чл. 5, ал. 5 от ЗЕУ за вписване в Административния регистър на средствата за електронна идентификация, чрез които гражданите и организациите заявяват ЕАУ;

- изискването в КЕП да фигурира ЕГН на лицето преклудира възможността чрез това средство да се идентифицират граждани, чиито КЕП са издадени в другите държавите членки на Европейския съюз и не съдържат ЕГН;

- необходимо е иницииране на промяна в Административния регистър с оглед вписването на средствата на електронна идентификация и тяхното ниво на осигуреност в специално създадено за целта поле.

5. Регистри, поддържани от администрацията

За отчетния период, съгласно данните, отчетени в ИИСДА в 165 администрации се поддържат регистри, свързани с предоставяне на електронни административни услуги. Общо в администрацията, в т.ч. централна и териториална, се поддържат 2 271 регистри, свързани с предоставянето на ЕАУ за гражданите и бизнеса, и 20 такива от административни структури на отчет пред Народното събрание. От всички тези регистри са отчетени:

- 1 875 регистри, които се поддържат в електронен вид;

- 224 регистри, които се поддържат на хартиен носител и подлежат на електронизация;

- 192 регистри, за които закон предвижда да се водят на ръка и не подлежат на електронизация.

Всички регистри, водени без нормативно основание, следва да отпаднат или да се уредят със закон. Съгласно приложение № 3 към Концепцията за регистрова реформа са включени 66 мерки, съгласно които административните органи предвиждат конкретни действия за заличаване на регистри или регламентирането им със закон. Според получената и обобщена информация, към края на 2021 г. са заличени 20 регистри, а други 8 са нормативно регламентирани:

- Регистър на представителите по индустриална собственост;

- Регистър на лицата, прехвърлили средства от българска пенсионна схема към пенсионна схема на Съюза, на ЕЦБ или на ЕИБ;

- Регистър на техниката по Закона за регистрация и контрол на земеделската и горската техника (ЗРКЗГТ) и на лицата, придобили правоспособност за работа с нея;

- Регистър на свидетелствата за правоспособност за работа с техника по Закона за регистрация и контрол на земеделската и горската техника;

- Регистър на издадените лицензи на Общността и заверените копия на лицензи;

- Регистър на издадените удостоверения за одобрение на ППС за превоз на опасни товари;

- Регистър на издадените разрешения за въвеждане в експлоатация на структурни подсистеми;

- Регистър на издадените и отнетите разрешения за осъществяване на дейности по Наредба № 8121з-531 от 2014 г. за реда и условията за осъществяване на дейността по осигуряване на пожарна безопасност на обекти и/или поддържане и обслужване на уреди, системи и съоръжения, свързани с пожарната безопасност, от търговци и контрола върху тях.

6 Споделени информационни ресурси

Съгласно § 1, т. 27 от Допълнителните разпоредби към ЗЕУ „Споделени информационни ресурси на електронното управление“ са техническата инфраструктура, единната електронна съобщителна мрежа, информационните центрове и държавния хибриден частен облак, които се създават и развиват от Министерството на електронното управление и се използват споделено от всички държавни органи.

6.1. Държавен хибриден частен облак (ДХЧО)

През 2021 г. завърши Втора фаза от проекта по надграждане на Държавния хибриден частен облак и изграждане на защитен интернет възел за публичните услуги на електронното управление, чиято цел е изграждането на сигурна и защитена (високоустойчива и резервирана) облачна инфраструктура, разположена в два центъра за обработка на данни, Контролно-технически център на електронното правителство и Център за възстановяване на данни, предоставяща инфраструктура като услуга.

Посредством изпратените въпросници е събрана актуална информация от администрациите относно промяната в нагласите и плановете им за използване на облачни технологии. Част от административните структури не са подали информация в определения срок, което редуцира обхвата на анализа. Въпреки това, може да бъде откроена продължаващата тенденция за значителен ръст при използването на споделените информационни ресурси на е-управление със следните проявления:

- по данни на ДАЕУ 91 администрации ползват облачни услуги на ДХЧО. Следва да се отбележи, че по информация от попълнените въпросници 51 администрации заявяват, че ползват публични облачни услуги извън ДХЧО, 160 администрации нямат намерение да ползват облачни платформи;

- 38 от отговорилите административни структури определят като полезно използването на ДХЧО и хранилището за данни на ЕУ, докато 84 анализират възможностите за неговото ползване, а 133 определят това като полезно в бъдеще за тяхната администрация, но все още не са направили пълен анализ;

- декларирана е допълнителна необходимост от ресурс за съхранение на данни в ДХЧО от общо 912 TB, което представлява увеличение с 20 %. Разпределението по вид администрация е както следва:

  - 343 TB за централната администрация;

  - 569 TB за териториалната администрация;

- 79 структури имат готовност за използване на текущо предоставяните от ДХЧО услуги за развойна дейност;

- 35 администрации подготвят информационни системи за миграция към ДХЧО, а някои от тях посочват срок за готовност предимно до края на 2022 г;

- 29 заявяват потребност от увеличаване на предоставения обем за съхранение на критични данни в хранилището на ЕУ;

- 97 посочват, че имат технически възможности и експертен капацитет за използване на ДХЧО и хранилището на ЕУ.

Сред причините по-голямата част от администрациите да не предвиждат присъединяване към ДХЧО в скоро време е недостигът на технически и административен капацитет. Същевременно много от тях заявяват необходимост от представяне на по-подробна информация относно начините за използване на споделените информационни ресурси.

През 2021 г. натоварването на ресурсите на ДХЧО е нараснало значително и е както следва:

За клъстер 1 на Основния център за данни на ДХЧО:

- 90 % от наличната изчислителна мощност;
- 63 % от хардуера за съхранение на данни.

За клъстер 2 на Основния център за данни на ДХЧО:

- 87 % от наличната изчислителна мощност;
- 92 % от хардуера за съхранение на данни.

Общо 41 системи на 8 администрации са разположени в инфраструктурата на ДХЧО, като ДАЕУ е собственик на 18 от тях.

6.2. Единна електронна съобщителна мрежа (ЕЕСМ)

През отчетния период продължава изпълнението на дейностите по развитие, осигуряване и поддържане на мрежовите и информационните ресурси, в това число ЕЕСМ. През 2021 г. са реализирани дейности по присъединяването на нови абонати; повишаване на ефективността на трафика и на електронните съобщения; обезпечаването на мрежовата и информационната сигурност. Високоскоростен, надежден и сигурен пренос на данни, глас и видео през ЕЕСМ за нуждите на държавното управление и националната сигурност се осигурява в режим 365/24/7.

Използваните в ЕЕСМ съвременни технологии позволяват виртуално да се обединят в единна национална информационна инфраструктура корпоративните мрежи на централната и териториалната администрация, като се запази тяхната информационна самостоятелност, автономното им управление и се изключи всяка форма на нерегламентиран достъп до пренасяната информация. Гаранционната и извънгаранционна поддръжка на ЕЕСМ се извършва от оторизирани фирми на производителя на мрежовото оборудване.

По заявки на ползвателите на ЕЕСМ през отчетния период са изградени 65 нови възли за достъп и са преконфигурирани други такива.

Същевременно са реализирани следните услуги и дейности:

- осигуряване на достъп до комуникационна среда на ЕЕСМ и предоставяне на облачна услуга за нуждите на Областни администрации Видин, Стара Загора, Сливен, Пазарджик, Варна, Пловдив, Монтана, Ловеч, Добрич, Хасково, Кърджали, Бургас, София, Ямбол, Благоевград, Кюстендил;

- изграждане на Защитен интернет възел (ЗИВ) и предоставяне на услуги до ДХЧО;

- изграждане на тестова L3 услуга и активиране на BGP сесия с ДХЧО и Национален статистически институт. Изготвяне на адресен и методологичен план за разширяване на предоставената услуга и до други държавни ведомства;

- изграждане на втора връзка с капацитет 1Gbps между опорните комутатори в градовете Силистра и Шумен с цел резервираност;

- изграждане на втора връзка с капацитет 1Gbps между опорните маршрутизатори в градовете Смолян и Кърджали с цел резервираност;

- изграждане на втора връзка с капацитет 10Gbps между опорните маршрутизатори в градовете Стара Загора и Сливен с цел резервираност;

- изграждане на втора връзка с капацитет 10Gbps между опорните маршрутизатори в гр. Стара Загора и в гр. Сливен с цел резервираност;

- тестване на 10 G и 100 G скорост по направление ДАЕУ – София 4 , Благоевград – Велико Търново;

- провизирана L3 услуга в градовете Сливен, Русе, Ловеч, , София, Бургас и Ямбол за тестове;

- провизиране на L2/L3 услуги по заявки за нуждите на: Министерство на вътрешните работи, Министерство на отбраната, Главна инспекция по труда, Прокуратура на РБ, Главна дирекция „Въздухоплавателна администрация“, Министерски съвет, Национална агенция за приходите, Главна дирекция „Охрана“, Министерство на здравеопазването, Министерство на финансите, Министерство на правосъдието, Община Аспарухово, Държавна агенция „Национална сигурност“, Национален осигурителен институт, ОА гр. Монтана, Областна администрация (ОА) гр. Ловеч, Централен регистър на особените залози, Български институт по метрология, ДА за бежанците, ОА гр. Бургас, ГД „Изпълнение на наказанията“, ОА гр. Ямбол, ОА гр. Пазарджик, Столична община, МРРБ, Министерство на земеделието, ВАС, Държавна агенция за научни изследвания и иновации, Агенция по геодезия, картография и кадастър, ЦИК, ОА гр. Добрич, КПКОНПИ;

- миграция и монтаж на опорен маршрутизатор в ОА Сливен на 10G свързаност;

- миграция на опорен маршрутизатор в ОА Ямбол. Пускане на комуникационни услуги;

- монтиране на 10Gbps транспондери за НАП, изграждане и тестване на връзка Ботевград - Велико Търново;

- направено е проучване за осигуряване на свързаност чрез EECM на структури от страната, напр. за някои ВРБ към министъра на финансите на територията на обл. Бургас, за свързаност за нуждите на Държавен Архив в обл. Бургас, за нови точки за нуждите на Министерство на регионалното развитие и благоустройство, проучване за Висшия съдебен съвет (ВСС) за осигуряване на свързаност, чрез EECM за нуждите на "Районен съд" на територията на обл. Бургас, за нуждите на Районен съд, Агенция „Митници“ и Агенция за държавна финансова инспекция в градовете Хасково, Смолян и Кърджали;

- изградена свързаност на НОИ Стара Загора;

- измерване на Оптични трасета по направления: ОА Хасково – ОА Кърджали, ОА Хасково – ОА Стара Загора; ОА Хасково – Стамболово;

- изградена тестова среда на L3 за проверка на новоизграждаща се система за свързаност на поделенията на Агенция „Митници“.

6.3. Хранилище за данни на електронното управление

Хранилището за данни на е-управление служи за бекъп (резервни копия) върху дискови устройства на данни на ведомства с критични системи и регистри на е-управление. То е разположено в основния център на е-управление и е напълно работоспособно. Съгласно утвърдената процедура, административните структури, които са първични администратори на критични бази данни и регистри, могат да съхраняват допълнителни резервни копия на критичните си данни.

