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 2023 г.

СЪДЪРЖАНИЕ

СЪДЪРЖАНИЕ ... 2
СЪКРАЩЕНИЯ ... 3
I. ВЪВЕДЕНИЕ ... 5
II. СТРАТЕГИЧЕСКА РАМКА ЗА РАЗВИТИЕ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ ... 6
1. Стратегия за развитие на електронното управление в Република България 2019 – 2025 г. ... 6
2. Единна политика за информационните ресурси ... 6
3. Архитектура на електронното управление ... 6
4. Основни източници на информация за състоянието на информационните ресурси ... 7
5. Референтна архитектура за оперативна съвместимост ... 8
III. СЪСТОЯНИЕ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ В АДМИНИСТРАЦИЯТА ... 8
1. Обезпеченост на администрациите с хардуер ... 9
2. Обезпеченост на администрациите със софтуер и лицензи ... 10
3. Информационни системи ... 10
3.1. Хоризонтални системи на електронното управление ... 11
3.1.1. Единен портал за достъп до електронни административни услуги (ЕПДЕАУ, egov.bg) ... 11
3.1.2. Система за електронна автентикация (е-Автентикация) ... 13
3.1.3. Система за електронно плащане (е-Плащане) ... 15
3.1.4. Система за проверка валидността на персонален цифров сертификат (е- Валидиране) ... 17
3.1.5. Система за управление на електронни форми (е-Форми) ... 17
3.1.6. Система за сигурно електронно връчване (ССЕВ, е-Връчване) ... 18
3.2. Централизирани системи за е-управление ... 20
3.2.1 Среда за междурегистров обмен на данни ... 20
3.3. Информационни системи в администрациите ... 23
4. Електронна идентификация ... 24
4.1. Електронна идентификация за нуждите на заявяване на ЕАУ ... 24
4.2. Трансгранична електронна идентификация ... 24
5. Регистри, поддържани от администрацията ... 26
6. Споделени информационни ресурси ... 26
6.1. Държавен хибриден частен облак (ДХЧО) ... 26
6.2. Единна електронна съобщителна мрежа (ЕЕСМ) ... 30
6.3. Хранилище за данни на електронното управление ... 32
7. Предоставяне на електронни административни услуги ... 33
7.1 Състояние на електронните административни услуги ... 33
7.2 Осигуряване на институционална идентичност и достъпност на уебсайтовете ... 34
IV. УКРЕПВАНЕ НА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ ... 37
1 Състояние на мрежовата и информационната сигурност ... 37
2 Мерки за повишаване нивото на мрежовата и информационната сигурност ... 41
2.1. Нормативна уредба ... 41
2.2. Национален координационен център ... 42
2.3. Национален екип за реакция на инциденти в компютърната сигурност ... 43
V. ЧОВЕШКИ РЕСУРС В ИКТ ... 44
VI. КОНТРОЛ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ ... 46
1 Контрол в рамките на бюджетния процес на разходите за е-управление и ИКТ ... 46
2 Контрол в процеса на утвърждаване на проектни предложения/дейности ... 47
3 Контрол за спазване на задължителните изисквания при изготвяне на технически спецификации ... 48
4 Контрол осъществяван върху лицата по чл. 1, ал. 1 и 2 от ЗЕУ и по Глава втора ... 50
VII. СЪЩЕСТВУВАЩИ ОГРАНИЧЕНИЯ ПРИ ИЗТОЧНИЦИТЕ НА ИНФОРМАЦИЯ ... 51
1 Интегрирана информационна система на държавната администрация ... 51
2 Регистър на информационните ресурси ... 52
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 ... 52
IX. ИЗВОДИ ... 55
ЗАКЛЮЧЕНИЕ ... 57

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“*
МЕУ	*Министерство на електронното управление“*
ДАНИИ	*Държавна агенция за научни изследвания и иновации*
ДХЧО	*Държавен хибриден частен облак*
ДЧ	*Държави членки*
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

Информационните ресурси на електронното управление се развиват като информационна и технологична екосистема, която се характеризира с балансираност, самостоятелност, разширяемост и устойчивост. 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.

Министерство на електронното управление (МЕУ) е отговорно за държавната политика в областта на ИР на електронното управление и има координираща роля в процесите по реализацията ѝ. Цифровите решения в услуга на гражданите и подобряването на бизнес средата са ключови европейски и национални приоритети. Необходимостта от ускоряването на цифровата трансформация и подобряване на свързаността през последните години се потвърди от развилата се ситуация с пандемията COVID-19, бързите промени в технологиите и не на последно място през изминалата година и икономическите условия в страната. Вследствие на всичко това през 2022 г. се забелязва повишаване на очакванията и изискванията на гражданите и бизнеса за устойчиво и надеждно електронно управление и защитен обмен на данни и информация 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.

Настоящият отчет представя информация относно състоянието на информационните ресурси (ИР) в администрациите за периода 01.01.2022 – 31.12.2022 г. През този период политиката за електронно управление и модернизация е изведена на най-високо държавно ниво. Създадено е Министерство на електронното управление и са извършени функционални и структурни промени, регламентирани в Устройствен правилник на МЕУ. Също така през 2022 г се създава и Изпълнителна агенция „Инфраструктура на електронното управление“, администрация към министъра на електронното управление за изпълнение на държавната политика в областта на електронното управление и на държавната политика в областта на мрежовата и информационната сигурност.

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

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 подход към „икономика на данни“, който цели 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, 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.

2. Единна политика за информационните ресурси

С РМС № 296 от 02.04.2021 г. 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).

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. 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.

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 повече от 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 2023 г.

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) и Регистъра на информационните ресурси (РИР).

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.

5. Референтна архитектура за оперативна съвместимост

През 2022 г. са разработени проекти на Референтна архитектура и Българска национална рамка за оперативна съвместимост, които пряко да допринесат за реализирането на целите на Европейската комисия за Единен цифров пазар.

Чрез Референтната архитектура и Националната рамка за оперативна съвместимост се постигат следните цели:

- Развитието на общество, ориентирано към услуги;
- Прозрачност на информацията, свързана с политическите решения по отношение на публичните информационни системи;
- Подпомагане съвместното развитие на услуги в публичния сектор;
- Създаване на условия за свободна конкуренция при разработка на ИКТ в администрацията;
- Намаляване и оптимизиране на разходите за ИТ в публичния сектор;
- Насърчаване и подкрепа при предоставянето на публични услуги в България чрез насърчаване на трансграничната, междусекторна и между отделните органи на администрацията оперативна съвместимост.

Разработени са и проекти на следните документи, които предстои да бъдат утвърдени:

- Стандарт за описание на информационни обекти;
- Предложения за нормативни изменения;
- Шаблони на споразумения за ниво на обслужване (SLA) в администрациите и други.

Референтната архитектура за оперативна съвместимост е разработена в съответствие с Европейската референтна архитектура EIRA, Европейската рамка за оперативна съвместимост, както и Българската рамка за оперативна съвместимост. Проектът за нейната разработка и планът за прилагане са от национално значение, тъй като изграждането и развитието на оперативно съвместими информационни системи в администрациите следва да бъде в съответствие с референтната архитектура за оперативна съвместимост.

Изготвен е „План за прилагане на РАОС“, съдържащ правила и отговорности за поддържане и прилагане на Българската референтна архитектура за оперативна съвместимост (РАОС) на централно ниво и локално от отделните административни органи. Идентифицирани са и са приоритизирани необходимите мерки/дейности, свързани с прилагането на РАОС, както по отношение на отделните администрации, така и по отношение на съвместно използваните ИТ ресурси. Изготвени са анализ на нормативната уредба и проекти на нормативни актове за регламентиране на прилагането на РАОС.

III. СЪСТОЯНИЕ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ В АДМИНИСТРАЦИЯТА

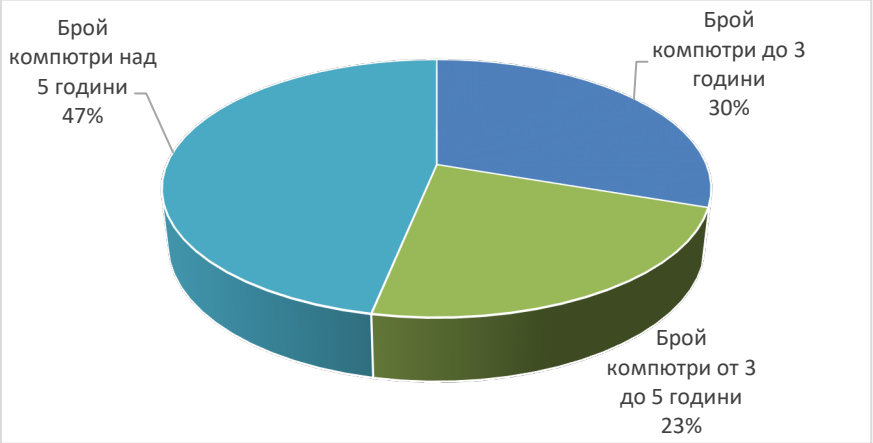
Съгласно чл. 55, ал. 1 от Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги (НОИИСРЕАУ), информационни ресурси са:

- хардуер, в т.ч. сървъри, настолни и мобилни компютри и устройства;

- мрежово оборудване;
- софтуер;
- софтуерни лицензи.

1. Обезпеченост на администрациите с хардуер

Към 31.12.2022 г. администрациите разполагат със 125 222 бр. работни станции, (спрямо 114 018 бр. към 31.12 2021 г.), като от тях 64% са в централната администрация и 29% - в териториалната администрация, а 7% са в администрации на отчет пред Народното събрание. Данните в ИИСДА показват, че 47% от работните станции са придобити преди повече от 5 г., а 23% са на възраст между 3 и 5 г., а 30 % са на възраст до 3 години. Тоест, почти 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 5 г.



Фигура 1. *Разпределение на работните станции по година на придобиване*

Разпределението на останалите видове активи, въведени в РИР е представено в таблица 1:

Вид актив	Брой	Стойност, лв.
Запаметяващи устройства	1 103	7 100 876
Поддържащи системи	7 671	17 802 628
Мрежово оборудване	12 624	44 746 194
Периферни устройства	105 372	83 531 182
Физически сървър	3 265	54 625 465
Стелажна система	1 682	9 016 141
Система за съхранение	373	21 043 949
Виртуална машина	668	467 657

Таблица 1. *Въведени активи в РИР*

За отчетния период, въведените в РИР данни показват намаление в обема на видовете хардуерни активи, като по-съществено намаление има при поддържащите системи - около 20 % (9 631 бр. през 2021 г.) и периферните устройства с 13 % (121 294 бр. през 2021 г.). Леко увеличение се наблюдава при стелажните системи.

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 ИИСДА данни за операционни системи на работни станции е видно, че над 30,04% 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. Най- често използваните системи за управление на бази данни са на Oracle – 61%. Поради липса на задължително поле за посочване на предназначение на софтуера, не може да бъде извлечена справка, която да даде пълни данни за използваните системи за управление на база данни (СУБД) в администрацията.

От инсталираните в администрациите сървъри за електронна поща и календар, осигуряващи лесно администриране и превенция срещу загубата на данни, 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 на административните органи в ИИДСА. Според наличната информация, най-използвани от администрациите са антивирусните решения на ESET, както и безплатен софтуер.

ESET Antivirus	*Panda Antivirus*	*F-Secure Business*	*Kaspersky Antivirus*	*Symantec Antivirus*	*Друг платен антивирусен софтуер*	*Безплатен антивирусен софтуер*
30,42%	*6,66%*	*8,56%*	*4,60%*	*3,80%*	*13%*	*45,96%*
192	*42*	*54*	*29*	*24*	*82*	*208*

Таблица 2. *Разпределение на антивирусния софтуер*

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.

Наблюдава се висок процент на желание от страна на администрациите за участие в процеса по развитие на електронното управление. Развитието на процесите на цифрова трансформация налагат администрацията да използва в дейността си актуални ИКТ решения.

3.1. Хоризонтални системи на електронното управление

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

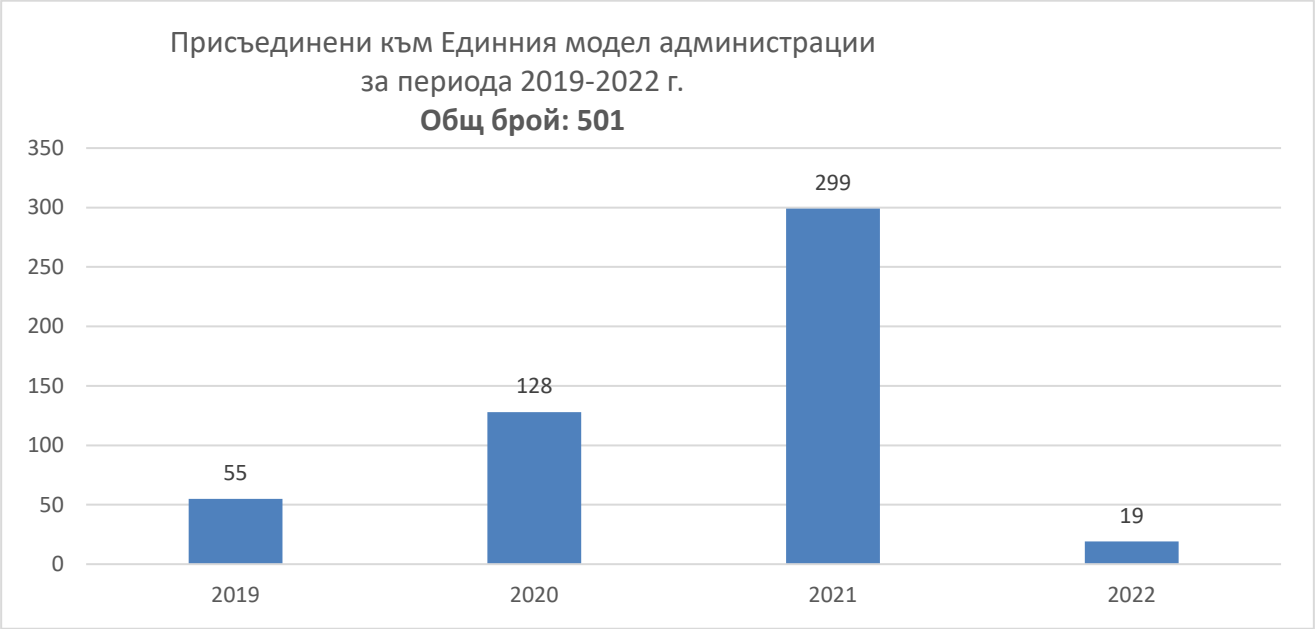
Единният портал за достъп до електронни административни услуги е реализиран като единна точка за достъп до ЕАУ. Към 31.12.2022 г. на портала е публикувана информация за 1 712 електронни услуги, от тях 1 132 ЕАУ са реализирани чрез централизирано и унифицирано заявяване. За заявяването им са разработени над 1 600 електронни форми на услугите и съпътстващите документи.

Като за 2022 година новите ЕАУ за централизирано заявяване, публикувани на ЕПДЕАУ са 272. Публикувана е и информация за 580 ЕАУ, предоставяни децентрализирано чрез разработени портали на администрациите - Министерство на вътрешните работи, Агенция по геодезия, картография и кадастър, Агенция „Митници“, НОИ, НАЦИД и др.



Фигура 2. Брой разработени услуги по години

В края на отчетния период централизирано се предоставят услугите на 501 администрации, от които 49 са централни, 302 общински и районни, 27 областни и 123 специализирани териториални администрации.