Осемте административни структури, включително Агенция по вписванията, които трансферират данни в хранилището, имат резервиран капацитет от 86ТБ.

За четири структури (ГД ГРАО, Агенция геодезия, картография и кадастър, Агенция „Митници“ и Национален осигурителен институт) са закупени и инсталирани допълнителни хардуерни устройства за използване на хранилището.

7 Предоставяне на електронни административни услуги

Ефективното реализиране на цифровата трансформация на администрацията, насочена към изпълнение на принципа „потребителя в центъра на административното обслужване“, изисква оптимизация на ресурси и реинженеринг на работните процеси при изграждането и развитието на информационните системи и приложенията за електронни услуги.

Развитието на хоризонталните и централизираните системи на електронното управление и налагането на Единния модел за заявяване, плащане и предоставяне на ЕАУ осигуряват възможност за предлагане на повече електронни услуги от ниво 3 (заявяване и получаване на услуги по електронен път) и ниво 4 (заявяване и получаване на услуги по електронен път, вкл. онлайн разплащане), в случай че изискват плащане, през единна входна точка, спестява ресурси на администрациите и осигурява по-добра координация и контрол по отношение на изискванията за оперативната съвместимост към информационните системи на администрациите.

7.1. Състояние на електронните административни услуги

Съгласно обобщената информация от годишните отчети за 2021 г. в ИИСДА, администрациите, предлагащи ЕАУ, са 398 от общо 587, отчели се администрации. Общият брой услуги[8], вписани в АР към 31.12.2021 г., е 38 876, от които 10 008 услуги се предоставят на ниво 3 или ниво 4. Справката към края на отчетния период показва, че продължава тенденцията на нарастване на броя на услугите от нива 3 и 4, като за първи път се отчита превес на услугите от ниво 4 (фиг. 19). Важно е да се отбележи обаче, че тази справка отчита всяка една услуга, предоставяна от отделен административен орган като отделна, и не отразява факта, че има множество еднотипни услуги, които се предоставят. Това обяснява и големия получен от справката брой на ЕАУ.

Следва да се отбележи, че голяма част от вписаните в АР услуги са едни и същи (предимно тези на общини, областни администрации и териториални администрации), но се предоставят от различни администрации. Невъзможността да бъдат агрегирани данните по еднотипни услуги, освен че води до разминаване в реалния брой услуги, води и до затруднения в интерпретацията на информацията що се касае до ЕАУ, предоставяни от общинските, от областните и от териториалните администрации.

[8] *Общинските, областните и видовете специализирани териториални администрации (СТА) могат да предоставят услуги от определени набори от услуги – съответно „Услуги предоставяни от общински администрации“, „Услуги предоставяни от областни администрации“, „Услуги предоставяни от специализирани териториални администрации“ - за всеки вид СТА, както и „Услуги, предоставяни от всички администрации“ (https://iisda.government.bg/adm_services/services); в посочения общ брой на услугите - 38 876, всяка конкретна услуга е отчетена за всяка администрация, която я предоставя и е вписала в АР*

Фигура 17. *Брой услуги от ниво 3 или ниво 4 по години*

Въпреки значителното увеличение на броя на административните услуги, предоставяни на нива 3 и 4, техният дял от общия брой предлагани услуги все още остава нисък (26 %).

7.2. Осигуряване на институционална идентичност и достъпност на уебсайтовете

Официалните интернет страници и порталите на държавните администрации трябва да подобряват, насърчават и реализират взаимодействието на административните органи и организации в Република България с гражданите и бизнеса - потребители на административни услуги и информация. Администрациите проектират, създават, поддържат и актуализират своите интернет страници, спазвайки единна рамка[9] за институционална идентичност, която гарантира, че интернет страниците и порталите на администрациите в Република България са ориентирани към потребителя и са с безпрепятствен, пряк и постоянен достъп, ясна навигация и съдържание.

Осигуряването на равен достъп до ЕАУ и онлайн информацията за всички потребители, включително за лица с увреждания и функционални ограничения, се гарантира с приложимите хармонизирани стандарти за достъпност, части от тях или технически спецификации, в съответствие с които трябва се изграждат и развиват интернет страниците на администрациите.

През 2021 г., в изпълнение на задълженията на България по наблюдение и прилагане на изискванията на Директива (ЕС) 2016/2102 относно достъпността на уебсайтовете и мобилните приложения на организациите от обществения сектор, са извършени проверки на 100 уебсайта на административни структури от различни нива на администрацията.

Проверките се осъществиха съобразно „Методология за наблюдение и проверки на достъпността на съдържанието на интернет страниците и мобилните приложения“[10], в съответствие с установената с Решение за изпълнение (ЕС) 2018/1524 на ЕК методика и

[9] *Правила за институционална идентичност на интернет страниците и портали на държавната администрация, определени със Заповед ДАЕУ-15967/ 15.11.2019 г. на председателя на ДАЕУ. Тяхната актуализация – изменения и допълнения, се осъществява по реда на определянето им в съответствие с чл. 40, ал. 1 на НОИИСРЕАУ*

[10] *Методологията и приложенията към нея (вкл. образец на декларация за достъпност) са публикувани на адрес: https://e-gov.bg/wps/portal/agency/home/%D0%B0ccessibility-websites/web-access-documentation.*

хармонизирания стандарт EN 301 549 V2.1.2 (2018-08)[11], разработен в подкрепа на Директива (ЕС) 2016/2102 и осигуряващ минималното равнище на достъпност. В процеса на проверките бяха включени и потребители с увреждания с използване на спомагателни технологии с цел допълнително идентифициране на реални проблеми с достъпността и използваемостта на уебсайтовете.

Проверките за достъпност на интернет страниците, извършени с автоматични инструменти с допълнително верифициране чрез ръчни проверки от проверяващите експерти и потребителско тестване от хора с увреждания, както и задълбочените проверки по всички изисквания на хармонизирания стандарт, установиха в по-голяма или по-малка степен несъответствия със стандарта, съответно недостъпно съдържание за хора с определени увреждания.

За наблюдаваните уебсайтове се извърши и проверка за изпълнение на задължението организациите да публикуват на видно място на официалните си интернет страници декларация за достъпност, която да осигурява полезна информация за потребителите. При прегледа за наличие на декларации за достъпност се констатира, че само за 14% от наблюдаваните уебсайтове има публикувана такава, като част от декларациите не са изготвени по изискуемия образец. В съществена част от проверените декларации се констатира липса на описание на недостъпното съдържание, а вместо това посочване на изисквания, които са неприложими за наличното съдържание на сайта.

Резултатите от проверките, с включени предписания и срок за отстраняването им, са предоставени на проверените администрации.

Анализът на резултатите показва, че най-често срещаните несъответствия с изискванията за достъпност са свързани с:

- липса на алтернативен текст за изображения, предоставящ еквивалентна информация за потребителите, които не могат да видят изображението и използват спомагателни технологии; неподходящ алтернативен текст; празен alt атрибут за изображения, които не са декоративни; не коректно маркирани декоративни изображения. В някои от сайтовете е използвана CAPCHA[12] без осигурени достъпни алтернативи, което превръща тази защита в непреодолима бариера за потребители, които са незрящи или сляпо глухи и ги лишава от правото, в констатираните случаи, да изпратят самостоятелно сигнал или да подадат формуляр за обратна връзка чрез сайта, или да получат достъп до услуга;

- етикети, които не са програмно свързани със съответстващите им текстови полета във формуляри, за да може както визуално, така и звуково да се възприема целта на полето и каква входна информация се очаква от потребителя;

- недостъпност на цялата функционалност и съдържание на страница с помощта на клавиатурата – наличие на елементи, които могат да се активират единствено с мишка;

- използване на комбинации между цвят на текст и неговия фон, които не осигуряват достатъчен контраст, съгласно изискването на хармонизирания стандарт; ниският контраст е най-често срещаната грешка, в почти всички сайтове;

- връзки с текст, който не описва разбираемо целта на връзката; връзки без текстово съдържание (като текст или текстова алтернатива) или без етикет, който идентифицира целта;

---

[11] *Съдържанието на интернет страниците на административните органи, на доставчиците на обществени услуги и на лицата, осъществяващи публични функции, трябва да отговаря на хармонизирания стандарт EN 301 549 Accessibility requirements for ICT products and services, последната версия, публикувана в Официален вестник на ЕС. Към настоящия момент това е EN 301 549* ***V3.2.1*** *(2021-03) (ОВ L 289/53 от 12.08.2021 г.), който реферира към WCAG 2.1 AA.*

[12] *Предназначена за установяване, че достъпът до съдържанието се осъществява от човек, а не от компютър*

- неправилно йерархично вложени заглавия (headings), липса на заглавие от ниво 1 за основната тема на страница; структура, която не представя правилно основните теми на страницата и вложените подтеми, както и празни заглавия (без съдържание), което затруднява навигацията и не осигурява бърз достъп до основното съдържание на страницата и възможност за пропускане на менюта и реклами;

- неидентифициран или неправилно определен основен език на страница, което затруднява интерпретирането от браузера, както и от спомагателните технологии чрез зареждане на подходящи шрифтове, фонетични правила за речевия синтез, брайлови кодови таблици и потребителите биха могли да изпаднат в невъзможност да прочетат и възприемат съдържанието;

- недостатъчно информативни заглавия на страници или заглавия, които не съответстват на добрата практика в началото да бъде информацията, уникална за страницата (първо специфичната информация за страницата и след това за сайта, към който принадлежи), напр. започват с наименованието на организацията.

Значителна част от документите, които могат да се свалят от проверените страници са недостъпни за ползватели с екранен четец - някои от тях са напълно нечетими (напр. pdf файлове със сканирани изображения), част са четими, но достъпността им е на най-ниско ниво (текстът може да бъде изчетен, но липсва достъпна навигация или PDF тагове например) и подлежи на подобрение.

В контекста на Директива (ЕС) 2016/2102, достъпността следва да се осигурява на всеки етап - при проектирането, създаването, поддържането и актуализирането на уебсайтовете, за да може те да станат по-достъпни за потребителите и по-специално за хората с увреждания.

С цел намаляване на разходите на администрациите при прилагането на политиките за е-управление, е създадена възможност за изграждане на портален сайт чрез шаблон, разработен в съответствие с изискванията за достъпност на хармонизирания стандарт и Правилата за институционална идентичност на интернет страниците и портали на държавната администрация. Шаблоните позволяват относителна персонализация на облика на уебсайта, но запазват структурата с цел улеснение на крайния потребител и създаване на единна визуална онлайн идентичност на държавните институции. На разположение на администрациите е услугата „Изграждане на федериран портал“, която представлява облачно решение за изграждане на множество портални уебсайтове в инфраструктурата на ЕПДЕАУ.

IV. УКРЕПВАНЕ НА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ (МИС)

Дистанционната работа в условията на извънредно положение и тази година е обичайна практика за много от българските администрации. Работещите от домовете си служители могат да представляват повишен риск, тъй като се оказват извън обхвата на защитните средства, използвани в административните мрежи. Важен фактор за повишаване на сигурността е и личната организация на всеки служител. Мрежите и информационните системи са взаимосвързани и предвид глобалния характер на интернет, много инциденти в областта на мрежовата и информационна сигурност надхвърлят националните граници.

1 Състояние на мрежовата и информационната сигурност

Посредством изпратените въпросници са получени и анализирани данни от 481 административни органа относно част от изискванията за минималните мерки за мрежова и информационна сигурност, които са разписани в Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС).

Основните тенденции, очертани от подадената информация, обобщени в таблицата по-долу, показват, че все още МИС не е приоритет за голяма част от администрациите, като

прави впечатление, че над половината от тях не са провели вътрешен одит на МИС, а при близо 40% липсва анализ и оценка на рисковете за информационната сигурност.

Показател	Да	Не	Без отговор
Въведена политика за информационна сигурност	50	19	31
Анализ и оценка на рисковете за информационна сигурност	29	39	32
Проведен вътрешен одит на МИС	14	55	31
Публично достъпни интернет сайтове	66	5	29
Въведена политика за архивиране на информацията	46	22	32
Собствен, управляван от Вас сървър за електронна поща	14	39	38
Web Application Firewall (WAF)	29	40	31
VPN	32	39	29
Използване на частни фирми за поддръжка на системи / предоставяне на услуги	25	46	29

Таблица 5. *Брой администрации, изпълняващи определени показатели по отношение на МИС*

За спазването на законоустановените мерки се извършват регулярни проверки.

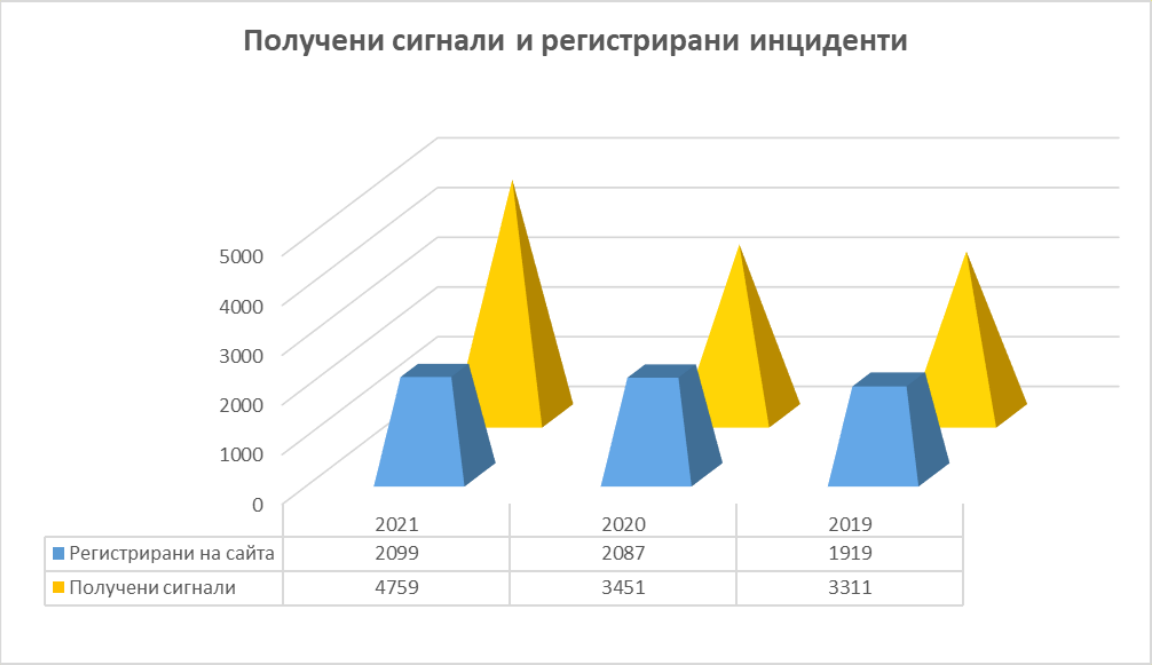
Въпреки че съществуват общи черти между подлежащите на решаване предизвикателства и проблеми, администрациите се различават по мерки и механизми за гарантиране на сигурността и устойчивостта, както и по нивото на експертни знания и готовност. За периода от 01.01.2021 г. до 31.12.2021 г. са извършени 14 оценки съобразно Методика и правила за извършване на оценка за съответствие с мерките за мрежова и информационна сигурност, определени с НМИМИС и Годишната програма за проверки по чл. 36, ал. 4 от НМИМИС. Средният резултат от извършените оценки е 66,29%. Резултатите показват, че продължава тенденцията по-голяма част от анкетираните администрации да привеждат документацията си съобразно изискванията на Наредбата – те имат разработени вътрешни правила и са направили преглед на адекватността на предприетите мерки през последната година. Все още се наблюдават проблеми при класификацията на информацията, като най-големият проблем е, че класификацията не е приложена върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето и унищожаването ѝ. Друг проблем, който се наблюдава е, че не са проведени инструктажи за повишаване на вниманието им по отношение на мрежовата и информационната сигурност за период от една година назад от датата на настоящото оценяване на служителите. Повишаването на информираността на служителите ще повиши бдителността и компетенциите им и това ще

допринесе за намаляване на инцидентите в организацията. Наблюдава се и повишаване на сигурността на уебсайтовете на институциите, като голяма част от тях са приложили изискванията на законодателството. При повечето от анкетираните администрации се прави регулярно резервно копие на информацията.

Бяха извършени сканирания на 546 домейна на администрациите, като резултатите са, както следва:

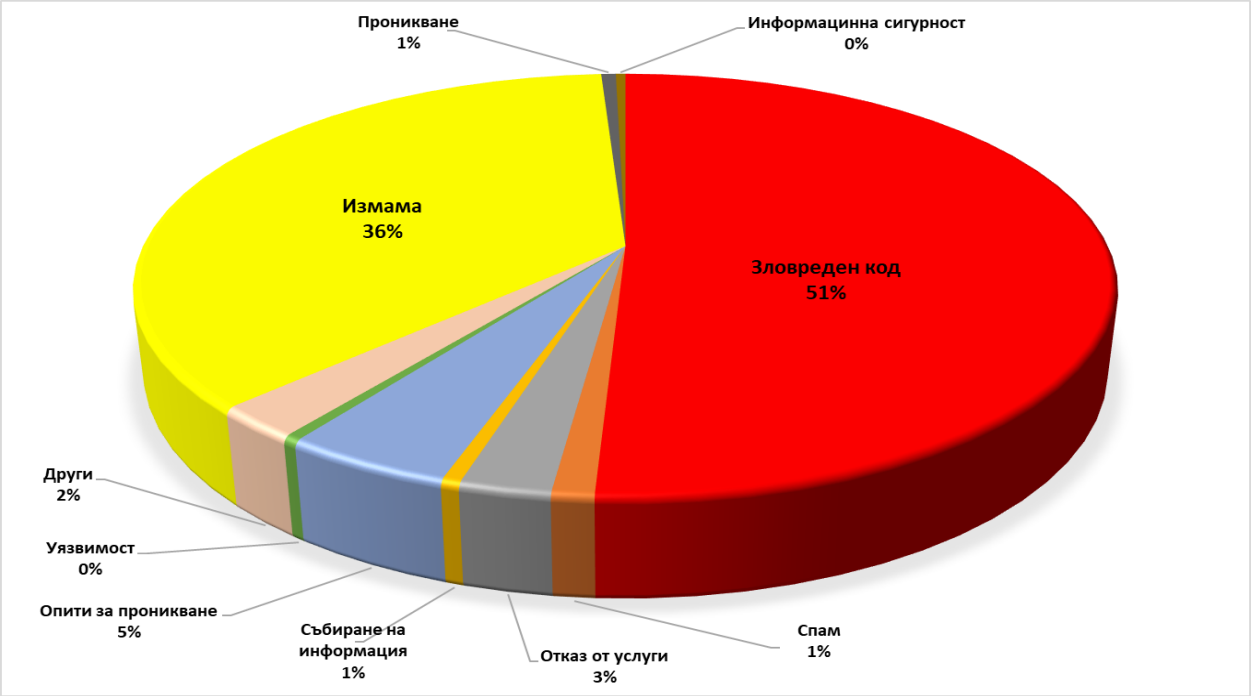
- 84% имат наличен Secure Sockets Layer (SSL) сертификат;
- 74% са съвместими с Transport Layer Security (TLS);
- 76% разполагат със Sender Policy Framework (SPF);
- 89% нямат Domain-based Message Authentication, Reporting & Conformance (DMARC) и при 86% липсват DNSSEC разширения.

В периода януари – декември 2021 г. Националният екип за реагиране при инциденти с компютърната сигурност констатира непрекъснато усложняване на обстановката в киберсигурността на страната, като са регистрирани 4759 сигнала. От тях като инциденти, съгласно таксономията на Европейската агенция за киберсигурност – ENISA, са регистрирани 2 099 бр., което представлява леко увеличение на получените сигнали спрямо същия период през изминалата година, но броят регистрирани инциденти се запазва почти същия.

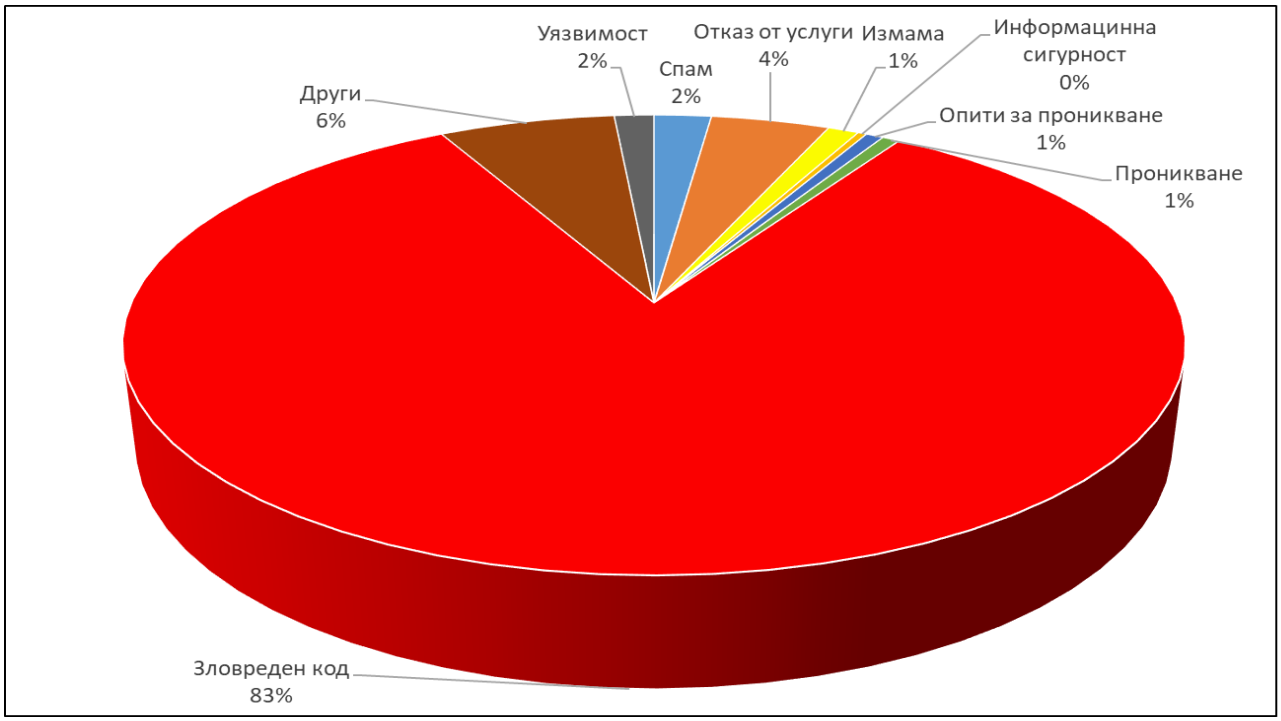


Фигура 18. *Получени сигнали и регистрирани инциденти*

През настоящия отчетен период най-често срещаните причини за инциденти остават разпространение на зловреден код и измама (phishing). За даване на указания и препоръки за разрешаването на инциденти и за преустановяването на нарушения Националният екип за реагиране при инциденти с компютърната сигурност е подготвил и изпратил близо 22 хиляди имейла. На графиките по-долу са показани видовете регистрирани инциденти за отчетния период.