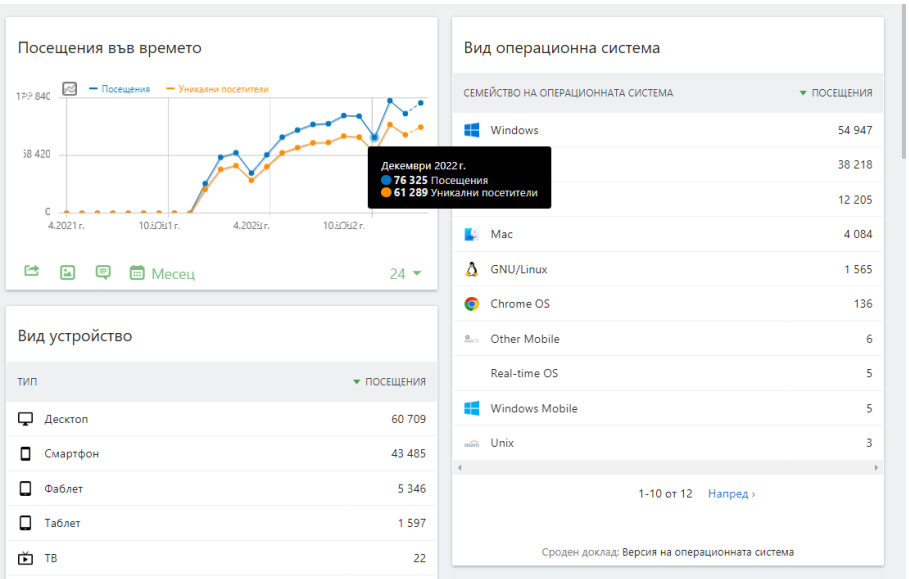


Фигура 3. *Брой присъединени към Единния модел администрации по години*

Осигурени са условия за всички областни, общински и районни администрации да предоставят техните услуги централизирано по Единния модел за заявяване, заплащане и предоставяне на ЕАУ. По модела централизирано се предоставят 21 услуги от областните администрации и 182 услуги от общини и техните райони.

Част от функционалността на портала е поддържането на работно пространство за граждани, бизнес и администрация, като за гражданите това е „Моето пространство“, чрез което може да се избира и достъпва с един клик специфична информация и да се достъпват най-често заявявани услугите от конкретното лице услуги. Поддържа се и централизиран профил за целите на електронното управление, в което се съхранява и актуализира специфична за лицето информация, като адреси за уведомяване, мобилни номера и др., вида на информацията може динамично да се разширява. Наличната в профилите информация е достъпна чрез уеб услуги за външни системи.

Интересът от страна на гражданите и бизнеса непрекъснато нараства, което е видно от представената графика.



Източник: https://analytics.egov.bg/

Фигура 4. *Справка за посещения на портала за 2022 г., вида устройство и видове операционни системи,*

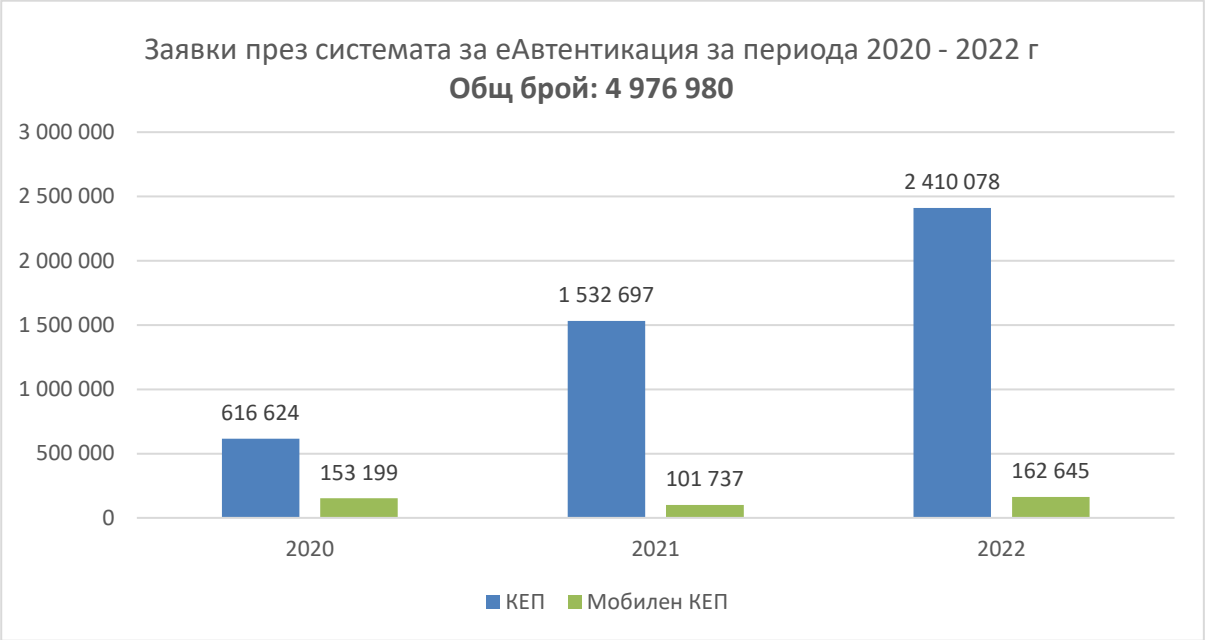
3.1.2. Система за електронна автентикация (е-Автентикация)

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.

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 е 4 976 980, като само за 2022 г. успешните автентикации са 2 572 723, от които 2 410 078 са с КЕП, а 162 645 са тези с мобилен КЕП

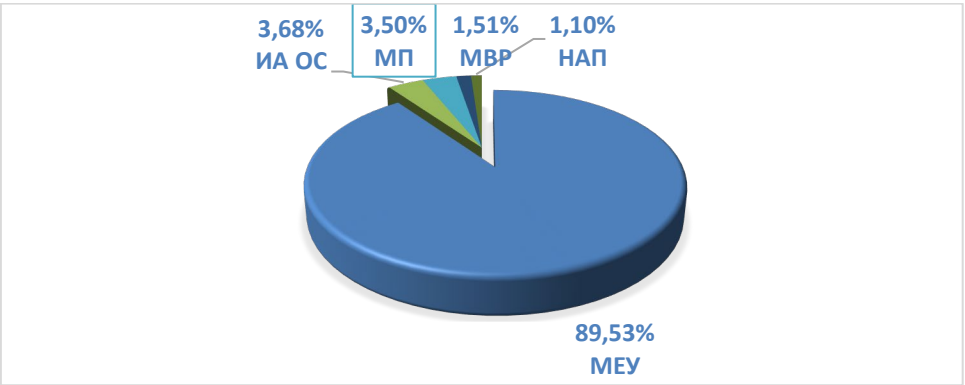
При сравнение с предходния отчетен период увеличението е близо с 65% когато автентикациите чрез КЕП са били 1 532 697 бр., а с мобилен – 101 737 бр.



Фигура 5. *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.

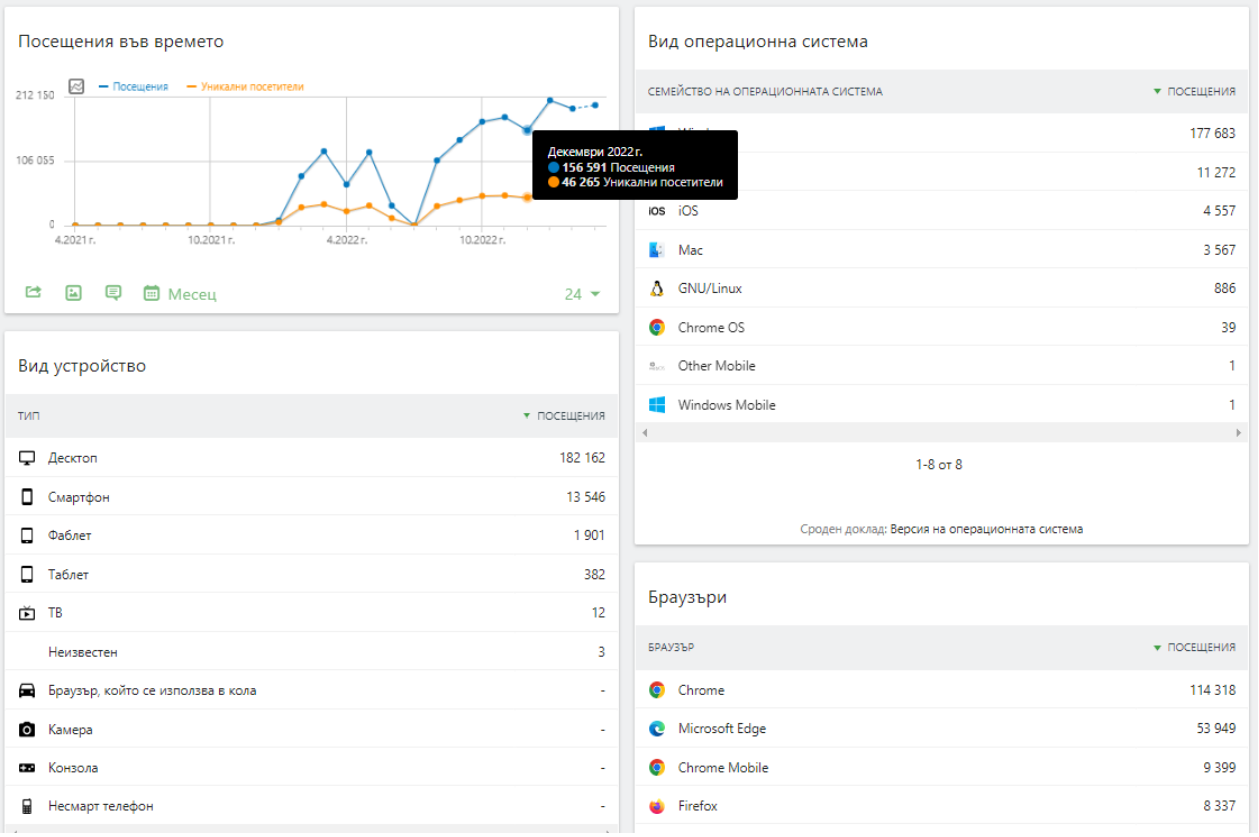
На фигурата по-долу са представени администрациите, чиито информационни системи и портали са интегрирани към еАвт 2.0 и техния дял при формиране на потребителски сесии.



Фигура 6. *Интегрирани системи на доставчици на услуги към системата еАвт 2.0*

Потреблението на системата за електронна автентикация непрекъснато нараства, което е видно от представената графика.

Потреблението на системата за електронна автентикация непрекъснато нараства, което е видно от представената графика.



Източник: analytics.egov.bg

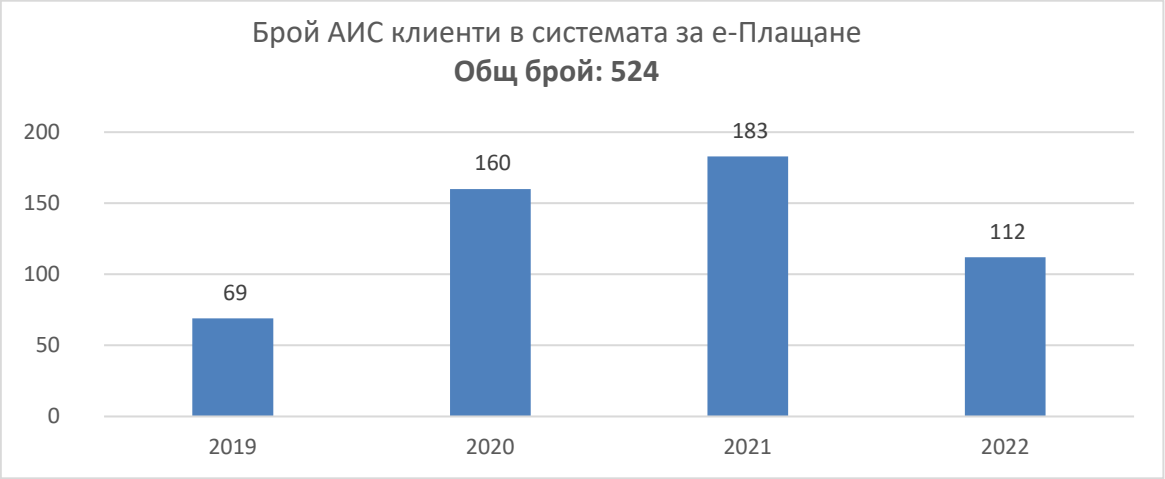
Фигура 7. *Справка за посещения на системата за електронна автентикация за 2022 г., видове устройства и видове операционни системи*

3.1.3. 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. Чрез системата могат да се заплатят услуги към всички областни и общински администрации и техните райони. С надградените нови функционалности на системата се предоставя още един канал за плащане – Централен виртуален ПОС терминал, по който задължените лица могат да заплатят. Заявяването на дължими такси от страна на администрациите се осъществява чрез предоставен от МЕУ достъп на всяка администрация до Средата за електрони плащания. На всяка администрация се предоставя възможност да заявява плащане на физическо или юридическо лице с функционалност за преглед на всички актуални статуси на задълженията в реално време.

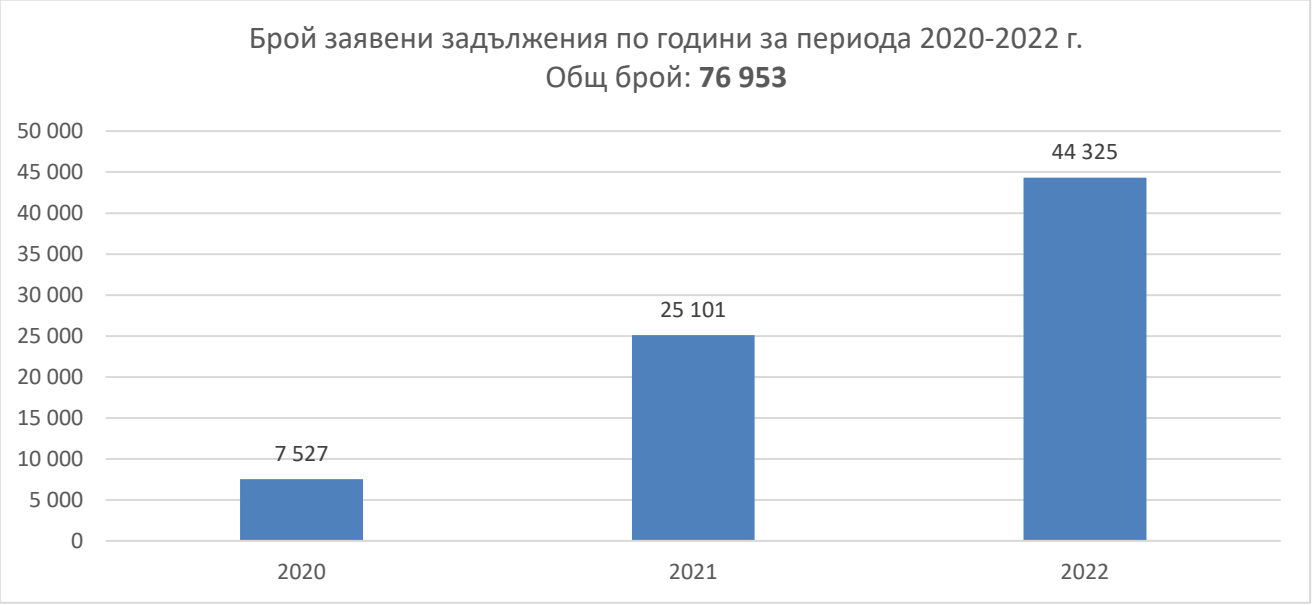
В края на 2022 г. администрациите, доставчици на ЕАУ са 524, а банките са 6. През 2022 г. към системата за електронни плащания са се включили 112 администрации. За отчетния период са регистрирани 44 325 заявки за плащане.

През 2022 г. са присъединени 112 бр. АИС клиенти. Извършените трансакции са 44 325 бр., като същите данни за 2021 г. са съответно 183 бр. АИС клиенти и 25 101 бр. успешни трансакции.