Фигура 19. *Видове регистрирани инциденти за периода 01.01.2021 г.-31.12.2021 г.*



Фигура 20. *Видове регистрирани инциденти в ДА за периода 01.01.2021 г.-31.12.2021 г.*

Хакерските групи продължават да се насочват към субекти в държавите-членки на ЕС, в т.ч. и България, с цел придобиване на чувствителна информация и създаване на условия за намеса върху поддържаната политика. Най-значимите атаки на тези хакерски групи са насочени към кражба на данни и мрежови устройства като рутери, комутатори, защитни стени, разположени в мрежите предимно на правителствени и частни организации, ръководители на обекти от критичната инфраструктура и доставчици на достъп до интернет (ISP), които поддържат тези сектори. По данни на Националния екип за реагиране при инциденти с компютърната сигурност за отчетния период има засегнати 276 970 IP адреса, което е с близо 30 % по-малко от 2020 г. В таблицата по-долу са представени данни за

последните три години, които включват брой засегнати IP адреси и съответно брой изпратени имейли.

	2021	2020	2019
Засегнати IP адреси	276 970	392 283	2 288 293
Изпратени имейли	18 103	18 617	21 883

Таблица 6. *Сравнителни данни за брой засегнати IP адреси и брой изпратени мейли през периода януари - декември 2019 г., 2020 г. и 2021 г.*

Продължаващата извънредна ситуация, която се създаде около пандемията COVID-19, промени изцяло стила на работа на всички, което наложи използването на допълнителни мерки за сигурност и защита от кибератаки. Увеличиха се драстично фишинг сайтовете свързани с COVID-19 и използването на уязвимости в софтуерите за организиране и провеждане на онлайн срещи и обучение, както и в софтуерите за отдалечен достъп. В много случаи това е използвано за разпространение на злонамерен софтуер от типа „рансъмуер“ и кражба на данни, което доведе до сериозни проблеми в работата на администрациите. Наблюдава се връщане към позабравени рансъмуер и активиране на вече използвани ботнети. Използването на ZeroDay и непачнати уязвимости се превърна в най-често използвания инструмент в ръцете на атакуващите.

Националният екип за реагиране при инциденти с компютърната сигурност ежемесечно, в изпълнение на проактивните си действия изпраща бюлетин до служителите в публичната администрация, отговарящи за мрежовата и информационната сигурност. Бюлетинът съдържа статистика на инцидентите за предходния месец, актуална информация и препоръки за добри практики. През отчетния период бяха изготвени и разпространение тематични бюлетини/предупреждения, свързани със зловредния код Pegasus, разпространението на рансъмуер, уязвимостта Log4j и сериозен пробив в сигурността на пощенските сървъри на Microsoft: Exchange Server 2013, Exchange Server 2016 и Exchange Server 2019.

2 Мерки за повишаване нивото на мрежовата и информационната сигурност

През отчетния период мерките за повишаване на нивото на мрежовата и информационната сигурност бяха насочени в следните направления:

От гледна точка на стратегическата база за киберсигурност беше актуализирана националната стратегия за киберсигурност „КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2023”, приета с Решение № 301на МС от 2 април 2021 г. и изготвена Пътна карта, публикувана на сайта на ДАЕУ. Изготвена е и 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 по обществена поръчка № 04312-2020-0001.

В допълнение, актуализиран е Планът за реакция при мащабни кибератаки и инциденти, при които са засегнати критични национални мрежови и информационни ресурси, чието блокиране, манипулиране и/или унищожаване би застрашило живота и здравето на гражданите, управлението на важни държавни и обществени процеси, би предизвикало паника, съизмерима с терористична заплаха, както и би довело до бизнес загуби в големи размери. Актуализиран е и съставът на Междуведомствената оперативна група и са проведени 3 тренировки по оповестяване и събиране на групата.

ДАЕУ, в ролята си на Национален компетентен орган за административните органи и сектора „Инфраструктури на финансовия пазар“, упражнява контрол за спазване на изискванията на Закона за киберсигурност и Наредбата за минималните изисквания за мрежова и информационна сигурност. Продължава и извършването на оценки за съответствие с изискванията, съобразно Методика и правила за извършване на оценка за съответствие с мерките за мрежова и информационна сигурност, определени с Наредбата за минималните изисквания за мрежова и информационна сигурност.

За отчетния период, по отношение на повишаване на нивото на мрежовата и информационна сигурност бяха извършени следните дейности:

- организираха се и се проведоха 4 броя обучения – две с отговорниците по МИС в администрациите на тема приложение на Наредбата за минималните изисквания за мрежова и информационна сигурност и две относно напътствия при одит по НМИМИС и процес по осъществяване на проверки съгласно чл. 12, т. 6 от ЗКС и разяснения по чл. 24 и чл. 25 от НМИМИС;
- извършиха се 7 сканирания за уязвимости в web сайтове и сървъри с публични IP адреси;
- изготвени бяха 7 доклада с констатирани уязвимости в web сайтове и сървъри с публични IP адреси и препоръки за отстраняването им;
- участие в 5 международни киберучения;
- участие в изготвянето на „Оценка на заплахите от организирана престъпност в България“ към Центъра за изследване на демокрацията;
- изготвени и изпратени бяха специални Указания за повишаване нивото на МИС при подготовката и провеждането на парламентарните избори;
- поддръжка на регистър на Операторите на съществени услуги по чл. 6 от Закона за киберсигурност;
- поддръжка на списък на извършените оценки за мрежова и информационна сигурност, съгласно изискванията на Методика и правила за извършване на оценка за съответствие с мерките за мрежова и информационна сигурност, определени с НМИМИС.

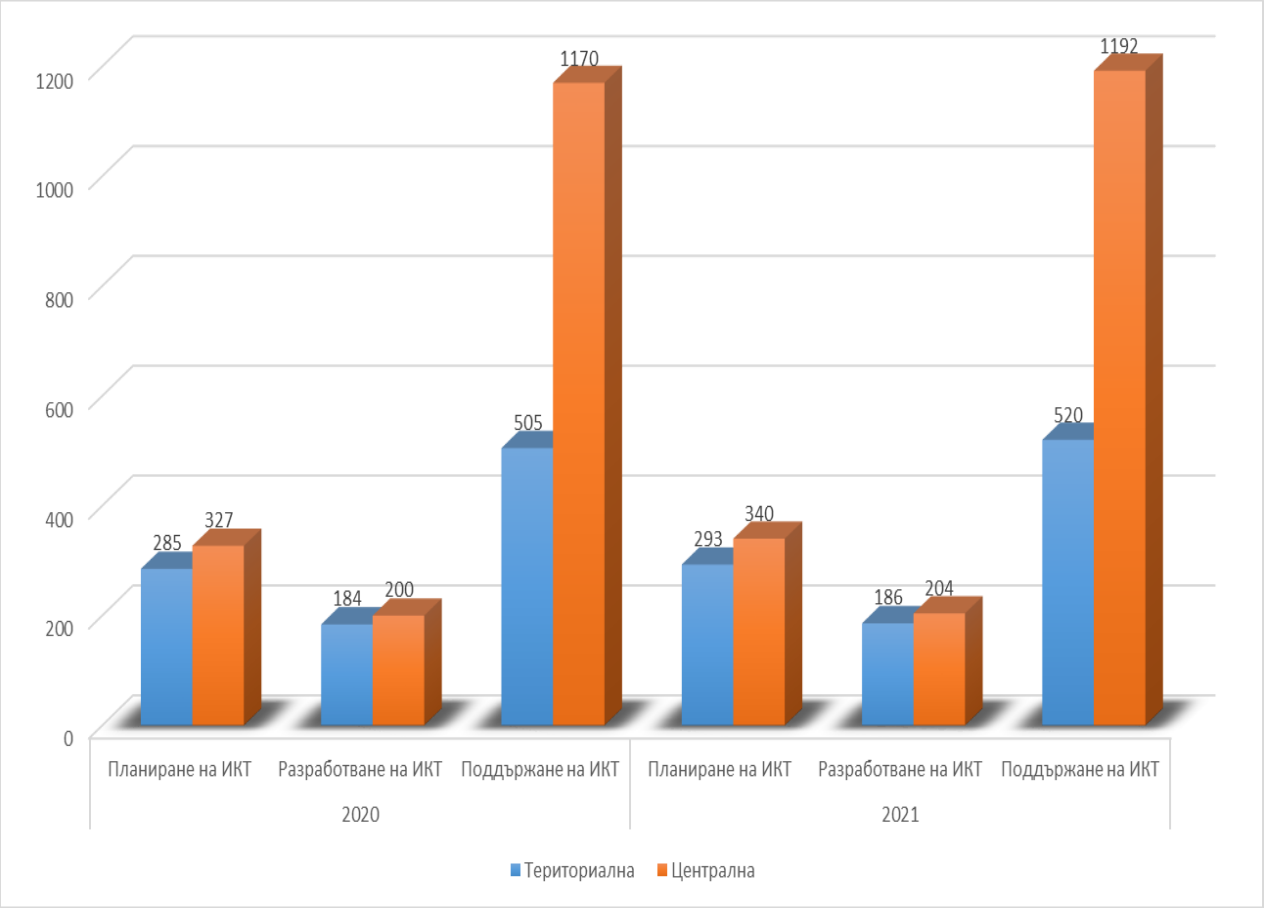
V. ЧОВЕШКИ РЕСУРС В ИКТ

За 2021 г. се запазва тенденцията в държавната администрация близо 37% от административните органи да разполагат с вътрешен ресурс – вътрешна структура (дирекция, отдел, звено) или отделни специалисти – за поддръжка на информационните ресурси в прилежащите им администрации. В сравнение с предходния отчетен период администрациите, които ползват както вътрешен, така и външен ресурс (външен изпълнител) нараства с повече от 7,5%, достигайки 28,5% от всички. 183 администрации или 31% от всички през 2021 г. разчитат изцяло на външни изпълнители за поддръжката на своите ИКТ. Положителна е тенденцията за намаляване на администрациите, които не ползват никакви механизми за поддръжка на своите информационни ресурси.

По вид администрация, по-голямата част от централната администрация ползва външен изпълнител или смесен подход (вътрешен ресурс и външен изпълнител) за поддръжката на информационните ресурси, докато най-малък дял от централните администрации разчитат изцяло на вътрешен капацитет. Някои, като например Агенция „Митници“, се насочват към използване на собствени ресурси за поддръжката на информационните ресурси и услуги в ИТ инфраструктурата си, на база на опита си при използването на смесен подход. Същата е тенденцията и при структурите на териториалната администрация, където близо 40% от всички териториални структури ползват изцяло вътрешен ресурс, но по-голямата част и от

тях също разчитат или на външен (32%) или смесен тип (25%). Както поради кадрови, така и икономически ограничения е налице невъзможност за изграждане на изцяло собствен административен капацитет в областта на ИКТ. Администрациите делегират експлоатационната поддръжка на информационните си системи или част от тях на външни изпълнители чрез договори с физически или юридически лица. С цел оптимизиране на разходите и за постигане на ефективност и ефикасност в държавната администрация е необходимо да се създадат условия общоразпространените функции по поддръжка на ИР да бъдат изведени като споделена услуга и да се оформят централни звена, които да осигуряват ИТ услуги в системата на дадена администрация или споделено между няколко администрации.

За 2021 г. общият брой на служителите в администрацията, занимаващи се с планиране, разработка или поддръжка на информационни ресурси е 2 517 или с 33 повече спрямо 2020 г. 4,5% е нарастването на служителите в териториалните структури на администрацията и 1% - в централната администрация. Детайлна разпределение на служителите по вид функция и вид администрация е представено в таблицата по-долу:



Фигура 21. *Брой служители в администрацията, ангажирани с ИР*

Спрямо 2020 г. се запазват и тенденциите относно нивата на заплащане на служителите в областта на ИКТ. Данните сочат, че разходите за възнаграждения на служители, занимаващи се с планиране, разработка или поддръжка на информационни ресурси, се запазват, въпреки възможностите, предоставени чрез вече изменената нормативна рамка за формиране на възнагражденията. В съчетание със силния конкурентен натиск на трудовия пазар от страна на частния сектор за специалисти в областта на ИКТ е необходимо разработването на единна политика за човешките ресурси за същите в държавната администрация. Политиката следва да цели:

- въвеждане на централизиран подбор на специалисти;
- привличане и задържане на висококвалифицираните кадри в администрацията, включително чрез залагане на по-високи нива на заплащане;
- въвеждане на ефективна система за атестиране с оглед превръщане на държавната администрация в предпочитано работно място за ИТ специалисти;
- разработване на инструментариум за кариерно развитие, включително „обучения през целия живот“ за повишаване и поддържане на знанията и уменията на служителите в областта на ИКТ в държавната администрация.

В заключение, предизвикателствата, породени от пандемията от COVID-19, потвърждават нуждата от повишаване на капацитета на служителите, отговарящи за ИКТ в администрацията, което е от основно значение за успешната реализация на политиката за е-управление, за информационната сигурност и за изграждането на ефективна цифрова администрация.

VI. КОНТРОЛ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ

1 Контрол в рамките на бюджетния процес на разходите за е-управление и ИКТ

Контролът в рамките на бюджетния процес се осъществява на основание чл. 7г от ЗЕУ и е съобразен с обхвата, определен от Закона за администрацията и съответната бюджетна процедура.

През 2021 г. всички административни органи изпращат за предварително съгласуване от председателя на ДАЕУ[13] тригодишните бюджетни прогнози за разходите за е-управление и за използваните ИКТ, проектобюджетите за следващата календарна година и актуализираните бюджетни прогнози за следващите две календарни години, промените във вече утвърдените бюджети за съответната година, както тримесечните и годишните отчети.

Проверките се извършват в съответствие със Задължителните разпореждания за предварително съгласуване на разходите на административните органи в областта на електронното управление и за използваните от тях информационни и комуникационни технологии в рамките на бюджетния процес.

Информацията по чл. 7г от ЗЕУ се подава от административните органи чрез Информационната система за извършване на предварителен, текущ и последващ контрол по целесъобразност в областта на електронното управление и използването на информационните и комуникационните технологии (ИСБК), изградена на основание разпоредбата на чл. 7г, ал. 1 от ЗЕУ, в рамките на проект „Разработване на публични регистри за бюджетен и проектен контрол на електронното управление и на портал за достъп до ресурси за разработка на софтуерни системи за електронно управление“, финансиран от Оперативна програма „Добро управление“.

ИСБК дава възможност за осъществяване на контрол по целесъобразност на разходите за ИКТ и е-управление в административните органи на ниво бюджетиране, планиране и изпълнение на проекти. Внедряването ѝ улесни начина, по който административните органи изпълняват задълженията си във връзка с разпоредбите на чл. чл. 7г от ЗЕУ. Системата е интегрирана с ИИСДА, Информационната система за управление и наблюдение на средствата от ЕС в България (ИСУН), РИР и RegiX.

[13] С обнародването на ЗИД на ЗЕУ, ДВ, бр. 15 от 22.02.2022г. Държавна агенция „Електронно управление“ към Министерския съвет се закрива. Правомощията на Председателя на ДАЕУ се поемат от Министъра на електронното управление.

В Закона за държавния бюджет на Република България са обособени целевите средства за е-управление и ИКТ. За 2021 г. те бяха в размер на 162 261 600 лв., като през годината, с 94 промени на утвърдените целеви разходи за е-управление и ИКТ, извършени по реда на Закона за публичните финанси, средствата достигнаха до 205 039 245 лв.

От тази сума, по предоставената към момента на изготвяне на настоящия отчет информация за отчета за касовото изпълнение на утвърдения бюджет за е-управление и ИКТ за 2021 г., административните органи са изразходвали общо 119 170 339 лв., или малко над 58%. Сравнително ниският процент усвояемост поставя множество въпроси, включително относно наличието на адекватен капацитет за навременно планиране и управление на дейностите на ниво отделен административен орган. Подобно неефективно разпределение на финансовия ресурс налага цялостно преосмисляне на съществуващите правила по отношение на разходите за електронно управление и информационни и комуникационни технологии, използвани от административните органи. Възможна причина за това е консервативната финансова политика на първостепенните разпоредители, които изкуствено „блокират“ финансов ресурс за второстепенните разпоредители пред по-голяма част от календарната година.

През октомври 2021 г., във връзка с подготовката и представянето на проектобюджетите на първостепенните разпоредители с бюджет за 2022 г. и актуализираните им бюджетни прогнози за 2023-2024 г. бяха съгласувани по целесъобразност средства целеви средства за е-управление и ИКТ за 2022 г. в размер на 212 102 200 лева, представени в ИСБК от 37 административни органи-първостепенни разпоредители с бюджет.

Следва да се отбележи, че измежду най-големите общини в страната, а именно областните центрове, общо 10 (или 37%) не са предоставили информация чрез ИСБК досега, съответно не са спазили задълженията си по нито една от разпоредбите на чл. 7г от ЗЕУ. Това са общините Варна, Видин, Кюстендил, Ловеч, Монтана, Перник, Плевен, Пловдив, Силистра, Търговище. Те са и общините, които разполагат ежегодно с едни от най-големите бюджети и същевременно се предполага, че заделят и най-много средства в областта на електронното управление и за използваните ИКТ. В допълнение, наблюдава се формално изпълнение по някои от разпоредбите от страна на Столична община. Последната еднократно подаде за съгласуване бюджет, който след като беше върнат за корекция, не беше изпратен повторно. Столична община няма подадена информация в изпълнение на задълженията си съгл. чл. 7г, ал. 2, т. 1, 2, и 4 от ЗЕУ.

Горното на практика означава, че огромна част от разходите на общините за ИКТ и е-управление не са съгласувани като целесъобразни.

През отчетния период част от общините подават електронни форми в ИСБК само при необходимост и/или вследствие на извършвана от инспектори на ДАЕУ проверка.

Най-често срещаните пропуски от страна на административните органи при вписване на информация в ИСБК са следните:

- липса на актуални годишни планове в Регистъра за информационните ресурси, в които трябва да бъдат въведени данни преди вписване в ИСБК на информация за тригодишните бюджетни прогнози или проектобюджета за следващата година и актуализираните бюджетни прогнози;

- в някои случаи постъпват форми, при които отчетените разходи надвишават предвидените такива в утвърдения бюджет за съответната година, което произтича от пренебрегването на задължението за своевременно подаване на искане за корекция на утвърдения бюджет при изменение на сумите за е-управление и ИКТ;

- неспазване на сроковете за вписване на информация;

- незавършване на създадените електронни форми, т.е не се пристъпва към тяхното финализиране и изпращане съгласно Задължителните разпореждания, което не позволява тяхното разглеждане и осъществяването на проверка по целесъобразност.

2 Контрол в процеса на утвърждаване на проектни предложения/дейности

Подаването на информация за произнасяне по реда на чл. 7в, ал. 2, т. 10 от ЗЕУ се осъществява задължително само чрез Регистъра на проектите, част от ИСБК, който е разработен на основание разпоредбата на чл. 7д, ал. 1 от ЗЕУ в рамките на проект „Разработване на публични регистри за бюджетен и проектен контрол на електронното управление и на портал за достъп до ресурси за разработка на софтуерни системи за електронно управление“, финансиран от Оперативна програма „Добро управление“. За периода 1 януари 2021 г. – 31 декември 2021 г. са утвърдени 43 проектни предложения/дейности.

През проверка по реда на чл. 7в, ал. 2, т. 10 от ЗЕУ са преминали 24 проектни предложения, допринасящи за постигането на целите на цифровия преход, с очаквано финансиране от Механизма за възстановяване и устойчивост, включени в Националния план за възстановяване и устойчивост.

Проблем от общ характер, а не при самото подаване на проектни предложения, е избирателното тълкуване на разпоредбата на чл. 7в, ал. 2, т. 10 относно необходимостта за утвърждаването на проектни предложения (ПП) по реда на ЗЕУ. Така, особено при проекти финансирани със средства от държавния бюджет, административните органи не изпращат за предварително утвърждаване проектно предложение за ИКТ и е-управление или подават такова едва след стартиране изпълнението на проекта. Подобна практика поставя под риск целесъобразността и съответствието на проектите и дейностите извършвани от административните органи с приетите стратегически и програмни документи.

Установени са следните най-чести пропуски при изготвяне на проектни предложения:

- посоченият индикативен бюджет на проектното предложение не е предварително съгласуван като целесъобразен, в рамките на процедурата по чл. 7г, ал. 2 от ЗЕУ;

- липсва ясна и подробна информация за предвидените за разработка, изграждане или внедряване на системи (в случай, че такова се предвижда). В съответното поле на ИСБК относно Краткото описание на изискванията към информационната система/регистри/бази данни, които ще бъдат включени в техническата спецификация, не се посочват предвидените външни и вътрешни интеграции, не са разписани начините на използване на системата, както и ефекта върху гражданите и бизнеса. Остава впечатлението, че административните органи често нямат ясна представа, дори на етап проектно предложение, за параметрите на информационните системи, които са им нужни. Липсата на ясна и подробна идея води до риск посоченият индикативен бюджет да се окаже недостатъчен. В общия случай приложените към проектното предложение индикативни оферти / пазарни консултации / са формални;

- често не е предвидено използване на споделените ресурси на електронното управление (напр. ДХЧО), както и липсва аргументация за предвидените разходи за закупуване на хардуерни ресурси и за поддръжка;

- при проектни предложения, различни от тези в Пътната карта, липсват проучвания, дали няма вече готови софтуерни решения, които могат да бъдат използвани, вместо да се разработват нови информационни системи.