Фигура 8. *Брой АИС клиенти в системата за е-Плащане*

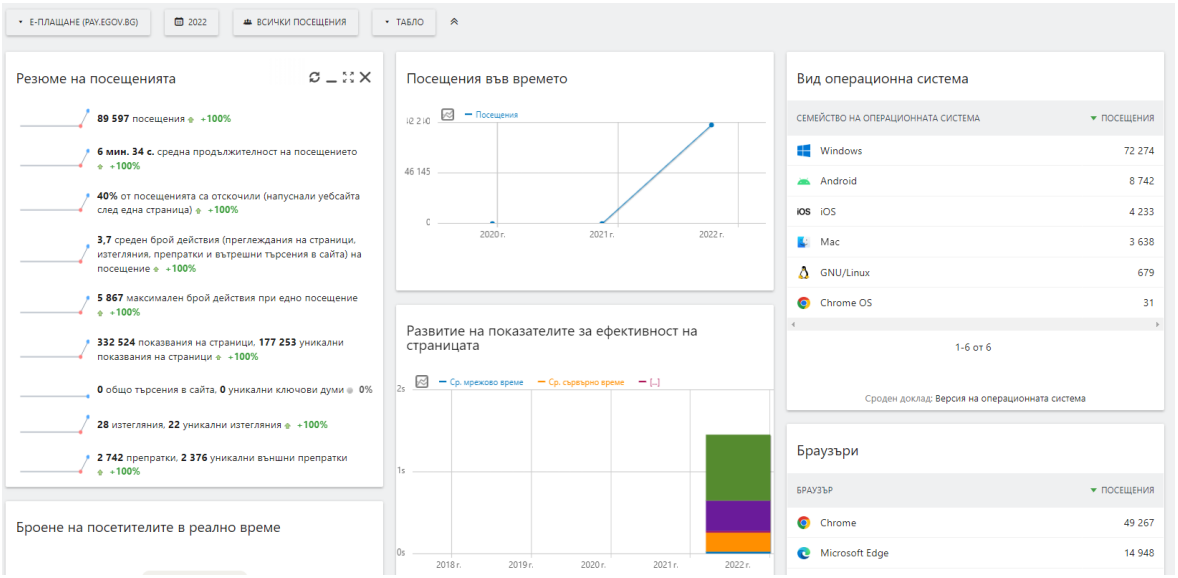
Извършените трансакции за 2022 г. са 44 325 бр., като същите данни за 2021 г. са съответно 183 присъединени АИС клиенти и 25 101 трансакции (съгласно фиг. 7).



Фигура 9. *Статистика за присъединени АИС клиенти на администрации и преминали трансакции в системата за е-Плащане*

През 2022 г. усилията се насочиха за реализиране на възможностите в реално време да се проверява за налични задължения и тяхното последващо заплащане.

Потреблението на системата за електронно плащане непрекъснато нараства, което е видно от представената графика.



Източник: analytics.egov.bg

Фигура 10. *Справка за посещения на системата за електронно плащане за 2022 г., показатели за ефективност, видове операционни системи*

3.1.4. 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 4 125 461 персонални цифрови сертификата. Повишението на ползваемостта на системата в сравнение с 2021 г. е близо 70%, когато броят на проверените цифрови сертификати е бил 2 823 411. Успешните заявки към услугата TimeStamp са 4 125 367, а броят на неуспешните е 94.

3.1.5. 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 1 132 ЕАУ, които са заявявани 140 995 пъти в периода 2019 – 2022 г. Формите са разработени по стандарт с цел унифициране на формуляри.

Списък на най-често заявявани централизирано услуги през 2022 г. е представен в Приложение 1.

От създаването на прототипа на системата статистика на заявените ЕАУ по години е представена на фиг. 11.



Фигура 11. *Брой заявявания на ЕАУ по години*

През 2022 г. прототипът се надгради до пълнофункционална система за управление на електронни форми, чрез която да се предостави възможност за заявяване на услуги чрез уеб базирани форми, както и интеграция на свързаните със заявяването дейности, като заплащане на дължими такси, връчване и др.

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

Системата за сигурно електронно връчване (еВръчване) е реализирана като система за управление на изпращането и/или получаването и съхраняването на електронни документи за/от публични органи, физически и юридически лица при еднозначно удостоверяване на момента на изпращане, получаване и връчване, както и за гарантиране на авторството и интегритета на същите.

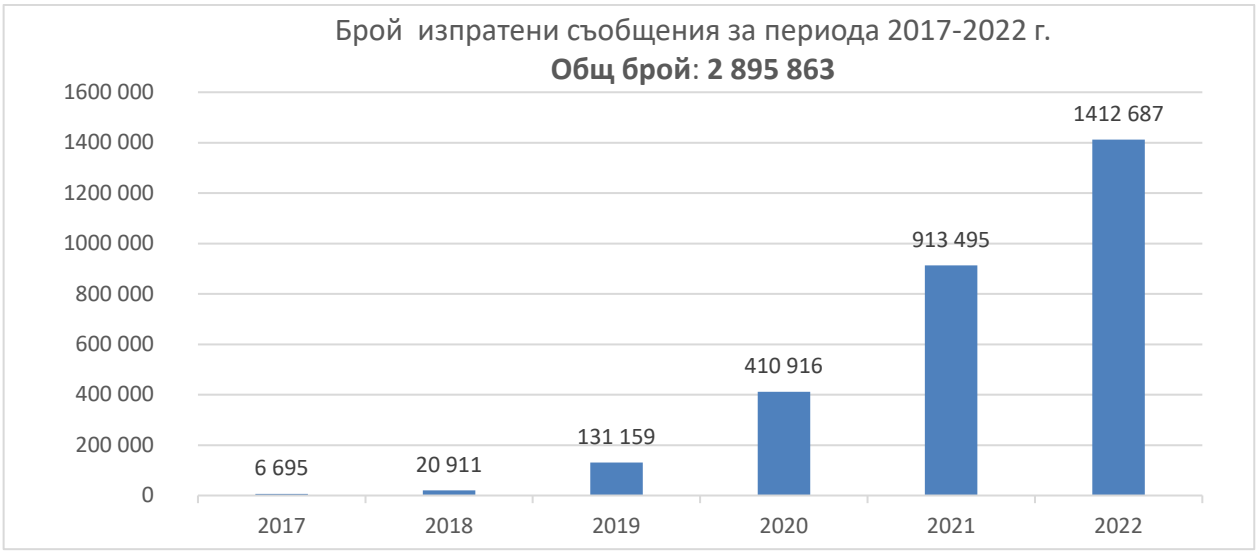
Активните профили в системата към 31.12.2022 г. са 216 434, от които 195 148 физически лица, 2 169 административни органи, 8 955 лица, предоставящи обществени и публични функции и 10 178 фирми. За 2022 г. в системата са регистрирани 3 953 организации, от които 2 655 са юридически лица, а 1 132 са лица по чл. 1, ал. 1 и 2 от ЗЕУ. Изпратените съобщения чрез системата са 1 412 687, което е близо с 60% увеличение в сравнение с 2021 г. – 913 495.

Справка за броя на регистрирани потребители в ССЕВ по години е представена на графиката.



Фигура 12. *Брой регистрираните потребители в ССЕВ по години*

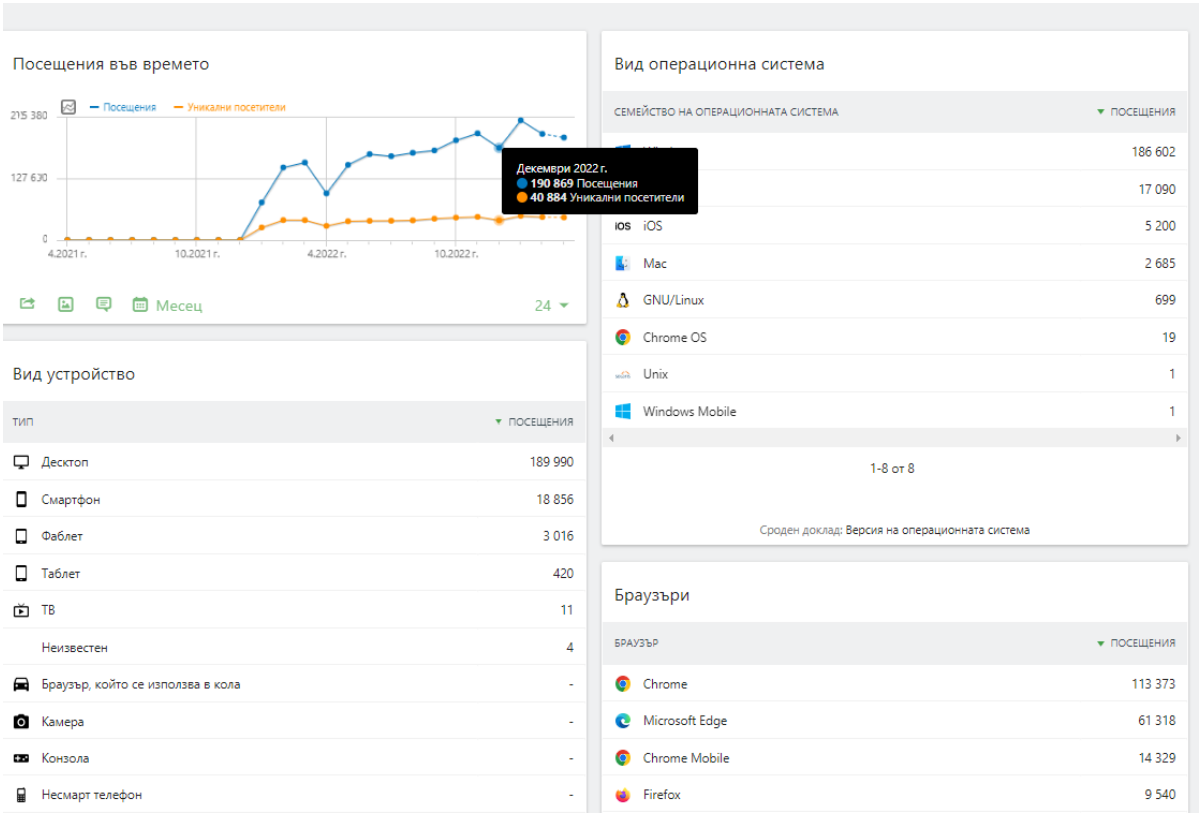
Обменените съобщения чрез ССЕВ към края на отчетния период са общо 2 895 863, като за 2022 г. броят на изпратените съобщения е 1 412 687. Справка за обменените съобщения по години е представена на следващата графика.



Фигура 13. *Справка за обменените съобщения по години*

Интегрираните със ССЕВ информационни системи на административни структури са общо 652, от които за 2022 г. в продукционна среда са 79, от които 64 на администрации, 14 на лица по чл.1 ал. 2 от ЗЕУ и 1 на юридическо лице.

Потреблението на ССЕВ, осигуряваща обмена на съобщения между граждани, бизнес и административни органи непрекъснато нараства, което е видно от представената графика.



Източник: analytics.egov.bg

Фигура 14. *Справка за посещения на системата за сигурно електронно връчване за 2022 г., вид на устойствата и видове операционни системи*

Системата поддържа централизирано хранилище на електронни документи, чрез което се премахва необходимостта един документ да се изпраща многократно до множество получатели (изпраща се линк към документа). В хранилището са разположени 4 315 591 документа, от които 4 007 914 са съобщения.

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:

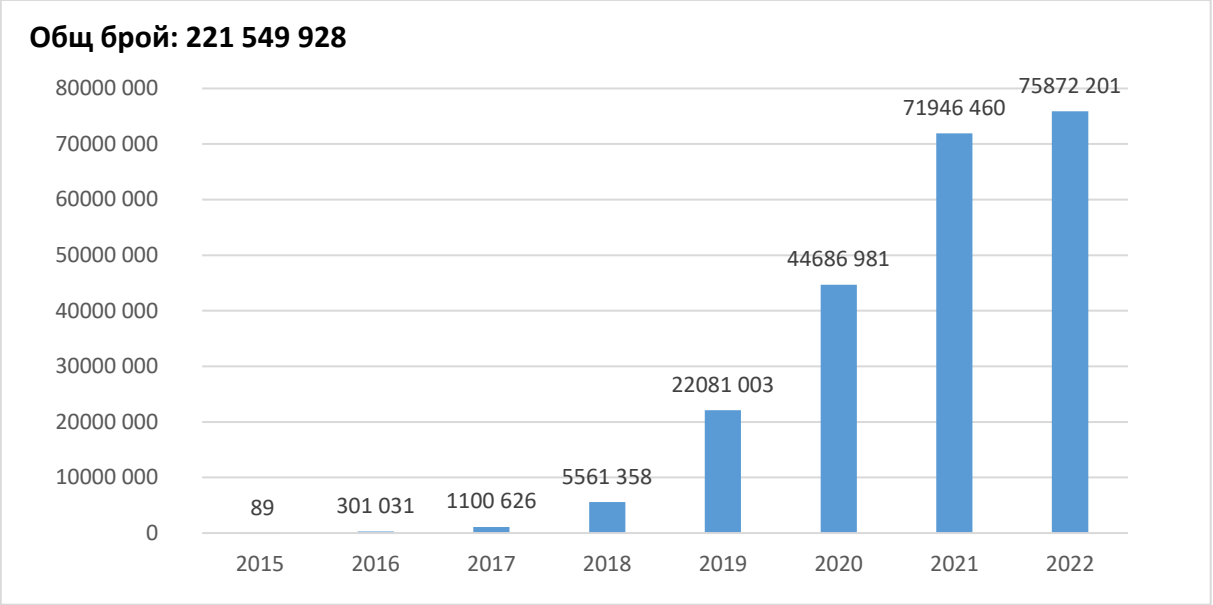
3.2.1 Среда за междурегистров обмен на данни

През 2022 година продължават усилията за разширяване на възможностите за служебен обмен на данни като вътрешни електронни административни услуги (ВЕАУ) между административните органи чрез Средата за междурегистров обмен на данни. Общият брой консуматори на справки е близо 1 100. Към средата са свързани 82 основни регистъра, администрирани от 28 централни администрации – министерства и изпълнителни агенции, и са реализирани 218 справки към регистрите.

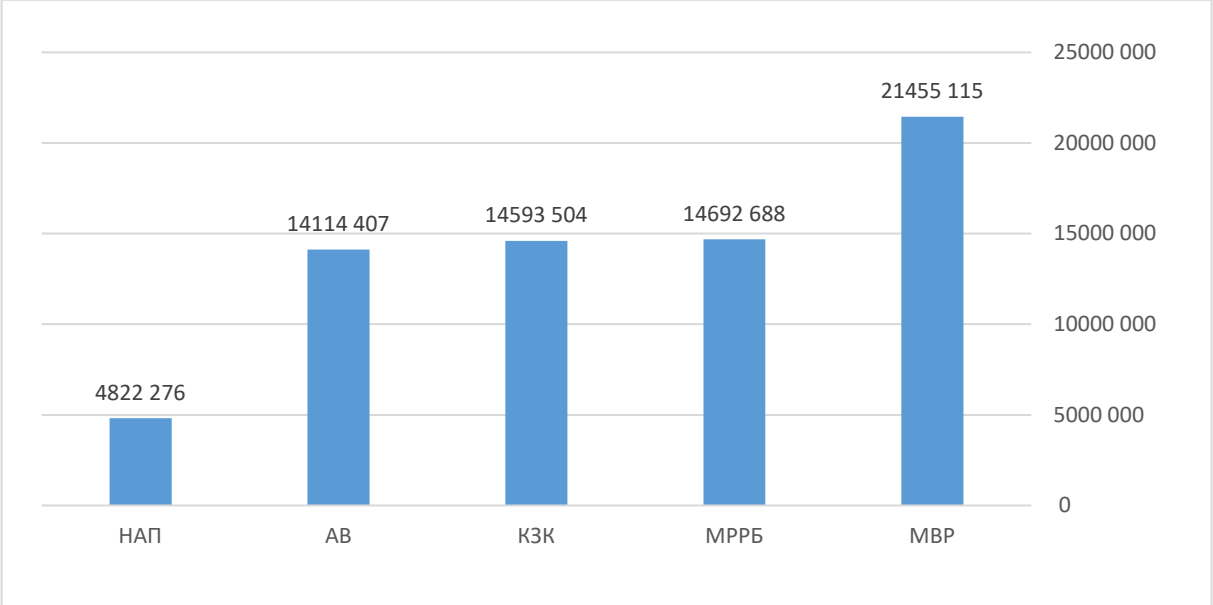
Към края на 2022 г. общият брой направени заявки към регистри е 221 549 749, като за отчетния период са извършени 75 872 201 справки. По данни от логовете на системата за 2022 г.:

- Агенцията по обществени поръчки е консуматорът с най-много извършени справки – 14 651 689;
- Министерството на вътрешните работи е предоставило най-много данни – 21 455 115;

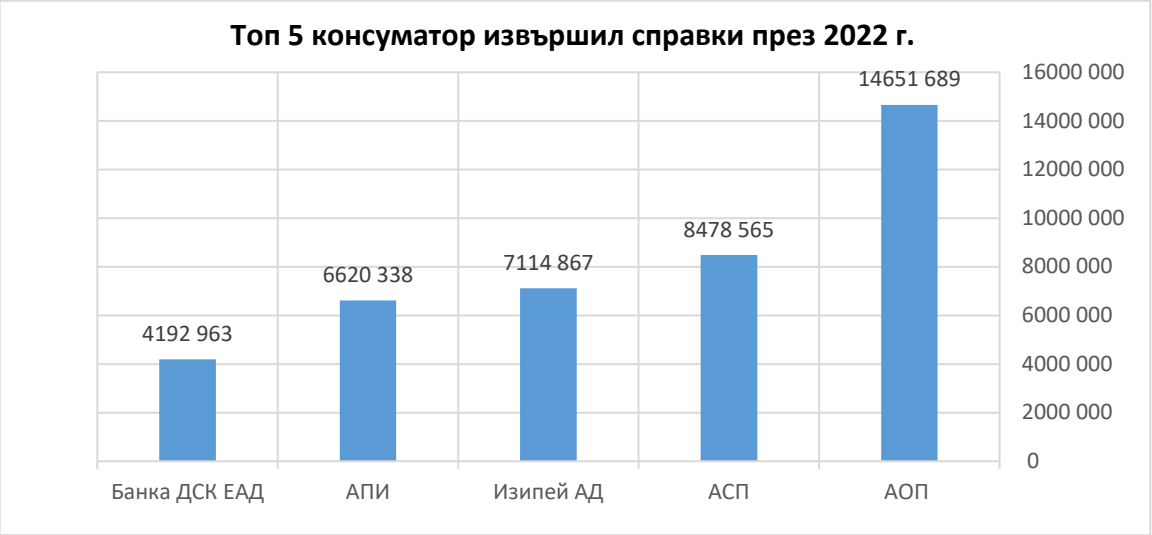
- Регистърът „Български документи за самоличност“ е най-често достъпван - 17 678 146.



Фигура 15. *Справки и посетени регистри за 2022 г.*



Фигура 16. *Топ 5 посещавани администрации през 2022 г.*

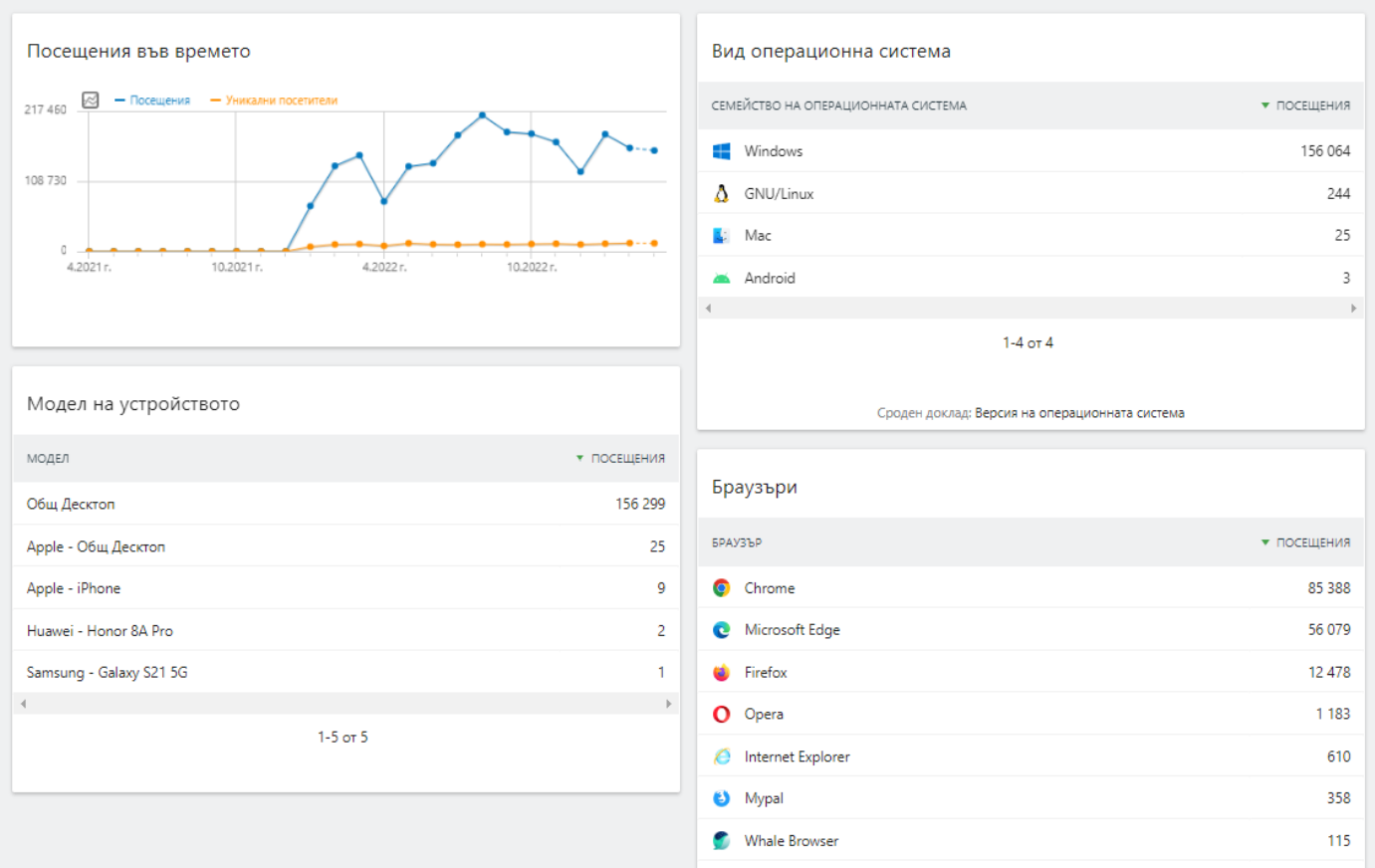


Фигура 17. *Топ 5 „Консуматор“ на справки*

В информационното 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 административно приложение, на електронен адрес: https://admin-regix.egov.bg/main и клиентското приложение: https://client-regix.egov.bg/main.

Към Средата за междурегистров обмен на данни са присъединени всички общински администрации. Засиленото използване на Средата за междурегистров обмен на данни 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.



Източник: analytics.egov.bg

Фигура 18 *Справка за посещения на системата за електронно плащане за 2022 г., показатели за ефективност, видове операционни системи*

Списък с администрациите и лица по чл. 1., ал. 2 от ЗЕУ с най-голям брой системи, присъединени към Средата за междурегистров обмен на данни е предоставен в Приложение 2.

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 показват леко намаляване във всички категории на броя на администрациите, които нямат внедрени информационни системи, като най-значително е намалението при системите за управление на база данни (близо 4%). Всички административни структури отчитат, че имат информационна система за счетоводство.

Администрации, които НЯМАТ внедрени информационни системи	***2020 г. %***	***2021 %***	***2022 г. %***
Административни информационни системи/ Система за документооборот	*5.79*	*5.45*	*3.10*
Система за управление на човешките ресурси	*25.7*	*23.51*	*22.4*

Система за труд и работна заплата	*2.4*	*2.7*	*1.20*
Система за счетоводство	*1.2*	*1.4*	*0.00*
Система за управление на база данни	*46.5*	*45.8*	*41.90*
Системи за управление на документи, потоци и съдържание през WEB	*46.7*	*44.5*	*43.20*
АИС за комплексно административно обслужване	*71.7*	*69.3*	*66.70*
Система за правно-информационни услуги	*16.9*	*16.6*	*15.80*

Таблица 3. *Администрации, които нямат внедрени информационни системи.* *Източник ИИСДА*

4. Електронна идентификация

4.1. Електронна идентификация за нуждите на заявяване на ЕАУ

Националната схема за електронна идентификация, предвидена в Закона за електронната идентификация все още не е изградена, което в определена степен ограничава достъпа на гражданите и бизнеса до ЕАУ, в т.ч. и трансгранични такива.

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. И през 2022 г. не е извършена промяна в Административния регистър с оглед вписването на средствата на електронна идентификация и тяхното ниво на осигуреност в специално създадено за целта поле.

През отчетния период няма промяна по отношение на нормативно определените средства за електронна идентификация – квалифициран електронен подпис, различни персонални идентификационни кодове (ПИК на НАП, ПИК на 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 Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги. Общинската администрация предоставя ЕАУ основно чрез ЕПДЕАУ и потребителите на тези услуги се идентифицират чрез средствата, които изисква портала. Това са КЕП, включително облачен/мобилен КЕП и ПИК на НАП/НОИ. Средствата, които не са правно регламентирани, но все още се ползват са КИН (клиентски идентификационен номер) и ПИН (персонален идентификационен номер). Гражданите се идентифицират чрез тях предимно пред общинската администрация.

Па данни в ИИСДА, 590 администрации са обявили, че предоставят достъп до ЕАУ с повече от едно средство за електронна идентификация.

Съгласно информацията 63% от администрациите изискват КЕП, 20% - ПИК и 17% - потребителско име и парола или друго средство.

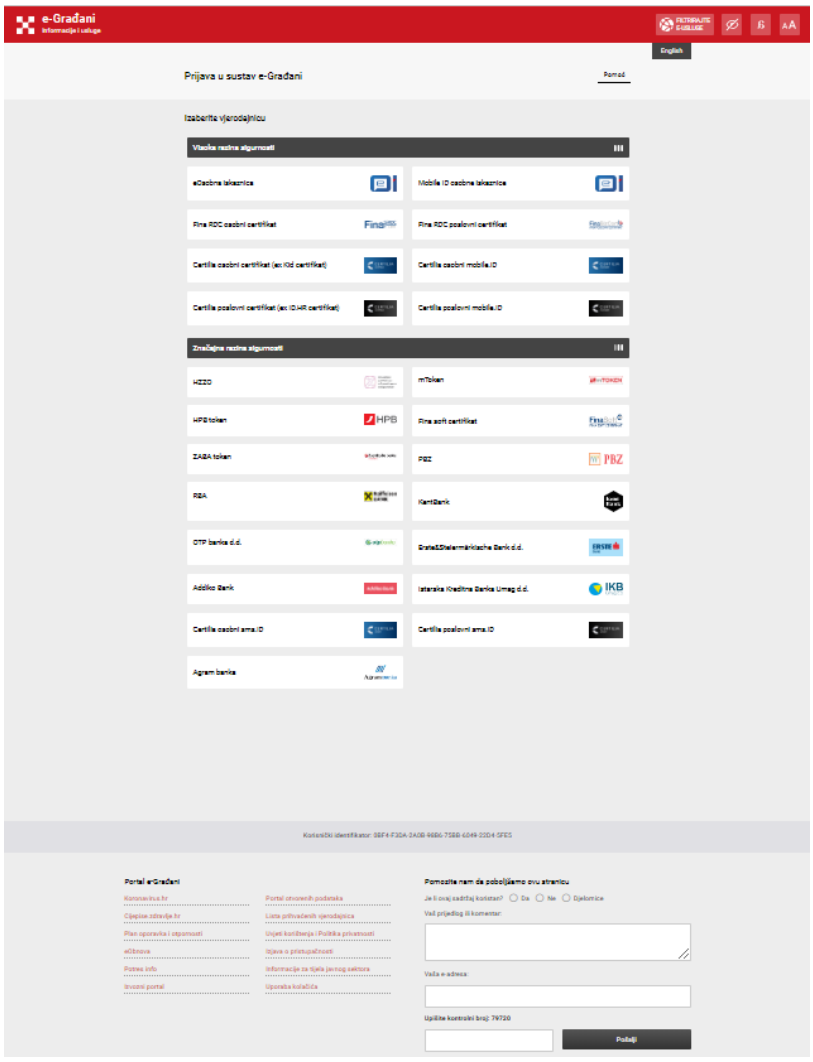
4.2. Трансгранична електронна идентификация

С проекта за развитие на националния eIDAS възел, интеграция с eIDAS възлите на другите държави - членки на ЕС, както и осигуряването на достъп до ЕАУ, се реализира надеждно трансгранично удостоверяване на автентичност, като се гарантира оперативната

съвместимост със схемите за електронна идентификация на държави членки. Проектът включва актуализиране на текущата версия на възела спрямо последната актуална техническа спецификация, предоставена от ЕК. С изграждането на точка на свързване, в съответствие с Регламент (ЕС) № 910/2014 и Регламент за изпълнение на Комисията (ЕС) 2015/1501, като част от архитектурата за оперативна съвместимост на електронната идентификация се реализира се поетапна реална интеграция с eIDAS възлите на останалите държави-членки на ЕС, при участие в трансграничното удостоверяване на автентичността на лица. Възелът е в състояние да разпознава, обработва или препраща данни към други възли, с което дава възможност националната инфраструктура за електронна идентификация на една държава членка да се свързва с националната инфраструктура за електронна идентификация на други държави членки.

Към края на 2022 г. е реализирана свързаност на eIDAS възела на България с eIDAS възлите на Германия и Испания.

Идентифицира се съществен проблем, свързан не само с липсата на национална схема за електронна идентификация, но и силното ограничаване на възможните средства за идентификация до квалифициран електронен подпис, ПИК на НАП и ПИК на НОИ. Посочените ограничения в никакъв случай не са свързани с технологични проблеми, а основно са в резултат на липсата на политическа воля за решаването на проблема. Пример в противоположната посока е държава като Хърватия с над 20 средства за идентификация и 15 ДЧ присъединени към националния им eIDAS възел (https://nias.gov.hr/en/Authentication/Step2):



5. Регистри, поддържани от администрацията

За отчетния период, съгласно данните, отчетени в ИИСДА 181 администрации поддържат 2 481 регистри. Отчетените регистри са както следва:

- 1 962 регистри, които се поддържат в електронен вид;
- 234 регистри, които се поддържат на хартиен носител и подлежат на електронизация;
- 285 регистри, за които закон предвижда да се водят на ръка и не подлежат на електронизация.

От регистрите, за които през 2022 г. е отбелязано, че имат обмен и интеграция на данни с други регистри разпределението е следното:

- 231 - обменът на данни се осъществява чрез автоматизиран обмен на данни;
- 45 - обменът на данни се осъществява на хартиен носител;
- 65 - обменът на данни се осъществява по друг начин.

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.

Инфраструктурата на споделените ресурси се състои от следните основни компоненти:

- Държавен хибриден частен облак (ДХЧО);
- Комуникационна инфраструктура (Единна електронна съобщителна мрежа на държавната администрация – ЕЕСМ, Интернет/Екстранет/Интранет);
- Хранилище за данни на електронното управление.

Основната опорна мрежа на ИКТ инфраструктурата на е-управлението е изградена върху устройства, които осигуряват мрежова свързаност с капацитет 10 Gb/s и 1Gb/s.

6.1. Държавен хибриден частен облак (ДХЧО)

Държавният хибриден частен облак (ДХЧО) е един от основните компоненти на споделените ресурси на електронното управление, чрез който се предоставят и конфигурират информационни ресурси (хардуер и системен софтуер) за изграждане на информационни системи, предоставящи електронни услуги за гражданите и бизнеса. Ефективното им използване зависи в голяма степен от осигуряването на достатъчно средства за поддържане на високо технологично ниво и за развитие на критична маса от потребители и услуги. В обхвата на ДХЧО се включват центровете за данни.

Центровете за данни са изградени в инженерно-технически съоръжения и имат за предназначение да осигуряват информационни ресурси за нуждите на е-управлението с високо ниво на наличност и сигурност. Те отговарят на повишени изисквания за производителност и надеждност на системите за обработка на информацията и за нейното съхранение, на комуникационната среда за достъп до информационните ресурси, на електрозахранването, климатизацията, пожарозащитата, сигурността и другите поддържащи

системи.

В центровете за данни са инсталирани следните основни системи:

- комуникационна система, осигуряваща мрежова сигурност и защитен мрежов достъп;
- Системи за оторизация и автентикация;
- Система за управление на достъпа до интернет и сигурен достъп до системата за електронна поща;
- Система за електронна поща и съвместна работа с потребителите;
- Система за оперативни актуализации на системите и приложните софтуерни пакети;
- Система за архивиране и възстановяване на критични данни.