- планира се „на парче“, без да е направена оценка за необходимият обмен на данни с други съществуващи системи в администрацията;

- липсва информация относно прилагането на подхода за оценка на всички разходи, свързани с избраното решение (TCO – Total Cost of Ownership).

3 Контрол за спазване на задължителните изисквания при изготвяне на технически спецификации

Дейността по удостоверяване на съответствие на технически спецификации с изискванията на чл. 58а от ЗЕУ е разписана в Правилата за удостоверяване на съответствието на технически спецификации за провеждане на обществени поръчки за разработка, надграждане или внедряване на информационни системи, вкл. интернет страници, мобилни приложения, софтуерни компоненти или електронни услуги.

При удостоверяване на съответствието с изискванията на чл. 58а от ЗЕУ и интеграцията с хоризонталните системи се отчитат спецификите и особеностите на съответните информационни системи и приложимостта на всяка една хоризонтална система при всяка една спецификация.

В обхвата на проверките по чл. 58а по реда на чл. 58б от ЗЕУ не попадат технически задания с обект доставка на оборудване (хардуерно и мрежово, включително компютърна техника), както и софтуерни лицензи. Извън обхвата на задължителните проверки са и технически спецификации за провеждане на обществени поръчки с прогнозна стойност под стойността по прага по чл. 20, ал. 4, т. 2 от Закона за обществените поръчки (70 000 лв. без ДДС).

Подаването на информация за произнасяне по реда на чл. 58б от ЗЕУ се осъществява задължително само чрез Регистъра на проектите, модул „Технически спецификации“.

Общият брой на проверените за съответствие с изискванията на чл. 58а от ЗЕУ технически спецификации за 2021 г. е 76, като 24% от тях са подлежали на редакции и корекции с цел привеждането им в съответствие с изискванията на чл. 58а от ЗЕУ. Има издадени и десет решения за отказ за удостоверяване на съответствието с изискванията на чл. 58а от ЗЕУ (за 13% от представените спецификации, съответните субекти по ЗЕУ не са се съобразили с дадените задължителни препоръките).

Най-често допусканите пропуски при изготвянето и изпращането на технически спецификации за удостоверяване на съответствието с изискванията на чл. 58а от ЗЕУ са:

- липсват някои от изискванията, заложени в Правилата за удостоверяване на съответствието на техническите спецификации, тъй като администрациите не са взели предвид актуалните Правила при изготвяне на спецификацията, например:

  - електронните административни услуги (ЕАУ) да се заявяват през Единния портал за достъп до ЕАУ чрез хоризонталната система за е-форми и съгласно Единния модел за заявяване, заплащане и предоставяне на ЕАУ;

  - изискванията за задължително наличие и използване на програмни интерфейси, изискуемите метаданни и атрибути за версия, достъпност за стари версии - минимум 24 месеца след публикуване на нова версия и други, съгласно формализираните описания в чл. 14 и чл. 41 от НОИИСРЕАУ;

  - унифициране на данните, които се вписват в регистъра на информационните обекти, съгласно формализираните описания в чл. 17, ал. 3 от НОИИСРЕАУ;

  - достъпността на Интернет страници и мобилни приложения, съгласно хармонизирания стандарт EN 301 549 V2.1.2 (2018-08);

- изискванията по отношение на мрежовата и информационна сигурност съгласно НМИМИС;

- не е представена аргументация на избраната прогнозна стойност, представената аргументация е грешна или не е актуална. Често срещана практика е да се представят спецификации за утвърждаване без прогнозната стойност на обществената поръчка да е предварително съгласувана като целесъобразна, в рамките на процедурата по чл. 7г, ал. 2 от ЗЕУ;

- неправилно е определен типа на техническата спецификация при започване на процеса по вписване на данни в модул „Технически спецификации“ на Регистъра на проектите. В следствие на това не са включени задължителни изисквания за дадения тип или са включени изисквания, които са неприложими към конкретната спецификация;

- изискването за предоставяне на отворени данни и интеграция с Портала за отворени данни често се определя като неприложимо от администрациите и не се включва в техническата спецификация, без тази липса да е аргументирана;

- често не е предвидено използване на споделените ресурси на електронното управление (напр. хоризонтални системи като е-Автентикация, е-Връчване, е-Плащане, RegiX и др.).

4 Контрол осъществяван върху лицата по чл. 1, ал. 1 и 2 от ЗЕУ и по Глава втора „Мрежова информационна сигурност“ от ЗКС

Едно от основните правомощия на ДАЕУ[14] е осъществяването на контрол по спазване на изискванията на ЗЕУ, ЗКС и подзаконовите нормативни актове за прилагането им. Контролът се осъществява чрез извършване на проверки.

В изпълнение на това всяка календарна година се разработва и утвърждава от председателя на ДАЕУ програма за извършване на проверки, с разчет в рамките на пет годишен период всички администрации да бъдат проверени. В програмата с приоритет се залагат за проверка администрации, според броя на предлаганите административни услуги и числеността им. В допълнение се извършват проверки при постъпил сигнал или след самосезиране на база публична информация. Обект на проверките са всички субекти попадащи в обхвата на ЗЕУ и ЗКС.

След обявяване на извънредното положение и извънредната епидемична обстановка, проверките се извършват дистанционно, без посещение на място. Беше създадена организация и бяха положени много усилия това да не доведе до понижаване на качеството на проверките. Осъществените през 2021 г. планови проверки са 115, а по сигнал – 8. В резултат от тях са изготвени: 90 протокола със задължителни предписания по ЗЕУ, 14 констативни протоколи, при които не са установени нарушения по ЗЕУ, 65 констативни протокола след изпълнени задължителни предписания и 22 доклада от проверки по ЗКС. Съставени са 11 бр. актове за установяване на административни нарушения и са издадени 10 бр. наказателни постановления.

Най-честите нарушения и пропуски при изпълнение на изискванията на ЗЕУ са както следва:

- административните органи, лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги изискват от гражданите и организациите

[14] С обнародването на ЗИД на ЗЕУ, ДВ, бр. 15 от 22.02.2022г. Държавна агенция „Електронно управление“ към Министерския съвет се закрива. Правомощията на Председателя на ДАЕУ се поемат от Министъра на електронното управление.

представянето или доказването на вече събрани или създадени данни, вместо да ги съберат служебно от първичния администратор на данните;

- много от административните органи не обявяват услугите си за вътрешно административни, с което негласно отказват предоставянето на вече събрани или създадени данни;

- административните органи не предоставят всички услуги в рамките на своята компетентност по електронен път;

- административните органи, главно общински администрации, не съгласуват с председателя на ДАЕУ разходите в областта на електронното управление и за използваните от тях информационни и комуникационни системи;

- информацията за електронните административни услуги е непълна, неясна, разхвърляна в различни рубрики на официалните интернет сайтове, като много често има разминаване на информацията и броя на услугите, вписана в административния регистър и публикуваната на официалните интернет сайтове;

- доставчиците на ЕАУ не изпращат потвърждение за получаването на входящ електронен документ или отказват регистрирането му без да уведомят подателя за причините;

- в много от администрациите не се извършва цялостен електронен обмен на документи, трудно се борави с електронни документи и служителите нямат квалифицирани електронни подписи;

- входящите електронни документи се разпечатват, ръчно им се поставя щемпел и се регистрират, слагат се резолюции и становища на хартиените копия и впоследствие се въвеждат в АИС, и обратно – изходящите документи се изготвят, съгласуват и подписват на хартия, поставя им се щемпел и се регистрират, след което се сканират и изпращат във формат PDF или JPEG, без в документа да има електронен подпис;

- за официалните интернет сайтове и пощенски сървъри се използват домейни, различни от „bg“ – „com“, „org“, „info“, „net“ и др.;

- освен e-mail адреси от официалните домейни на администрациите за контакти се обявяват адреси от доставчици на безплатна web-базирана електронна поща – например, но не само gmail.com, yahoo.com, abv.bg, mail.bg и др.;

- не се спазват правилата за институционална идентичност;

- в много от администрациите вътрешнонормативните документи, касаещи административните/електронните административни услуги и документооборота/електронния документооборот, са разработени в периода 2014-2015 г. и от тогава не са актуализирани.

Най-честите нарушения и пропуски при изпълнение на изискванията на ЗКС са както следва:

- в голяма част от администрациите няма изградена комплексна система от мерки за управление на мрежовата и информационна сигурност;

- в голяма част от администрациите не е определен служител или административно звено, отговарящ за мрежовата и информационната сигурност, който да е на пряко подчинение на административния орган и не са определени отговорници за териториалните звена;

- в голяма част от администрациите вътрешните правила, политики, процедури, инструкции и други документи, касаещи мрежовата и информационна сигурност, ако са разработени, не се преразглеждат минимум веднъж годишно и не се актуализират;

- в по-голяма част от администрациите изготвените документи и предприетите действия касаят основно информационните и комуникационните системи, а не всички информационни активи;

- в по-голяма част от администрациите не са идентифицирани информационните активи, различни от информационните и комуникационните системи, и съответно за неидентифицираните активи не са определени отговорници, не се анализира, оценява и управлява риска;

- в голяма част от администрациите няма разработени правила за класификация на информацията и ако има – те касаят само документите от системата за управление за мрежова и информационна сигурност, а не цялата информация на администрацията;

- в по-голяма част от администрациите не се договарят достатъчно подробно изисквания за мрежова и информационна сигурност при установяване на взаимоотношения с доставчици на стоки и услуги, наречени „трети страни“;

- при голяма част от администрациите се установява липсата на извършен анализ и оценка на риска, по методика, която да гарантира съизмерими, относително обективни и повтарящи се резултати.

Основна причина за нарушенията и пропуските в дейността на администрациите е ненавременното актуализиране на вътрешноведомствените актове съобразно изискванията на актуалните текстове на ЗЕУ, ЗКС и подзаконовите нормативни актове за прилагането им, което от своя страна води до реалното им неизпълнение.

VII. СЪЩЕСТВУВАЩИ ОГРАНИЧЕНИЯ ПРИ ИЗТОЧНИЦИТЕ НА ИНФОРМАЦИЯ

1 Интегрирана информационна система на държавната администрация

Към момента по отношение на ИИСДА са идентифицирани редица проблеми и пропуски, които силно ограничават целесъобразността на системата и пълнотата на данните в нея:

- липса на адекватна структура при представянето на администрациите. Повечето административни органи не вписват всички обстоятелства съгласно Наредбата за Административния регистър за техните администрации. Съществува възможност за самостоятелно вписване на звена, които сами по себе си не са административни органи (например отделни дирекции в министерства), което поражда проблеми при автоматизираното получаване на информация за ключови информационни системи, респективно води до изкривяване на анализите и изводите;

- справките, които ИИСДА предоставя, са тромави за използване, без да позволяват обработка. Информацията, която се генерира, често не подлежи на анализ или не е с необходимото ниво на детайл;

- много администрации, предимно общини, не вписват пълния набор от административни услуги, които предоставят;

- многократно вписване на еднотипни услуги. Едни и същи услуги (предимно предоставяни от областни администрации и общини) се вписват от всички администрации, които ги предоставят, и се отчитат от ИИСДА като отделни услуги. Това силно изкривява информацията за броя на предоставяните административни услуги;

- липса на информация за средствата за електронна идентификация, които се използват при заявяване на ЕАУ и тяхното ниво на осигуреност. Със ЗЕУ се въвежда изискването за вписване в Административния регистър на информация за средствата за електронна идентификация и електронните образци за заявяване на ЕАУ. Във връзка с тези разпоредби е утвърдена Методика за определяне от лицата по чл. 1, ал. 1 и 2 от ЗЕУ на средствата за електронна идентификация, които се използват при заявяване на ЕАУ и тяхното ниво на осигуреност, която следва да бъде прилагана от всички администрации, които предоставят ЕАУ;

- липса на информация относно свързани услуги като например информация кои други администрации изискват акта, издаден в резултат от услугата, кои са потребителите на услугата и др.

Предвид ролята на ИИСДА за процесите в администрацията, във връзка с посочените ограничения, е необходимо своевременно предприемане на адекватни мерки за преодоляването им. Ключовият характер на тази система не предполага дългия период на липса на развитието и надграждането ѝ – над 5 години.

В ИИСДА е интегрирана Информационната система за попълване на отчетите за дейността и състоянието на администрацията (ИСПОДСА), която служи основно за създаването на Годишния доклад за състоянието на администрацията. Информацията в системата се подава от администрациите отново чрез попълване на въпросници. По този начин е формирана единна входна точка за подаване на информация, но липсва възможност администрациите да създават своите въпросници на това място, като те да са достъпни за попълване от съответните компетентни органи.

2 Регистър на информационните ресурси

Административните органи са длъжни да вписват в РИР данните за информационните си ресурси в едномесечен срок от въвеждането, съответно от извеждането им от експлоатация. Въпреки това, се наблюдава тенденцията много от тях да не въвеждат своите новопридобити активи в срок или своевременно да актуализират информацията за тях, като липсата на тази информация дава грешна картина за състоянието на ресурсите, с които разполагат. Това обстоятелство се явява и съществен проблем при планирането и контрола на средствата за ИКТ и електронно управление.

Основната роля на РИР е регистърът да служи като инструмент за планиране развитието на информационните ресурси в администрацията, но тази негова функция не може да бъде реализирана поради недобро качество на данните в него, както и липсата на достатъчно функционалности за целта. Това, от своя страна, се дължи на липсата на адекватни контроли и номенклатури при въвеждане на информацията, което позволява полета със задължителен характер да бъдат попълвани с произволни данни.

Регистърът функционира като самостоятелна система, която има ограничена интеграция с ключовата за контрола на разходите за електронно управление Информационна система за бюджетен контрол единствено в частта за годишно планиране на ресурсите. Взаимното обвързване на РИР и ИСБК има потенциала за доведе до значително опростяване на взаимосвързаните процеси по планиране, бюджетиране и разходване на средства за обновяване и поддръжка на ИР на административните органи.

Практиката за събиране на информация при изготвяне на доклади и отчети и чрез въпросници, макар и доказана във времето, създава риск от дублиране, произволно попълване и ненавременно получаване на информацията.

VIII. ГОДИШЕН ПЛАН ЗА РАЗВИТИЕ И ОБНОВЯВАНЕ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ В АДМИНИСТРАЦИЯТА И ИНФОРМАЦИОННИТЕ РЕСУРСИ НА ЕДИННАТА ЕЛЕКТРОННА СЪОБЩИТЕЛНА МРЕЖА НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ И ЗА НУЖДИТЕ НА НАЦИОНАЛНАТА СИГУРНОСТ

През 2021 г. се отчита предприемането на по-директен подход към прилагането на нормативните изисквания на Закона за електронно управление и по-специфично чл. 55 от НОИИСРЕАУ, при който административните органи нямат право да подават информация за планирани разходи за разработване или надграждане на информационни системи без преди това да са въвели нормативно определените планове за обновяване на ИКТ ресурси – хардуерен и мрежови информационен ресурс, софтуер (ИС) и лицензиран софтуерен продукт в Регистъра на информационните ресурси.

Към 31.12.2021 г. 385 административни органа са въвели общо 8 611 записа в раздел Годишен план. В съответствие с нормативните изисквания на чл. 55 от НОИИСРЕАУ, по-голямата част от тях са създали записи по групи ИКТ ресурси, разпределяйки своите планирани разходи на такива за хардуерни устройства, за закупуване или подновяване на лицензни споразумения, и за разработка на информационни системи. Някои административни органи са приели по-директен подход при оценката на нуждите си от допълнителни ИКТ активи или идентифицирането на тези, които подлежат на замяна, поради което са генерирали индивидуални планове за обновяване на съответните активи, предимно хардуерни. Средствата, необходими за обновяване на съответните ИКТ ресурси на административните органи, са разчетени в рамките на одобрените бюджети на заинтересованите първостепенни разпоредители с бюджет за съответната година.

Според въведените в РИР стойности, общата сума от необходими за обновяване на ИКТ ресурси средства за текущия четиригодишен период възлиза на 905 018 677 лева. Разпределението съответно за 2021 г., 2022 г., 2023 г. и 2024 г. може да се види на следната фигура:

Фигура 22. *Планирани средства за обновяване на ИКТ ресурси*

267 административни органа са въвели 1874 записа в раздел Годишен план в РИР за 2022 г. Бройките Годишни планове за обновяване са разпределени по следния начин: 58,43 % от тях са на централната, специализираната териториална и областната администрация, а

41,57 % - на общинските администрации. Съответно и планираните средства за обновяване са на стойност 285 700 649 лв., като по-голямата част от тях - 96,96 % - в централната, специализираната териториална и областната администрация, а едва 3,04 %- в общински администрации.

Годишните планове за 2022 г. за група „хардуерен и мрежови информационен ресурс“ са на стойност 169 177 006 лв. 95,31 % от тази сума е заложена от централната, специализираната териториална и областната администрация, а едва 4.69 % - от общинските администрации.

Планираните средства за 2022 г. за група „софтуер“ са на стойност 112 429 865 лв. 111 974 018 лв. (99,59 %) са заложени от централната, специализираната териториална и областната администрация, а едва 455 847 лв. (0.41 %) са заложени от общинските администрации.

От планираните за 2022 г. средства за група „лицензи“ – 4 093 778 лв., почти цялата сума е заложена от централната, специализираната териториална и областната администрация. Едва 0.92 % от сумата представлява прогнозите на общинските администрации.

Демонстрираната по-горе явна асиметричност на разходите (с минимални дялове на брой записи и планирани суми) в общинските администрации се обуславя от факта, че въпреки че броят общински администрации представлява около 45% от общия брой административни органи, в тях работят значително по-малък брой служители и те използват в пъти по-малко устройства и програмни продукти в работата си, за разлика от териториалните звена на някои централни администрации, като НАП, министерствата и техните второстепенни разпоредители с бюджет и пр.

Въпреки наличната в РИР информация относно плановете за развитие на информационните ресурси, не съществува инструментариум за проследяване на реалните нужди на администрациите от ИКТ. Планираните обновления трябва да бъдат базирани на обосновки относно наличната в Регистъра информация за активите на всяко ведомство. От тази гледна точка през 2022 г. ще бъде наблегнато на проверки за спазване на изискванията на чл. 7е от ЗЕУ като основна предпоставка за прозрачността и ефективността на разходите за ИКТ и електронно управление. Като необходима стъпка се предвижда реализирането на механизъм, които да гарантира, че разходваните средства обезпечават реална необходимост, включително дефиниране на показатели за измерване на резултатите (KPI) и прилагане на добри практики описани в процесите по управление на ИКТ активи. Данните от РИР и ИИСДА следва да подпомагат използването на бюджетни инструменти за наблюдение и автоматизиране на отчетността, свързана с ИКТ и ресурсите за електронно управление.

Използваният софтуер и хардуер в администрацията следва да покрива дейностите, които извършва всяко ведомство според своите компетенции. Въпреки това има обичайни дейности, които изискват еднакви ресурси. От тази гледна точка е необходимо да бъде разработен Национален стандарт за видовете и типовете софтуер и хардуер, които се използват в администрацията.

През 2022 г. е предвидено изпълнението на 13 проекта, свързани за разработването и/или надграждането на следните информационни системи и регистри:

- „Надграждане на Търговския регистър за интеграция с платформата за обмен на данни между Търговските регистри в ЕС, вграждане на регистъра на юридическите лица с нестопанска цел, интеграция с имотния регистър, единна входна точка и прехвърляне на централния регистър на особените залози“, Агенция по вписванията;
- Развитие на информационната система и публичния регистър на Комисията за защита на конкуренцията“, Комисията за защита на конкуренцията;

- „Дигитализация на архива на недвижимите културни ценности от световно и национално значение, изграждане на специализирана информационна система, електронен регистър и публичен портал“ – Министерство на културата

- „Разработване и внедряване на електронна информационна система "Национален регистър на запорите“, Министерство на правосъдието;

- „Реализиране на Национален регистър на пълномощните“, Министерство на правосъдието;

- „Изграждане на система за управление на собствеността, включително единен регистър на държавната и общинската собственост“, Министерство на регионалното развитие и благоустройството

- „Изграждане на Единен публичен регистър по устройствено планиране на територията, инвестиционно проектиране и разрешаване на строителството и информационна система за неговото обслужване“, Министерство на регионалното развитие и благоустройството;

- „Оптимизация и електронизация на регистрите и работните процеси в БАБХ“, Българска агенция по безопасност на храните;

- „Разработване и прилагане на Референтна архитектура за оперативна съвместимост (РАОС) и на Информационна система за централизирано изграждане и поддържане на регистри (ИСЦИПР)“, Държавна агенция „Електронно управление“;

- „Създаване, надграждане и обединяване на електронни регистри на Националния център за информация и документация (НАЦИД) в областта на висшето образование“, Национален център за информация и документация;

- „Е - Натура 2000 - развитие на Единната информационна система за НАТУРА 2000“, Министерство на околната среда и водите;

- „Електронна система за управление работата на администрацията на омбудсмана“ - Омбудсман на Р България;

- „Надграждане на основните системи на Агенция „Митници“ за предоставяне на данни и услуги – БИМИС 2020 (фаза 3)“, Агенция „Митници“, включващо:

  - Развитие и въвеждане на Институционална архитектура на АМ по отношение на Проект по МКС: Подобряване на новата компютризирана система за транзит (NCTS) етап 5 (1.7 UCC Transit system including NCTS – phase 5) върху Cloud архитектура;

  - Развитие и въвеждане на Институционална архитектура на АМ по отношение на Проект по МКС: Система за контрол на вноса (СКВ 2) версия 2 (1.19 UCC – Import Control System 2 (ICS 2 release 2), вкл и Проект по МКС: Уведомление за пристигане (2.1 UCC Notifications of arrival) върху Cloud архитектура;

  - Развитие и въвеждане на Институционална архитектура на АМ по отношение на модул „Анализ на риска“ (МАР) – отразяване на промените, произтичащи от Система за контрол на вноса (СКВ 2) версия 2 (реализирана в изпълнение на проекти по МКС: 1.19 UCC – Import Control System 2 (ICS2 Release 2) и 2.1 UCC Notifications of arrival), Митническа автоматизирана система за изнасяне (МАСИ) (реализирана в изпълнение на проекти по МКС: 1.6 UCC Automated Export System (AES) и 2.6 UCC Special procedures harmonisation (EXP)) и Митническата информационна система за транзит (МИСТ2) (реализирана в

изпълнение на проект по МКС: 1.7 UCC Transit system including NCTS – phase 5), върху Cloud архитектура.“.