Информационните компоненти на инфраструктурата на споделените ресурси на е-управлението са разположени в центрове за данни както следва:

- Основен център за данни в СОСП „Ботевград 2“;
- Контролно-технически център за данни Бояна;
- центрове в процес на изграждане – резервен център за данни, за който предстои издаване на акт 16 и Център за възстановяване на данни при бедствия и аварии (Disaster Recovery Center-DRC), който е в процес на изграждане в СОСП.

В края на отчетния годишен период предоставените информационни ресурси от ДХЧО са както следва:

На 80 (осемдесет) министерства и ведомства са предоставени:

- 1 217 броя виртуални машини;
- 1 188 ТБ дисково пространство.

На 78 министерства, агенции и общини са дадени 2 492 пощенски кутии от Електронна поща.

Има 1 601 потребителя (министерства, агенции и общини) на Системата за електронен обмен на съобщения (СЕОС).

Копие на данни в хранилището за данни на ИА „Инфраструктура на електронното управление“ правят 28 министерства, агенции и общини, като за тази цел са предоставени 628 ТБ от наличните 800 ТБ.

Колокация на инфраструктура в центровете за данни използват 4 министерства и ведомства.

В таблицата са показани държавните организации, ползващи ресурси в ДХЧО към момента.

ДЪРЖАВНА ОРГАНИЗАЦИЯ
Изпълнителна агенция „Инфраструктура на електронното управление“
Министерски съвет
Министерство на регионалното развитие и благоустройството
Изпълнителна агенция по рибарство и аквакултури
Държавна агенция „Безопасност на движението по пътищата“
Държавна агенция за метрологичен и технически надзор
Министерство на иновациите и растежа

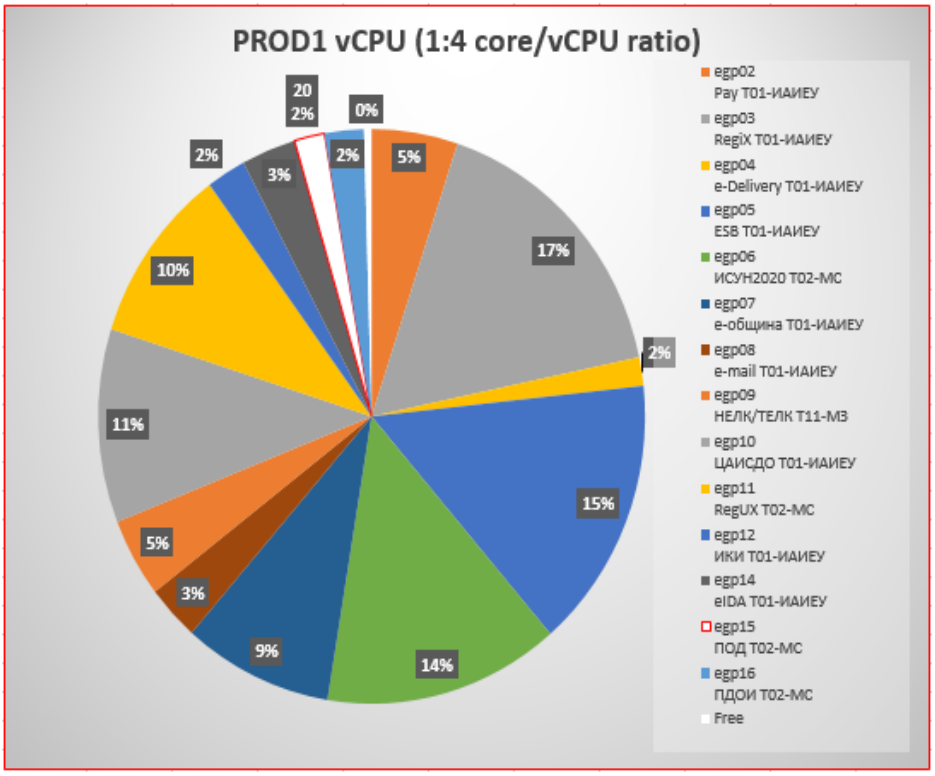
ДЪРЖАВНА ОРГАНИЗАЦИЯ
Министерство на транспорта и съобщенията
Агенция по обществени поръчки
Министерство на икономиката и индустрията
Министерство на здравеопазването
Изпълнителна агенция по горите
Национален статистически институт
Изпълнителна агенция борба с градушките
Комисия за регулиране на съобщенията
Министерство на електронното управление
Комисия за защита на конкуренцията
Български пощи
Омбудсман на РБ
Прокуратура на Република България
Народно Събрание
Министерство на земеделието
Централна Избирателна Комисия
Община Троян
Министерство на околната среда и водите
Министерство на младежта и спорта
Държавна агенция "Архиви"
Изпълнителна агенция "Одит на средствата от Европейския съюз"
Българско национално радио
Комисия за финансов надзор
Министерство на труда и социалната политика
Министерство на туризма

***Таблица 4**. Списък на държавните организации, ползващи ресурси в ДХЧО*

През отчетния период натоварването на ресурсите на ДХЧО е нараснало значително и е както следва:

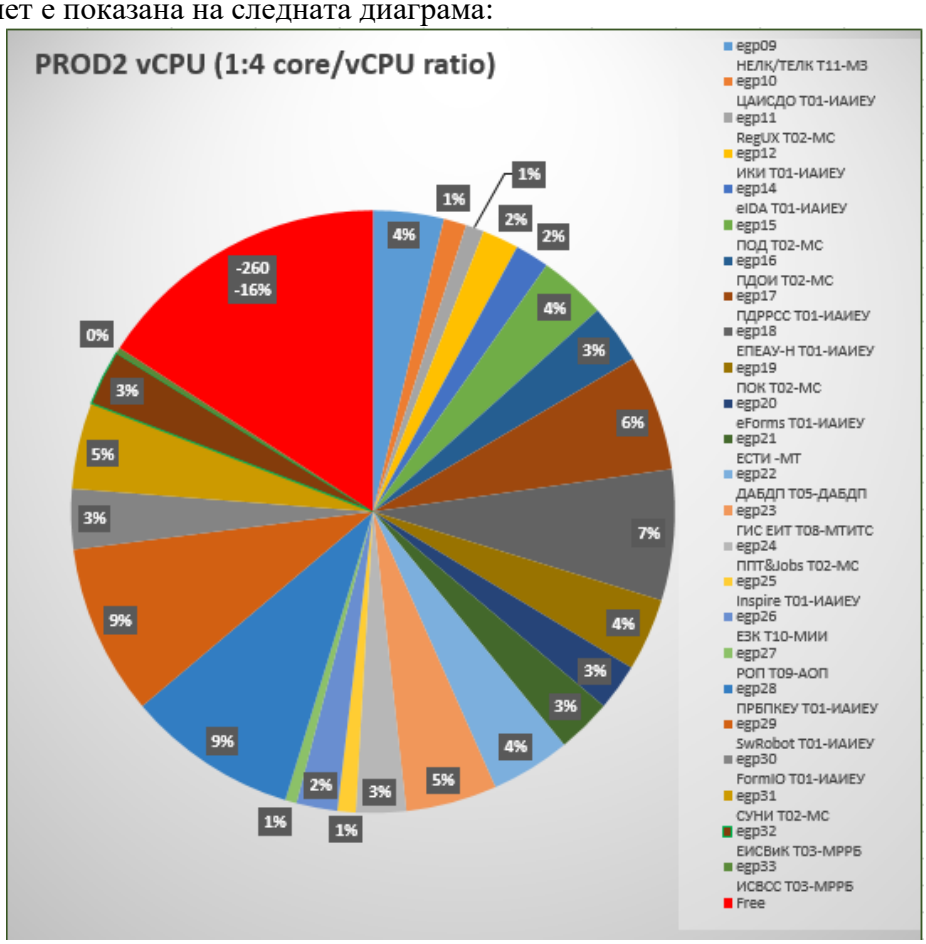
- За клъстер 1 на Основния център за данни на ДХЧО (фиг. 19):
  - 98 % от наличната изчислителна мощност
  - 67 % от хардуера за съхранение на данни
- За клъстер 2 на Основния център за данни на ДХЧО (фиг. 20):
  - 84 % от наличната изчислителна мощност
  - 93 % от хардуера за съхранение на данни

Натовареността на изчислителните ресурси за клъстер 1 на ДХЧО към датата на годишния отчет е показана на следната диаграма:



Фигура 19 Заетост на продукционната среда за клъстер 1 на ДХЧО

Натовареността на изчислителните ресурси за клъстер 2 на ДХЧО към датата на годишния отчет е показана на следната диаграма:



Фигура 20. *Заетост на продукционната среда за клъстер 2 на ДХЧО*

И през 2022 г. е осигурена експлоатационна поддръжка на работоспособността на инфраструктурната среда на системи на електронното управление и техническа поддръжка на софтуер от производителя.

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 2022 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 ИА ИЕУ – 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;

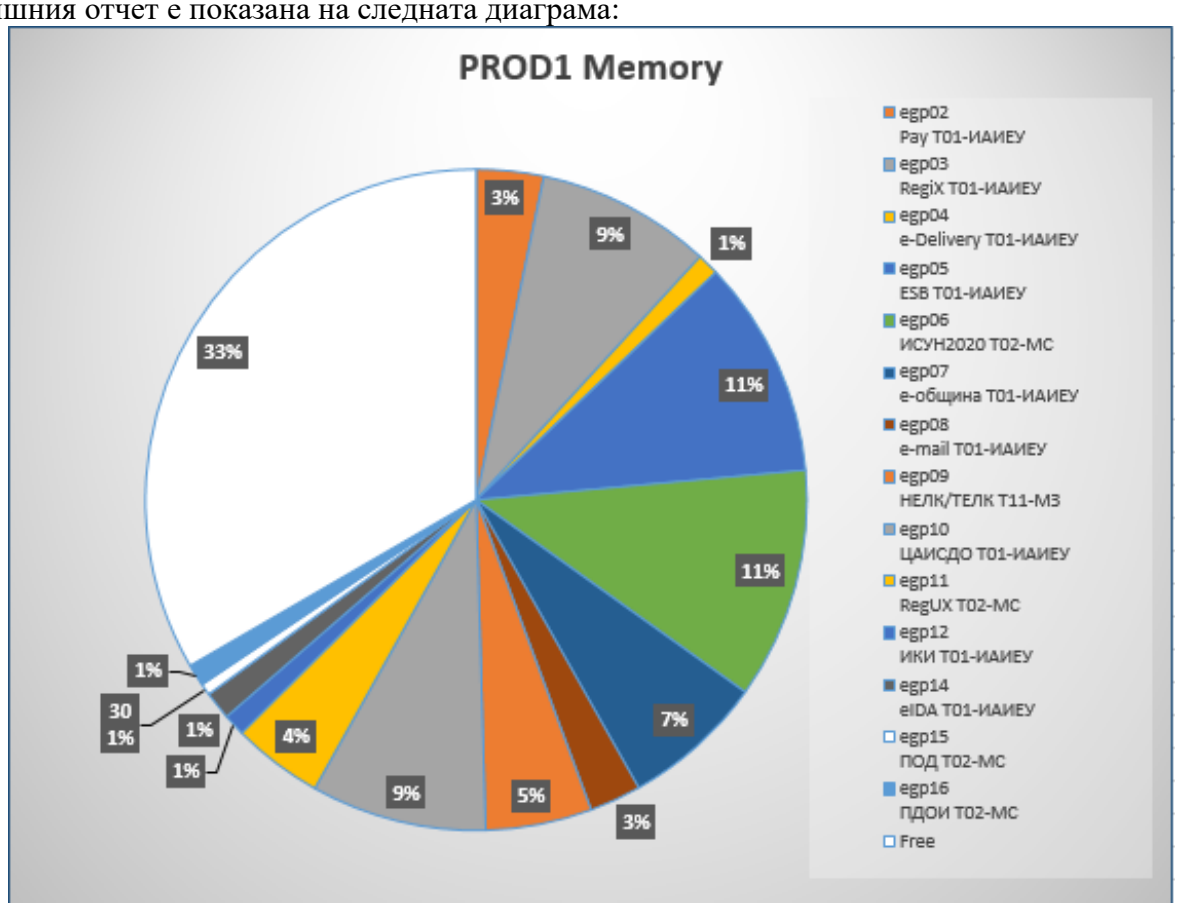
- миграция и монтаж на опорен маршрутизатор в ОА Сливен на 10G свързаност;
- миграция на опорен маршрутизатор в ОА Ямбол. Пускане на комуникационни услуги;
- монтиране на 10Gbps транспондери за НАП, изграждане и тестване на връзка Ботевград - Велико Търново;
- направено е проучване за осигуряване на свързаност чрез ЕЕСМ 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 ЕЕСМ 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“.
- Миграция на специализираната централизирана система за управление и контрол на политиките за достъп до комуникационните устройства в ЕЕСМ - Access Control Server (ACS) към нова и по-надеждна система за управление и администриране (Identity Services Engine - ISE);
- 39 общини са свързани към документно-оборотната система;
- 10G свързаност в северна България + Велико Търново – Габрово - Стара Загора – Варна – Несебър - Бургас;
- Изградени две независими оптични трасета за връзка с Cloud Flare, защитаващ всички мрежи на Министерски съвет, ДХЧО и ЗИВ;
- 15 ведомства използват преноса през ЕЕСМ за връзка с ДХЧО;
- BGP свързаност на десет ведомства към ЗИВ за връзка с Интернет;
- Всички мрежи на Министерски съвет излизат през ЗИВ за връзка с Интернет;
- Разширяване на съществуващите услуги до нови 150 точки;
- BG Allert;
- Преминаване от L2 на L3 услуги за цялата мрежа на Министерство на финансите + АДФИ, АМ, НАП
- 60 ново изградени възли за достъп (ВД);
- Пуснати интернет доставчици – Hurricane Electric, Evolink, Vivacom, GTT, BIX;

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.

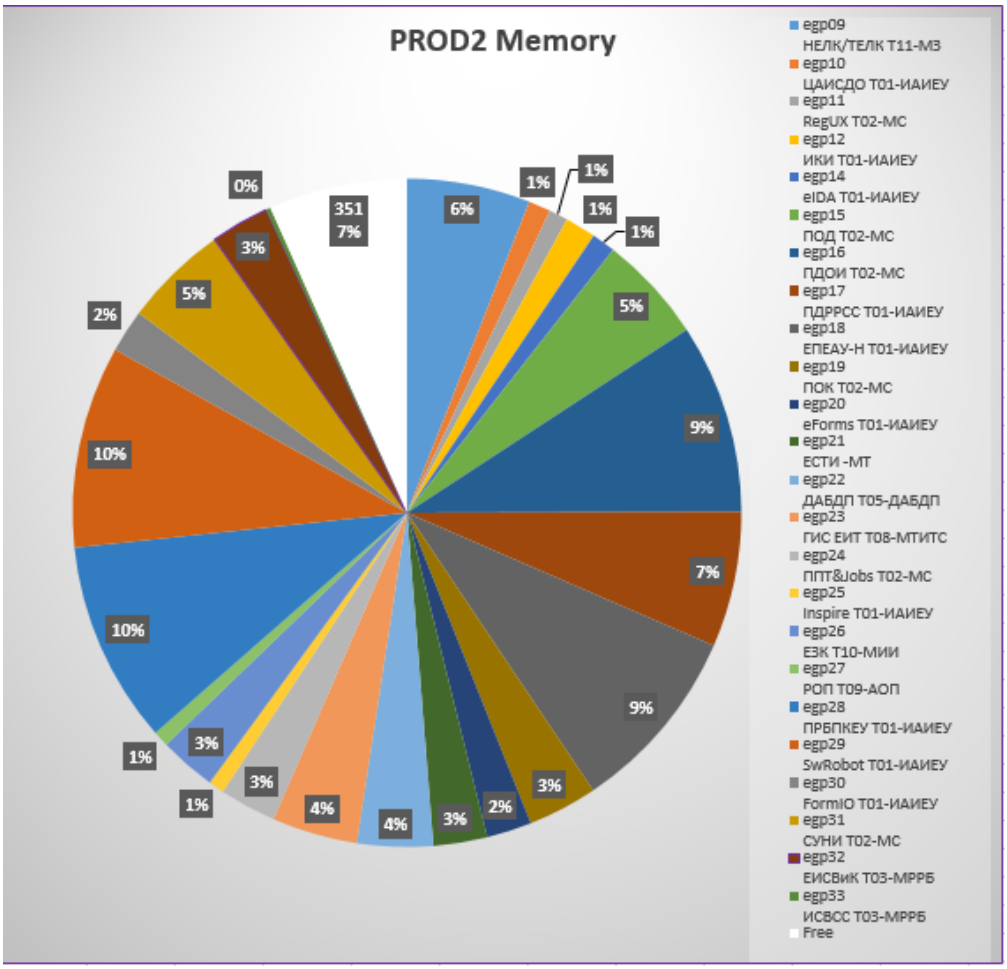
Използваемостта на хранилището за данни на ДХЧО (за клъстер 1 и клъстер 2) към датата на годишния отчет е показана на фиг. 20 и фиг. 21

Използваемостта на хранилището за данни за клъстер 1 на ДХЧО към датата на годишния отчет е показана на следната диаграма:



Фигура 21. *Използваемост на хранилището за данни за клъстер 1 на ДХЧО*

Използваемостта на хранилището за данни за клъстер 2 на ДХЧО към датата на годишния отчет е показана на следната диаграма:



Фигура 22. *Използваемост на хранилището за данни за клъстер 2 на ДХЧО*

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, през единна входна точка, 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). По този начин се спестяват ресурси на администрациите и се осигурява по-добра координация и контрол по отношение на изискванията за оперативната съвместимост към информационните системи на администрациите.

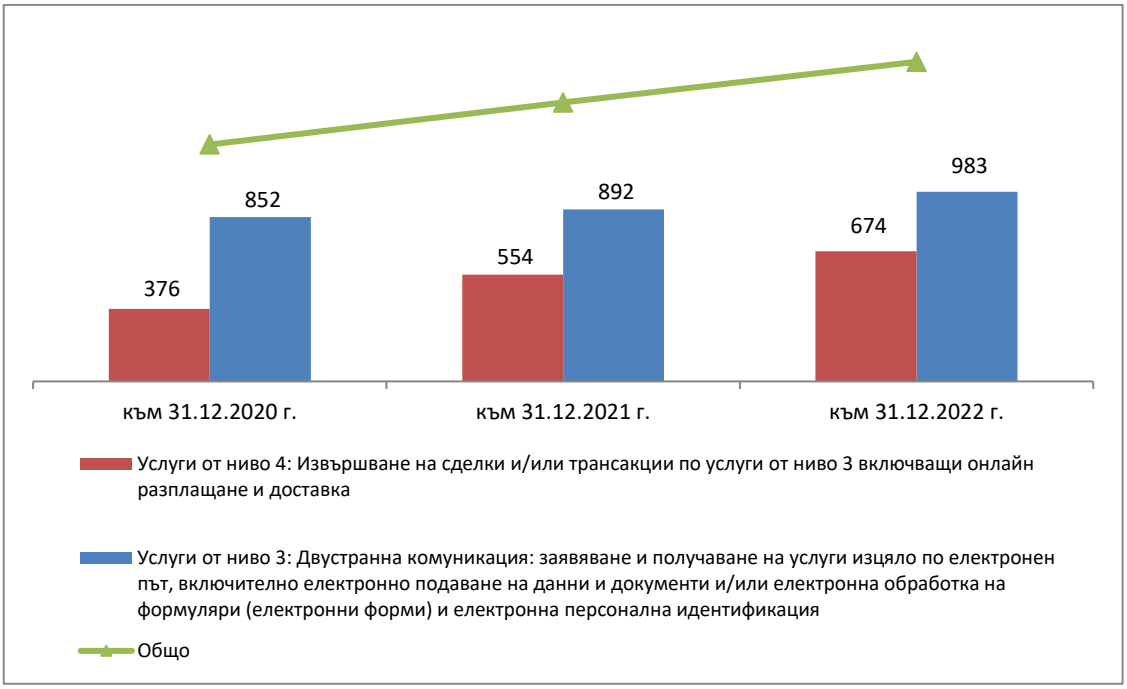
7.1 Състояние на електронните административни услуги

Общият брой услуги[1], вписани в АР към 31.12.2022 г., е 2 505, от които 1 657 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 (фиг. 19). Важно е да се отбележи обаче, че тази справка отчита всяка една услуга с данните за нивата на предоставяне, които не са едни и същи за еднотипни услуги, предоставяни от отделните

[1] източник: Интегрирана информационна система на държавната администрация https://iisda.government.bg/adm_services/services

административни органи. С това се обяснява и големият получен от справката брой на ЕАУ.

Следва да се отбележи невъзможността да бъдат агрегирани данните по еднотипни услуги, което води до разминаване в реалния брой услуги по нива, и до затруднения в интерпретацията на информацията що се касае до ЕАУ, предоставяни от повече от една администрация.



Фигура 23. *Брой услуги от ниво 3 или ниво 4 по години*

Забелязва се увеличение на броя на административните услуги, предоставяни на нива 3 и 4 спрямо общия брой предлагани услуги и техният дял вече е над 50%.

7.2 Осигуряване на институционална идентичност и достъпност на уебсайтовете

В изпълнение на изискванията на Директива (ЕС) 2016/2102 относно достъпността на уебсайтовете и мобилните приложения на организациите от обществения сектор официалните интернет страници и порталите на държавните администрации трябва да бъдат достъпни с цел осигуряване на равен достъп за всички до интернет среда. Административните органи, лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги, са нормативно задължени (чл. 58в от Закона за електронното управление) да осигуряват достъпност на съдържанието на своите интернет страници и мобилни приложения в съответствие с приложимите хармонизирани стандарти, части от тях или технически спецификации.

Наблюдението и проверките се извършват в съответствие с Методология за наблюдение и проверки на достъпността на съдържанието на интернет страниците и мобилните приложения[2] на лицата по чл. 1 ал. 1 и ал. 2 от Закона за електронното управление. Методологията е съобразена с Решение за изпълнение (ЕС) 2018/1524 от 11 октомври 2018 г. за установяване на методиката на наблюдение и реда и условията за докладване от държавите членки в съответствие с Директива (ЕС) 2016/2102 и изискванията на хармонизирания стандарт EN 301 549 V3.2.1 (2021-03).

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 за институционална идентичност[3], която гарантира,

[2] https://egov.government.bg/wps/portal/ministry-meu/home/web-accessibility/monitoring
[3] https://egov.government.bg/wps/portal/ministry-meu/strategies-policies/institutional-identity/institutional-identity

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 2022 г. (в рамките на втория период на наблюдение) е извършено наблюдение на уебсайтовете на организации от обществения сектор (лица по чл. 1, ал. 1 и ал. 2 от ЗЕУ), както следва:

- в периода 01.01.2022 г. – 31.12.2022 г. – наблюдение на уебсайтове по метода на опростеното наблюдение (218 сайта);
- в периода 07.10.2022 г. – 31.12.2022 г. – наблюдение на уебсайтове по метода на задълбоченото наблюдение (21 сайта);

Извадката обхваща държавни уебсайтове от централната администрация, регионални, местни и други уебсайтове, както следва:

- държавни уебсайтове – 23 бр.;
- регионални уебсайтове (NUTS1, NUTS2, NUTS34) – 33 бр.;
- местни уебсайтове (LAU1, LAU25) – 41 бр.;
- уебсайтове на публичноправни организации, които не принадлежат към горните три категории – 121 бр.

Включените в извадката уебсайтове предоставят възможно най-голям брой услуги, в различни сектори на обществения живот, включително:

- социална защита – сайтове на пенсионноосигурителни дружества, комисии, агенции, асоциации – 14 бр.;
- здравеопазване - сайтове на лечебни заведения: болници и лаборатории; регионални здравни инспекции и др. държавни сайтове – 17 бр.;
- транспорт - сайтове на превозвачи (автобусни, тролейбусни) и др. – 9 бр.;
- образование - сайтове на регионални управления на образованието, университети, училища - 72 бр.;
- опазване на околната среда – регионални инспекции по околна среда и водите, изпълнителни агенции - 9 бр.;
- култура и отдих - сайтове на домове на културата, читалища – 4 бр.;
- комунални услуги – сайтове на ВИК оператори, топлофикационни дружества, електроразпределителни дружества – 11 бр.;
- обществен ред и безопасност – сайтове на застрахователни дружества - 2 бр.;
- логистика - сайтове на доставчици на куриерски и пощенски услуги - 9 бр.
- финанси – сайтове на банки – 5 бр.

За наблюдаваните уебсайтове се извърши и проверка за изпълнение на задължението

[4] *Според класификацията на териториалните единици за статистически цели в България NUTS 1 – Райони от ниво 1; NUTS 2 – Статистически райони; NUT 3 – Области*

[5] *LAU 1 – Общини; LAU 2 – Населени места*

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:

- неосигурен еквивалентен алтернативен текст за изображения и активни изображения - липса на alt атрибут или празен alt атрибут за изображения, които не са декоративни, неподходящ алтернативен текст, вкл. текстове на английски език;

- некоректно маркирани декоративни изображения, така че да остават скрити за спомагателните технологии.

- етикети, които не са програмно свързани със съответстващите им текстови полета във формуляри (формуляри за обратна връзка, за сигнали и др.) и полета без етикети (например за полето за въвеждане на ключови думи във формата за търсене); често атрибутът placeholder се използва като единствен метод за осигуряване на етикет за текстово поле.

- използвани са комбинации между текст и неговия фон, които не осигуряват достатъчен контраст, съгласно изискването на стандарта (за малък текст – поне 4:1.5, за голям текст – поне 3:1). Ниският контраст е най-често срещаната грешка, в почти всички сайтове.

- връзки с текст, който не подсказват действието, което ще се изпълни при активирането на връзката или празни връзки;

- връзки, включени с атрибута href, без текстово съдържание (като текст или текстова алтернатива) или без етикет, който идентифицира целта (aria-label или aria-labelledby).

- неправилно йерархично вложени заглавия (хединги) – част от сайтовете използват заглавия от различни нива, но в много случаи не е спазена йерархията при тяхното влагане: прескачане на нива; липса на заглавие от ниво 1 за основната тема на страницата; основно заглавие от ниво 2 или по-ниско, вместо от ниво 1;

- структура от заглавия, която не представя правилно основните теми и подтеми;

- елементи за заглавие без съдържание;

- списъци, които не са обозначени чрез използване на семантично маркиране.

- неидентифициран основен език на страница (липса на атрибут lang в html елемента);

- в някои сайтове езикът на страница не съвпада с идентифицирания език - страници с основно съдържание на български език, за които езикът е неправилно определен като английски.

- заглавия, които не описват адекватно и информативно съдържанието на страниците; заглавия, които съдържат само наименованието на организацията;

- 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), напр. започват с наименованието на организацията.

В част от проверените страници се констатира, че документите, които могат да се

изтеглят от тях, са недостъпни за ползвателите 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 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.

До момента общо са публично достъпни федерирани портали на 54 администрации, в т. ч. през 2022 г. са внедрени портали на 33 администрации.

IV. УКРЕПВАНЕ НА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ

Мрежовите и информационните системи се превърнаха в централен елемент на всекидневния живот на фона на бързата цифрова трансформация и взаимосвързаността на обществото, включително в трансграничния обмен. Това развитие води до разширяването на броя на киберзаплахите, пораждайки нови такива, и изисква адаптирани, координирани и новаторски реакции във всички държави членки. Броят, мащабите, сложността, честотата и въздействието на инцидентите се увеличават и представляват съществена заплаха за функционирането на мрежовите и информационните системи. В резултат на това инцидентите могат да причинят финансова загуба, да подкопаят доверието на потребителите и да причинят съществени вреди на икономиката и обществото.

1 Състояние на мрежовата и информационната сигурност

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.

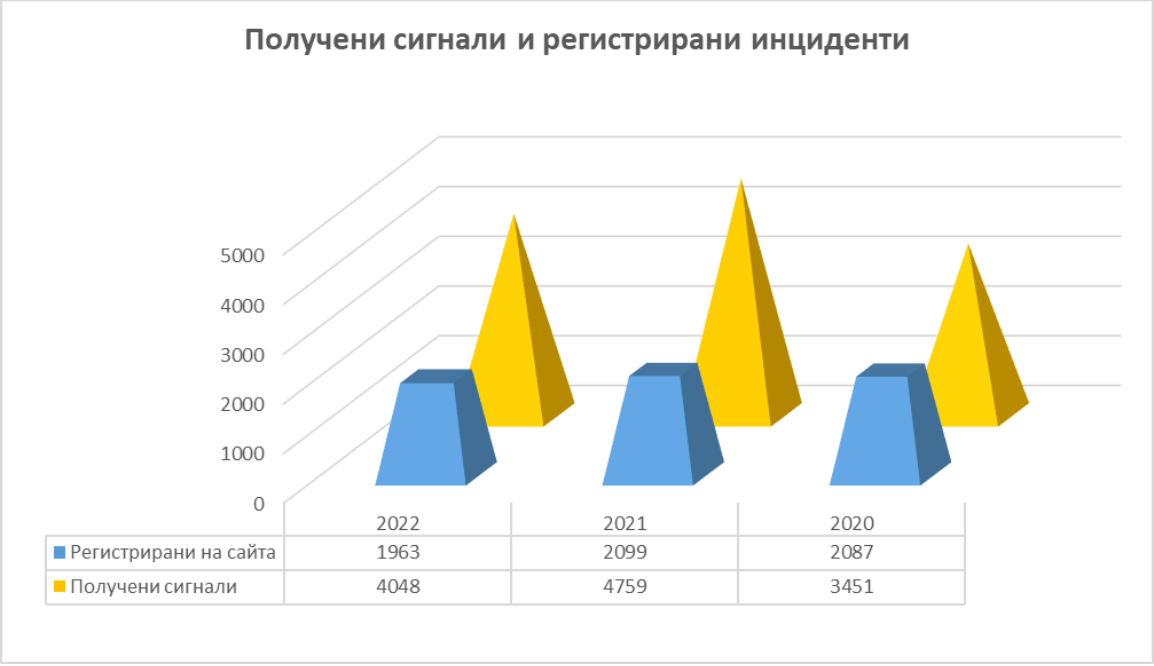
За спазването на законоустановените мерки се извършват регулярни проверки. За периода от 01.01.2022 г. до 31.12.2022 г. са извършени 12 проверки по закона за киберсигурност. Резултатите показват, че продължава тенденцията по-голяма част от администрации да привеждат документацията си съобразно изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност – разработени са вътрешни правила, но все още липсва регулярност при обновяване на политиките за сигурност. Най-големият проблем при класификацията на информацията е, че не е приложена върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето и унищожаването ѝ. Друг проблем е, че не са провеждани регулярно инструктажи за повишаване на вниманието по отношение на мрежовата и информационната сигурност. Информираността на служителите повишава бдителността и компетенциите им и това допринася за намаляване на инцидентите в организацията. На процеса на управление на риска все още не се обръща достатъчно внимание.

Наблюдава се повишаване на сигурността на уебсайтовете на институциите, като голяма част от тях са приложили изискванията на законодателството, но все още има и

такива, които допринасят за понижаване на общото ниво на киберсигурност, като например:

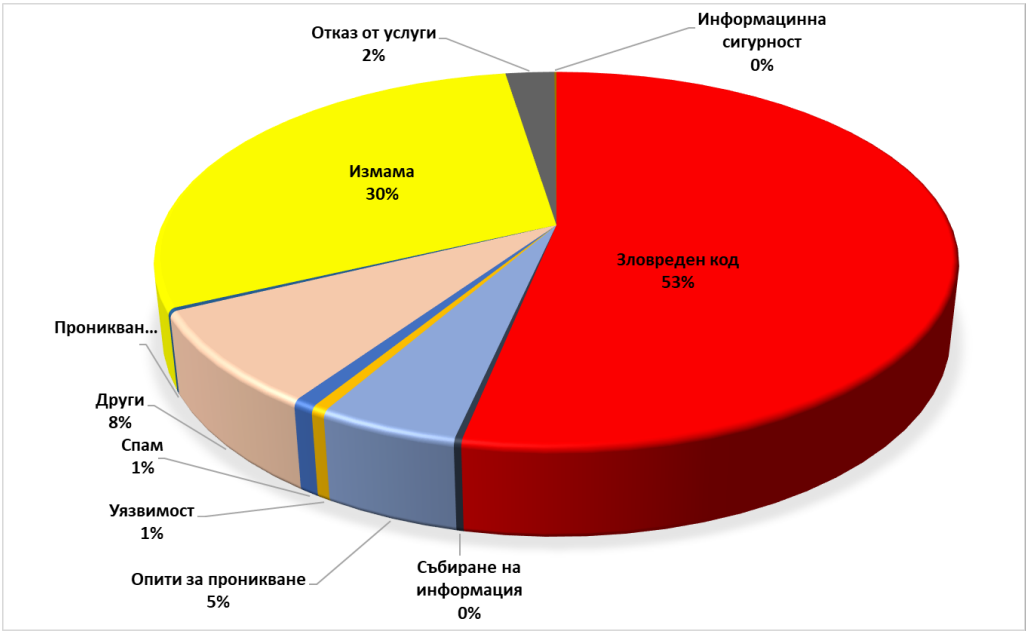
- Информационната система позволява използване на стара версия на протокол TLS версия 1.0 и 1.1;
- Не беше засечено използването на web application firewall;
- Не беше засечена защита от brute force атаки на възможните полета за влизане в системата;
- Не беше установено наличието на DNSSEC;
- Не беше установено наличието на записите DMARC (Domain-based Message Authentication, Reporting and Conformance) и SPF (Sender Policy Framework);
- В хедърите на отговорите на заявките се предоставя информация за вида на платформата;
- В отговорите на HTTPS заявките липсват редица хедъри като HSTS и други.