Въз основа на анализа и на данните от отчета ясно могат да бъдат очертани следните стъпки, които следва да бъдат предприети през 2022 г. по отношение на развитието на информационните ресурси в административните органи:

1 Да се изготви нов стратегически документ за развитие на електронното управление, информационните технологии и информационното общество с хоризонт на действие 2030 г., включително на нови механизми за наблюдение и оценка на изпълнението на целите и дейностите в него.

2 Да се актуализира и разшири Архитектурата на електронното управление, с включване на допълнителни процеси, извън основния процес за предоставяне на ЕАУ.

3 Да се разработят проекти на архитектури по области на политики, които да описват функционалните, системни и технологични елементи на е-управлението в съответните сектори и взаимовръзките с останалите сектори на държавно управление.

4 Да се разработи самата политика за развитие на информационните ресурси, съобразена и допълнена със съответните правила, стандарти и процедури за развитие и управление на ИР, както и да бъдат разработени методически указания към администрациите по изпълнението ѝ.

5 Административните органи да заложат в бюджетите си ресурс за обновяване на хардуер с изчерпан жизнен цикъл.

6 Да бъдат свалени от експлоатация на ИР, които съставляват риск за мрежовата и информационна сигурност.

7 Да бъдат надградени РИР и ИИСДА, както и ЦАИС ЕОП, с оглед на получаване на необходимата актуална и достоверна информация за ИР.

8 Да бъде разширено използването на осигурената възможност за плащане по електронен път – административните органи да променят вътрешните си работни процеси за използване на ЦВПОС.

9 Да бъдат осигурени стимули за увеличаване на използването на ЕАУ, например чрез намаляване на таксите за предоставяне на услуги по електронен път.

10 Министерството на електронното управление да осъществи засилени проверки за предоставяне на АУ по електронен път, с фокус върху най-често използвани услуги.

11 Да бъде проведена разяснителна кампания за ползите от използване на ДХЧО.

12 Да бъдат предприети действия по засилване на мерките за осигуряване на високо ниво на мрежова и информационна сигурност и за изпълнение на нормативните изисквания, включително чрез санкции при неизпълнение.

13 Да бъде разработена единна политика за човешките ресурси в областта на ИКТ в държавната администрация.

14 Да бъдат преосмислени механизмите за финансиране на дейности за е-управление и ИКТ.

15 Да бъдат засилени проверките от страна на МЕУ по ЗЕУ и ЗКС и контролът в процеса на утвърждаване на проектни предложения/дейности и контролът за спазване на задължителните изисквания при изготвяне на технически спецификации.

16 Да бъдат предприети действия за преминаване съм оценка на бюджетите на проектитните предложения на принципа TCO – Total Cost of Ownership.

17 Да бъдат въведени проверки за съответствие със ЗЕУ на поръчки за готови софтуерни продукти (напр. системи за документооборот).

IX. ИЗВОДИ

Продължава повишаването на използваемостта на хоризонталните и централизирани системи на електронното управление. Особено отличителен ръст бележи Единният портал за достъп до електронни административни услуги (ЕПДЕАУ), в който през 2021 година са реализирани 462 нови електронни административни услуги за централизирано заявяване – над 8 пъти повече в сравнение с 2020 г.

Според данните в ИИСДА през отчетния период продължава тенденцията на нарастване на броя на услугите от ниво 3 (заявяване и получаване на услуги по електронен път) и ниво 4 (заявяване и получаване на услуги по електронен път, вкл. онлайн разплащане), като за първи път се отчита превес на услугите от ниво 4. Качеството на данните обаче прави трудно извличането на точния брой реализирани на практика услуги на тези нива.

Все още не е изградена националната схема за електронна идентификация, предвидена в Закона за електронната идентификация, което допринася за забавяне развитието на е-управлението и в определена степен ограничава достъпа на гражданите и бизнеса до електронни административни услуги, в т.ч. и трансгранични такива. Необходимо е инициирането на промяна в Административния регистър с оглед вписването на средствата на електронна идентификация и тяхното ниво на осигуреност в специално създадено за целта поле.

Над 200 регистъра продължават да подлежат на електронизация, което затруднява и пълноценното използване на централизираните и хоризонталните системи на електронното управление.

Продължава развитието на Държавния хибриден частен облак (ДХЧО). През 2021 г. с над 20%, до 39 е нараснал броят на администрациите, използващи ДХЧО, а още 35 администрации подготвят информационни системи за миграция към ДХЧО. Необходими са допълнителни усилилия за привличането на ключови администрации за използването на хранилището за данни на електронното управление.

В областта на мрежовата и информационна сигурност нормативната база е добре развита, но остава проблемът с нейното прилагане от административните органи. Над половината от тях не са провели вътрешен одит на МИС, а при близо 40% липсва анализ и оценка на рисковете за информационната сигурност.

Леко нараства относителният дял на инцидентите със значително увреждащо въздействие в мрежовата и информационната сигурност с висока степен на опасност. Най-голям е процентът на регистрираните инциденти, дължащи се на зловреден код (malware), следвани от измама (phishing). Извънредната ситуация, породена от COVID-19, промени изцяло стила на работа на всички, което наложи използването на допълнителни мерки за сигурност и защита от кибератаки. Увеличиха се драстично фишинг сайтовете, свързани с COVID-19, и използването на уязвимости в софтуерите за организиране и провеждане на онлайн срещи и обучение, както и в софтуерите за отдалечен достъп. В много случаи това е използвано за разпространение на злонамерен софтуер от типа „рансъмуер“ и кражба на данни, което доведе до сериозни проблеми в работата на администрациите. Наблюдава се връщане към позабравени рансъмуери и активиране на вече използвани ботнети. Използването на ZeroDay и непачнати уязвимости се превърна в най-често използвания инструмент в ръцете на атакуващите.

В областта на човешките ресурси в ИКТ е необходимо разработването на единна политика за човешките ресурси за същите в държавната администрация. Установените процедури за координация и контрол на разходите, проектите и дейностите за електронно управление и за задължителен предварителен контрол на всички технически спецификации

за провеждане на обществени поръчки за изграждане на информационни системи функционират ефективно.

Анализът на данните в Информационната система за извършване на предварителен, текущ и последващ контрол по целесъобразност в областта на електронното управление и използването на информационните и комуникационните технологии показва тенденция да се използват по-малко от 60% от утвърдените целеви разходи за е-управление и ИКТ. В допълнение, анализът на бюджетните процеси в областта на електронното управление разкрива наличието на някои предизвикателства, които ограничават способността да се отдава приоритетно значение на проекти с по-голяма възвръщаемост.

ЗАКЛЮЧЕНИЕ

Развитието на електронното управление изисква продължаване на целенасочената политика за постигане на оперативна съвместимост и системна интеграция на информационните ресурси на администрациите при устойчив модел за дългосрочно е-управление. Въпреки постигнатия напредък, още много работа предстои в полето на достъпността и използваемостта на електронните услуги. Капацитетът на споделените ресурси на е-управлението също все още не се използва достатъчно интензивно.

Схемата за електронна идентификация, предвидена в Закона за електронната идентификация, все още не е изградена, което забавя развитието на електронното управление и ограничава достъпа на гражданите и бизнеса до електронни административни услуги.

Всички направени изводи се основават на данните от основните източници на информация за състоянието на информационните ресурси – ИИСДА и РИР, където се наблюдават непълноти, разминавания и слабости при попълването или наличните функционалности. Това от своя страна ограничава възможността да бъде направени пълна и точна оценка на състоянието на отделните видове информационни ресурси. Проблемите с данните относно ИР са констатирани вече в няколко последователни отчета за състоянието и развитието на ИР и през 2022 г. следва да се работи по тяхното отстраняване.

Приложение № 1:

Брой служители, регистрирани в РИР към 31.12.2021 г. .

Вид администрация на изпълнителната власт	Вид административна структура	Брой служители
Териториална администрация	Общинска администрация	7199
Централна администрация	Адм.структура, създадена с нормативен акт, която има функции във връзка с осъществяването на изпълнителната власт	3624
Централна администрация	Изпълнителна агенция	3244
Териториална администрация	Специализирана териториална администрация, създадена като юридическо лице с нормативен акт	1784
Териториална администрация	Общинска администрация на район	655
Централна администрация	Министерство	442
Централна администрация	Държавна агенция	401
Териториална администрация	Областна администрация	388
Централна администрация	Адм. структура по чл. 60 от закона за администрацията	106
Централна администрация	Администрация на държавна комисия	102
Централна администрация	Администрация на Министерски съвет	5
Администрация отчитаща дейността си пред Народното събрание	Административна структура създадена със закон	1

Приложение № 2:

Най-често заявявани централизирано услуги през 2021 г.

Номер и наименование на услуга	**Администрация предоставящ услугата**	**Брой заявявания**
1168 Приемане на заявления и регистрация на търсещи работа лица	Агенция по заетостта	3 626
3121 Отпускане на еднократна помощ за ученици, записани в осми клас	Агенция за социално подпомагане	2 619
649 Отпускане на месечни помощи за дете до завършване на средно образование, но не повече от 20-годишна възраст по реда на ПП на ЗСПД	Агенция за социално подпомагане	2 551
778 Отпускане на еднократна помощ за ученици, записани в първи клас	Агенция за социално подпомагане	2 328
3123 Отпускане на месечна целева помощ при обявено извънредно положение или обявена извънредна епидемична обстановка	Агенция за социално подпомагане	2 185
2198 Освобождаване на лица от винетни такси при ползване на републиканските пътища	Агенция за социално подпомагане	2 165
2396 Издаване на удостоверение за данъчна оценка на недвижим имот и за незавършено строителство	Общински администрации	1 805

Приложение № 3:

Администрации и лица по чл. 1., ал. 2 от ЗЕУ

с най-голям брой системи, присъединени към RegiX

Консуматор	Брой системи	% системи
Държавна агенция „Електронно управление“	10	12
Национален статистически институт	10	12
Изпълнителна агенция "Автомобилна администрация"	6	7
Министерство на външните работи	6	7
Агенция "Митници"	6	7
Агенция по заетостта	4	5
Министерство на правосъдието	4	5
Община Пловдив	4	5
Агенция по вписванията	3	4
Изпълнителна агенция по рибарство и аквакултури	3	4
Министерство на туризма	3	4
Районен съд -Поморие	3	4
Столична община	3	4
Агенция "Пътна инфраструктура"	2	2
Агенция за устойчиво енергийно развитие	2	2
Администрация на Министерски съвет	2	2
Изпълнителна агенция по околна среда	2	2
Министерство на здравеопазването	2	2
Министерство на земеделието	2	2
Министерство на образованието и науката	2	2
Министерство на труда и социалната политика	2	2
Национален център за информация и документация	2	2
Национална агенция за приходите	2	2