В периода януари – декември 2022 г. Националният екип за реагиране при инциденти с компютърната сигурност констатира непрекъснато усложняване на обстановката в киберсигурността на страната, като са регистрирани 4048 сигнала. От тях като инциденти, съгласно таксономията на Европейската агенция за киберсигурност – ENISA, са регистрирани 1 963 бр., което представлява намаление на получените сигнали спрямо същия период през изминалата година, както и с броят регистрирани инциденти също се наблюдава леко намаление.

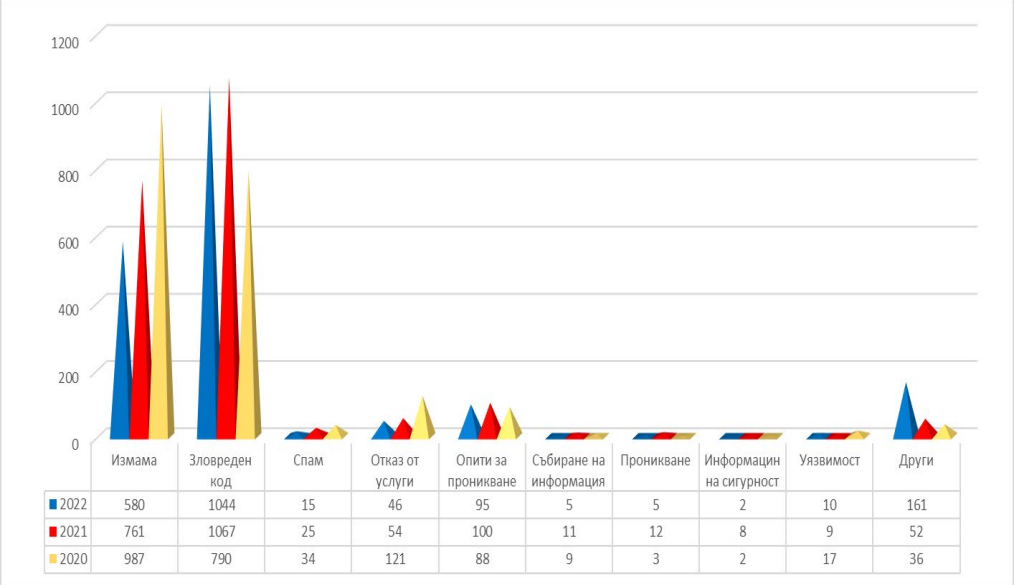


Фигура 24. *Получени сигнали и регистрирани инциденти*

Най-често срещаните причини за инциденти остават разпространение на зловреден код и измама (phishing). С препоръки и указания за разрешаването на инциденти и за преустановяването на нарушения Националният екип за реагиране при инциденти с компютърната сигурност е подготвил и изпратил близо 15 хиляди имейла. На графиките по-долу са показани видовете регистрирани инциденти за отчетния период.



Фигура 25. *Видове регистрирани инциденти за периода 01.01.2022 г.-31.12.2022 г.*



	Измама	Зловреден код	Спам	Отказ от услуги	Опити за проникване	Събиране на информация	Прониква	Информацин на сигурност	Уязвимост	Други
2022	580	1044	15	46	95	5	5	2	10	161
2021	761	1067	25	54	100	11	12	8	9	52
2020	987	790	34	121	88	9	3	2	17	36

Фигура 26. *Сравнителна таблица на видове регистрирани инциденти за периода 01.01.2019 г.-31.12.2022 г.*

Леко нараства относителният дял на инцидентите със значително увреждащо въздействие в мрежовата и информационната сигурност със средна степен на опасност.



Фигура 27. *Сравнителна таблица приоритет на регистрираните инциденти за периода 01.01.2020 г.-31.12.2022 г.*

С избухване на войната в Украйна се наблюдава рязко увеличаване на кибератаките срещу държавите-членки на ЕС, в т.ч. и България. Държавно-спонсорираните хакерски групи продължават да се насочват към субекти в държавите-членки, с цел придобиване на чувствителна информация и прекъсване на важни услуги. Доказателство за това е увеличението с 80 % на DDoS атаките срещу държавната администрация. По данни на Националния екип за реагиране при инциденти с компютърната сигурност за отчетния период има засегнати 193270 IP адреса, което е с близо 40 % по-малко от 2021 г. В таблицата по-долу са представени данни за последните три години, които включват брой засегнати IP адреси и съответно брой изпратени имейли.

	2022	*2021*	*2020*
Засегнати IP адреси	*193270*	*276 970*	*392 283*
Изпратени имейли	*15023*	*18 103*	*18 617*

Таблица 5. *Сравнителни данни за брой засегнати IP адреси и брой изпратени мейли през периода януари - декември 2020 г., 2021 г. и 2022 г.*

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. Шест администрации бяха сериозно засегнати в следствие на успешни рансъмуер атаки. Причините за успешните атаки най-често са уязвимости в системата или човешка грешка, породена от любопитство, незнание или неволно кликване върху зловредния линк или отваряне на прикачен файл.

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 сериозен пробив в сигурността на пощенските сървъри на Microsoft: Exchange Server 2013, Exchange Server 2016 и Exchange Server 2019; уязвимост в ExSi сървър.

На база сключено споразумение между Трой Хънт и Министерство на електронното управление за използване на ресурсите на платформата Have I Been Pwned бе извършена проверка от страна на CERT България и бе установено, че множество служебни акаунти са включени в масив с изтекли данни (data leak) в публичния и Dark Web. Засегнатите потребители бяха своевременно уведомени. В процеса на събиране на актуална информация за използваните служебни адреси, домейни поддомейни бе установено, че много от тях не отговарят на Методическите указания за формиране наименованията на домейните и поддомейните, както и на адресите на електронната поща на административните органи в Република България в съответствие с чл. 47 от Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги, приета с постановление № 3 на Министерския съвет от 2017 г. (ДВ бр.47 от 24.06.2022 г.), в частта от чл. 9 до чл. 15.

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:

2.1. Нормативна уредба

След влизането в сила на Директива (ЕС) 2016/1148 бе постигнат значителен напредък при повишаването на нивото на киберустойчивост на Съюза. Прегледът на посочената директива показа, че е послужила като катализатор за институционалния и регулаторния подход към киберсигурността в Съюза, като е проправила пътя за значителна промяна в нагласите. Директивата осигури завършването на националните рамки относно сигурността на мрежовите и информационните системи чрез създаването на национални стратегии за сигурност на мрежовите и информационните системи и създаването на национални способности и чрез изпълнението на регулаторни мерки, обхващащи съществени инфраструктури и субекти, установени от всяка държава членка. Директива (ЕС) 2016/1148 допринесе и за развитието на сътрудничеството на равнището на Съюза посредством установяването на групата за сътрудничество и мрежата от национални екипи за реагиране при инциденти с компютърната сигурност. Прегледът на Директива (ЕС) 2016/1148 обаче разкри, че независимо от тези постижения, тя има и присъщи слабости, които пречат на намирането на ефективни решения за настоящите и възникващи предизвикателства в областта на киберсигурността. Директива (ЕС) 2016/1148 бе отменена и заменена с ДИРЕКТИВА (ЕС) 2022/2555 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 14 декември 2022 година, относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2)

С отмяната на Директива (ЕС) 2016/1148 приложното поле следва да се разшири така, че да обхване по-голяма част от секторите на икономиката, за да се осигури пълно включване на сектори и услуги от жизненоважно значение за ключови обществени и икономически дейности във вътрешния пазар. По-специално настоящата директива има за цел да преодолее недостатъците, свързани с разграничаването между оператори на основни услуги и доставчици на цифрови услуги, което е доказано остаряло, тъй като не отразява значимостта на секторите или услугите за обществените и икономическите дейности във вътрешния пазар. Засегнатите сектори от седем нарастват на осемнадесет.

С оглед на взаимовръзките между киберсигурността и физическата сигурност на субектите следва да се осигури съгласуван подход между Директива (ЕС) 2022/2557, относно

устойчивостта на критични субекти и Директива МИС 2. За постигането на тази цел субектите, които са установени като критични субекти съгласно Директива (ЕС) 2022/2557 следва да се считат за съществени субекти съгласно настоящата директива. В настоящата Директива МИС 2 се обръща особено внимание на спазването на мерките за управление на риска в областта на киберсигурността и задълженията за докладване.

Предстои транспониране на Директивата МИС 2 в българското законодателство до 17.10.2024 г., което е свързано с промяна на Закона за киберсигурност, Наредбата за минимални изисквания за мрежова и информационна сигурност, Методиката за определяне на операторите на съществени услуги. Трябва да се определят мерки за управление на риска в областта на киберсигурността и национални рамки за управление на кризи в областта на киберсигурността. Предстои актуализация и на националната стратегия за киберсигурност „Киберустойчива България 2023“.

През отчетния период МЕУ пое ангажиментите по досието Cyber Resilience Act като водеща страна заедно с Министерство на икономиката и индустрията. Има изготвена и изпратена рамкова позиция на РБългария. Работата по досието продължава и през следващата година.

През месец септември Европейската агенция по киберсигурност – ENISA, представи разработена Европейска рамка за умения за киберсигурност (ECSF). Европейската рамка за умения за киберсигурност (ECSF) е практически инструмент в подкрепа на идентифицирането и формулирането на задачи, компетенции, умения и знания, свързани с ролите на европейските специалисти по киберсигурност. ECSF обобщава всички роли, свързани с киберсигурността, в 12 профила, които се анализират индивидуално в подробности за съответните им отговорности, умения, синергии и взаимозависимости. Той осигурява общо разбиране на съответните роли, компетенции, необходими умения и знания, улеснява признаването на уменията за киберсигурност и подпомага проектирането на програми за обучение, свързани с киберсигурността. Рамката е допълнена от ръководство за потребителя, което представлява практическо ръководство за нейното използване, базирано на примери и случаи на употреба. Наръчникът включва три примера за частни организации, които трябва да наемат, повишат уменията и/или преквалифицират своя персонал в областта на киберсигурността, заедно със случаи на употреба, които отразяват опита на седем организации, използващи ECSF в различни контексти.

През 2022 год. се проведе едно извънредно заседание на Съвета по киберсигурността (СКС). От съображения за сигурност и по предложение на председателят на Съвета извънредното заседание бе закрито, а всички документи и гласувани решения са класифицирана информация. Протокол от проведеното заседание се съхранява в регистратурата за класифицирана информация на Министерство на електронното управление.

2.2. Национален координационен център

В съответствие с „Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета от 20 май 2021 година за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове“ и на „Устройствен правилник на Министерството на електронното управление“ от 20.05.2022г., приет с ПМС № 89 от 19.05.2022 г., обн. ДВ. бр.38 от 20 Май 2022г., беше създадена и новата структура в дирекция „МИС“ – отдел „Национален Координационен Център“ NCC.bg (НКЦ).

Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността“ (ECCC), създаден в Букурещ, Румъния, през 2021 г., ще помогне на ЕС да запази и развие технологичния и промишлен капацитет за киберсигурност. Чрез управлението на фондовете за киберсигурност в рамките на

следващата многогодишна финансова рамка 21-27‘, ECCC ще помогне за създаването на взаимосвързана индустриална и изследователска екосистема за киберсигурност в целия ЕС. Инициативата ще помогне на ЕС и ДЧ да възприемат проактивна, по-дългосрочна стратегическа перспектива към индустриалната политика за киберсигурност, надхвърляща научноизследователската и развойна дейност. Този подход ще спомогне да се намерят революционни решения за предизвикателствата в киберсигурността, пред които са изправени частният и публичният сектор, и ще подпомогне ефективното внедряване на тези решения. Това ще позволи на съответните научноизследователски и индустриални общности и публични органи да създадат по-широки и по-силни връзки на сътрудничество и да получат достъп до допълващи се знания и капацитет, както и съоръжения за тестване и експериментиране.

Една от основните цели на НКЦ е участието и взаимодействието с „Мрежата от национални координационни центрове (NCCs Network)“, както и създаване на Българска киберобщност. За осъществяване на посочените цели през месец юни бе отворена първата покана за кандидатстване за финансиране по Европейска програма, която предвиждаше да подпомогне създаването и развитието на европейските НКЦ, Мрежата на НКЦ и Кибер-общностите. Програмата Цифрова Европа – „Digital Europe Work Programme 2021-2022“ (DEP) е първата програма на ЕС, която има за цел да ускори възстановяването и да стимулира цифровата трансформация на Европа чрез инвестиции на стойност над 7,6 милиарда евро. Програмата е част от следващия дългосрочен бюджет на ЕС (многогодишната финансова рамка) и обхваща периода от 2021г. до 2027 г.

За съжаление поради ограниченият срок, и провеждащата се трансформация от ДАЕУ към МЕУ, българският НКЦ не успя да се включи в подаването на проектно предложение на тази първа покана (както и по–голямата част от европейските Центрове), тъй като едно от най–важните условия за кандидатстване беше НКЦ да има акредитация от Европейската Комисия. Към днешна дата акредитацията на българското НКЦ е факт, като с официално писмо с реф.№ (2022) 5661876/09.08.2022 г. българския НКЦ беше акредитиран с отлична оценка от Lorena Boix-Alonso - Director, Miguel Gonzalez-Sancho, Martin Ubelhor и Francesco Barbato.

2.3. Национален екип за реакция на инциденти в компютърната сигурност

Министерството на електронното управление, 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.

Проектът “Изграждане на капацитета и подобряване на предоставяните от Националния Център за Действие при Инциденти в Информационната Сигурност услуги“/ Capacity Building and Services Enhancement of CERT Bulgaria (CBSEC-BG) беше осъществен съгласно административен договор № INEA/CEF/ICT/A2018/1801024 за предоставяне на безвъзмездна финансова помощ по процедура CEF-TC-2018-3.

Основната цел на проекта беше повишаване капацитетът на екипите, които се занимават с превенция и реагиране на инциденти в условията на Закона за киберсигурност.

В закона е указано, че се създават национален екип и секторни екипи за реагиране при инциденти с компютърната сигурност, в съответствие с методическите указания на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA). Посочени са всички изисквания, на които трябва да отговарят екипите, за да изпълняват своите дейности. За повишаване капацитета на екипите за реагиране при инциденти в компютърната

сигурност European Health and Digital Executive Agency (HaDEA) като официален представител на Европейската комисия по програма Connecting Europe Facility 2014-2020 Telecommunications Sector подсектор Киберсигурност, се обявиха специални направления за Националните екипи на държавите членки. Българският национален екип за реагиране при инциденти в компютърната сигурност (CERT България), кандидатства с проектно предложение, което беше одобрено през 2019г.. Целта на проекта е повишаване капацитета на CERT България (Националния екип за реагиране при инциденти във връзка с компютърната сигурност) както чрез осигуряване на необходимия технически инструментариум, така и чрез повишаване квалификацията, знанията и уменията на екипа да отговаря на предизвикателствата в сферата на киберсигурността, както и подобряване на разполагаемият инструментариум и подобряването на времето за реакция

Основните дейности, които бяха осъществени в рамките на проекта, са:

- Изграден център за национални и международни обучения в областта на киберсигурността, който позволява провеждането на учения, обучения и тренировки за повишаване на капацитета не само на CERT-BG, но и на секторните ЕРИКС;
- Изградена лаборатория за анализ на зловреден код, която позволява самостоятелен анализ и предприемането на мерки срещу новооткрит зловреден код;
- Изградена лаборатория за forensic анализ, която позволява ускорено възстановяване на работоспособността на засегнатите от инцидент организации;
- Изградена Национална мрежа на екипите за реагиране при инциденти в компютърната сигурност за споделяне на информация за рискове, заплахи и уязвимости, свързани с киберсигурността;
- Присъединихме се към основната платформа за услуги на мрежата на европейските екипи за реагиране при инциденти в компютърната сигурност (MeliCERTes Core Services Platform) за международно сътрудничество в областта на киберсигурността;

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 срещи със секторните ЕРИКС;
- 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 4 национални и международни киберучения;
- 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.

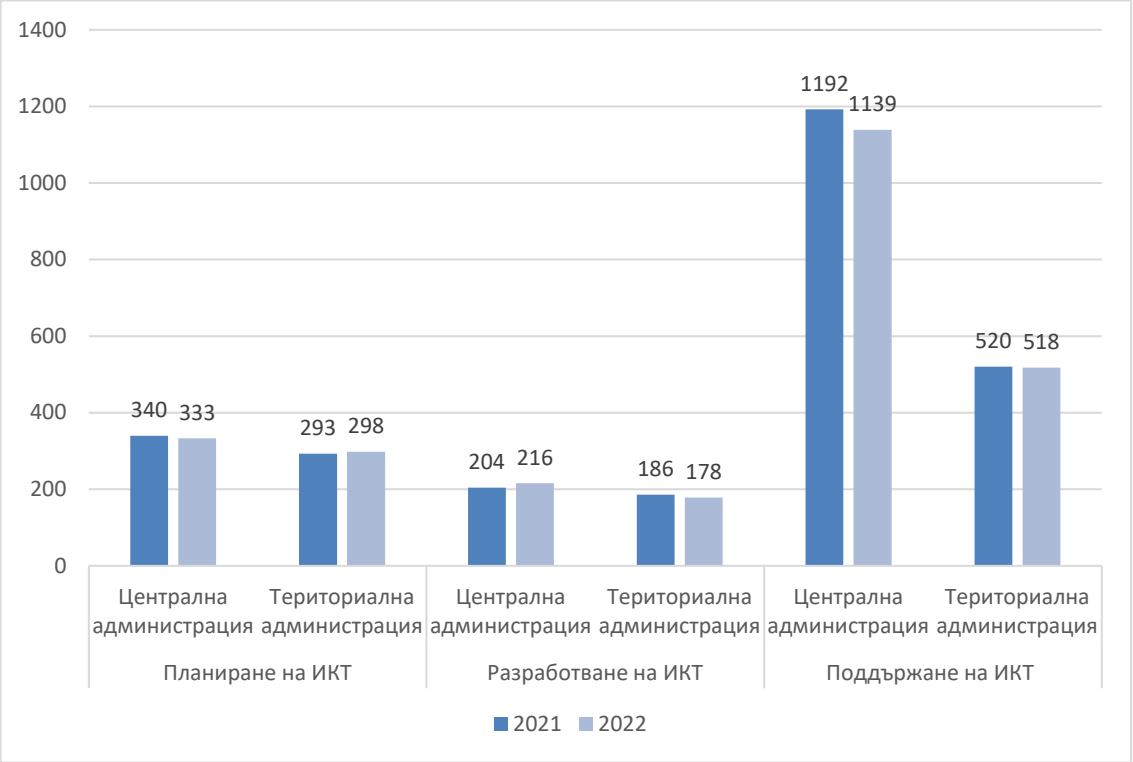
V. ЧОВЕШКИ РЕСУРС В ИКТ

За 2022 г. се запазва тенденцията малко повече от 37% от администрациите да разполагат с вътрешен ресурс – вътрешна структура (дирекция, отдел, звено) или отделни специалисти, които да отговарят и извършват поддръжка на информационните ресурси. В сравнение с предходния отчетен период администрациите, които ползват както вътрешен, така и външен ресурс (външен изпълнител) нараства с около 2%, достигайки 30% от всички.

175 администрации или 30% от всички през 2022 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, за 2022 г. малко над 50% от централната администрация ползва външен изпълнител или смесен подход (вътрешен ресурс и външен изпълнител) за поддръжката на информационните ресурси, а дела на централните администрации, които разчитат изцяло на вътрешен капацитет е малко под 50 %. Запазена е тенденцията от 2021 г. при структурите на териториалната администрация, където 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 резултатите по отношение на поддръжката на споделените ресурси все повече се налага необходимост от създаване на 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. Реализирането на тази необходимост ще доведе до оптимизиране на разходите за поддръжка и развитие на информационните ресурси за постигане на ефективност и ефикасност в държавната администрация.

За 2022 г. общият брой на служителите в администрацията, занимаващи се с планиране, разработка или поддръжка на информационни ресурси е 3 091 или с 574 повече спрямо 2021 г. Забелязва се намаляване на служителите в териториалните с 1% и в централните администрации с близо 3%. Детайлна разпределение на служителите по вид функция и вид администрация е представено в фигурата по-долу:



Фигура 28. *Брой служители в администрацията, ангажирани с ИР*

Остава необходимостта от разработването на единна политика за човешките ресурси в държавната администрация, която 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, данните от 2022 г. потвърждават необходимостта от повишаване на капацитета на служителите, отговарящи за ИКТ в администрацията, което е от 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.

Съгласно цитираната разпоредба, всички административни органи изпращат за предварително съгласуване от председателя/ министъра на ДАЕУ[13] /Министерство на електронното управление /МЕУ/ 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 през 2020 г. 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 Средата за междурегистров обмен на данни.

По предоставената към момента на изготвяне на настоящия отчет информация за отчета за касовото изпълнение на утвърдения бюджет за е-управление и ИКТ за 2022 г., административните органи са изразходвали общо **115 491 100** лв.

През октомври 2022 г., във връзка с подготовката и представянето на проектобюджетите на първостепенните разпоредители с бюджет за 2023 г. и актуализираните им бюджетни прогнози за 2024-2025 г. бяха съгласувани по целесъобразност средства целеви средства за е-управление и ИКТ за 2023 г. в размер на 78 684 400 лева, представени в ИСБК от 24 административни органи-първостепенни разпоредители с бюджет.

Следва да се отбележи, че 9 от най-големите общини в страната, а именно областните центрове, или не са предоставяли никаква чрез ИСБК до 31.12.2022 г. или са попълвали частично такава, или не са спазвали сроковете са представянето й. В резултат на активните проверки от страна на МЕУ през последното тримесечие на 2022 г., бяха установени редица нарушения за тези 9 общини, а като ефект беше постигнато значително нарастване на обема от данни и информация, която се вписа за съгласуване в ИСБК.

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

- 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“. В резултат на извършените проверки бе постигнато значително дисциплиниране на администрациите по отношение на вписването на проектни предложения и дейности в Регистъра на проектите и предоставянето им за утвърждаване по реда на чл. 7в, ал. 2, т. 10 от ЗЕУ, като нарасналия в пъти брой на представените за съгласуване данни в Информационната система за бюджетен контрол и Регистъра на проектите, говорят сами по себе си за постигнатите резултати по осъществяване на контролната дейност на МЕУ и повишаването на авторитета на министерството. През отчетния период, съвместно с отдел СПЕУ в дирекция ПЕУ и дирекция МИС, са извършени 221 проверки на проектни предложения и дейности, като по 4 от тях е направен отказ за утвърждаване. За сравнение, за цялата 2021 г. проверките на проектни предложения и дейности са били 43.

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 2022 г. е 78, 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 пет решения за отказ за удостоверяване на съответствието с изискванията на чл. 58а от ЗЕУ.

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, Среда за междурегистров обмен на данни 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 МЕУ 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 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.

През 2022 г. са извършени 298 броя проверки, от които 287 бр. планови проверки за спазване на изискванията на ЗЕУ, ЗКС и подзаконовите нормативни актове по прилагането им и 11броя проверки по постъпили сигнали от граждани и организации. В резултат на извършените проверки са съставени 291 бр. протоколи/резултати от извършени проверки със дадени задължителни предписания, изготвени са 4 броя доклади след извършени проверки по ЗКС и са съставени 2 броя актове за установяване на административно нарушение.

Пример за нарушения и пропуски при изпълнение на изискванията на ЗЕУ са:

- 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.;

Пример за нарушения и пропуски при изпълнение на изискванията на ЗКС са а:

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

- 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.

Може да се отбележи, че в регулярно разглежданите проектни предложения приоритетно се наблюдава липса на адекватни и комплексни изисквания за мрежова и информационна сигурност, основани на анализ и оценка на риска, с цел да се гарантира, че изискваното ниво на сигурност на информацията, мрежите и информационните системи е заложено още в етапа на разработка и внедряване.

Анализът и оценката на риска са основополагащите елементи, посредством които се идентифицират рискове и конкретни заплахи за информационната система. Въз основа на така идентифицираните рискове и заплахи, следва да се въведат механизми за тяхното смекчаване с цел постигане на определено ниво на сигурност на информацията, мрежата или информационната система. Основно водещо правило при имплементиране на смекчаващи механизми е използването на такива, които са пропорционални на рисковете, в частност на щетите, които те биха могли да нанесат.

Необходимостта от включване в техническата спецификация на изисквания за конкретни адекватни и пропорционални на рисковете смекчаващи механизми, които се основават на анализ и оценка на риска, трябва да бъде допълнено с ясно аргументирана връзка между механизмите и анализа и оценката на риска, като бъде описано по ясен и еднозначен начин.

VII. СЪЩЕСТВУВАЩИ ОГРАНИЧЕНИЯ ПРИ ИЗТОЧНИЦИТЕ НА ИНФОРМАЦИЯ

1 Интегрирана информационна система на държавната администрация

По отношение на ИИСДА идентифицираните проблеми и пропуски продължават от 2021 г., 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 –.

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.

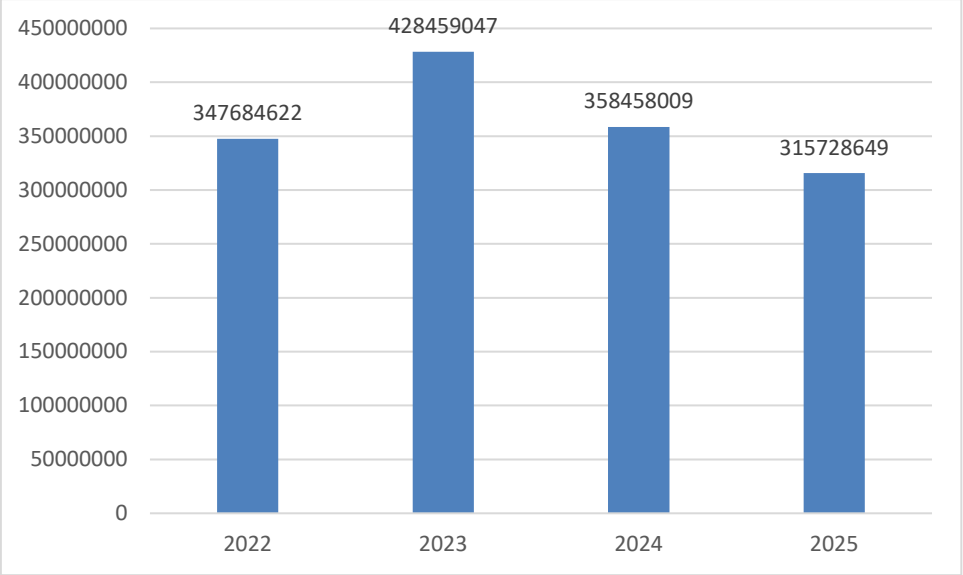
Регистърът функционира като самостоятелна система, която има ограничена интеграция с ключовата за контрола на разходите за електронно управление Информационна система за бюджетен контрол единствено в частта за годишно планиране на ресурсите. Взаимното обвързване на РИР и ИСБК има потенциала за доведе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

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 2022 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 31.12.2022 г. 578 административни органа са въвели общо 15 192 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 **1 450 330 327** лева. Разпределението съответно за 2022 г., 2023 г., 2024 г. и 2025 г. може да се види на фигура 28.



Фигура 29. *Планирани средства за обновяване на ИКТ ресурси*

В раздел Годишен план в РИР за 2023 г. 249 административни органа са въвели 3411 записа са. 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 428 459 047 лв., като по-голямата част от тях - 96,96% - в централната, специализираната териториална и областната администрация, а 3,04%- в общински администрации.

Годишните планове за 2023 г. за група „хардуерен и мрежови информационен ресурс“ са на стойност 112 936 772 лв. като 95,31% от тази сума е заложена от централната, специализираната териториална и областната администрация, а 4,69% - от общинските администрации.

Планираните средства за 2023 г. за група „софтуер“ са на стойност 256 570 751 лв. като 99,59% са заложени от централната, специализираната териториална и `областната администрация, а 0,41% са заложени от общинските администрации.

От планираните за 2023 г. средства за група „лицензи“ – 5 138 296 лв., почти цялата сума е заложена от централната, специализираната териториална и областната

администрация, докато 0,92% от сумата представлява прогнозите на общинските администрации.

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

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 и през 2023 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.

Въз основа на анализа и на данните от отчета очертаните през предходния период стъпки, следва да бъдат реализирани през 2023 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 продължат засилените проверките от страна на МЕУ по ЗЕУ и ЗКС, 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 към оценка на бюджетите на проектните 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 бележат броят на изпратени съобщения през системата за сигурно електронно връчване и броят на вътрешните електронни административни услуги. Единният модел за централизирано заявяване, заплащане и предоставяне на електронни административни услуги оказа въздействие за подобряване на качество и стандартизирането на процесите по предоставяне на услугите, икономии за бизнеса и гражданите, както и осезаемото подобряване на бизнес средата в България. Повишеното използване на системите на електронното управление носи значителни ползи (спестено време, екологосъобразност, ефикасност на ресурси, осигурява гъвкавост) за гражданите, бизнеса и, като цяло, за публичния сектор, но и създава значителен обем от данни.

Тенденцията за нарастване на потреблението носи съществени ползи както за администрациите, така и за гражданите и бизнеса. Гражданите и бизнесът вече ползват възможността да взаимодействат изцяло цифрово с администрациите през Системата за електронно връчване. Вече е възможно по електронен път да се контролира как институциите използват нашите данни чрез предоставяната от МЕУ услуга „Персонална справка на физическо лице за достъп до лични данни по идентификатор (ЕГН) и период“. Тази услуга все повече се ползва като ефективен инструмент за граждански контрол върху институциите, но и за повишаване на качеството на данните в основните регистри на държавата, при гарантиране на необходима защита на личните данни.

Предприемат се конкретни действия за ефективното прилагане на един от основните

принципи на електронното управление – администрациите да обменят данни помежду си служебно, вместо да ги изискват от гражданите и от бизнеса. Основните регистри и системи на централната администрация вече са свързани през Средата за междурегистров обмен на данни.

Само генерираните през системата за междурегистров обмен над 200 милиона заявки до края на 2022 г. са спестили много над 200 милиона лева на обществото на базата на премахната необходимост да се посещават физически администрации и да се предоставят на хартия удостоверения за настоящ, постоянен адрес, семейно положение, липса на задължения и редица други.

Създадената възможност за заплащане на задължения чрез Централен виртуален ПОС, премахва необходимостта гражданите да заплащат преводни такси и комисионни, както и осигурява възможност за заплащането им от всяка точка на света с кредитни или дебитни карти издадени включително и извън страната. Акцент за 2023 г. трябва да е бързата интеграция на неприсъединените администрации със системата за еПлащане.

По отношение на информационните системи е необходимо те да отговарят на единен критерий за внедряване, експлоатация и поддръжка, което да осигури безпроблемно и сигурно функциониране на електронното управление. Интегрирането на информационните системи на администрациите с хоризонталните и централизираните системи на електронното управление е задължително, за което следва да се предвиди необходимият бюджетен ресурс в рамките на тригодишните бюджетни прогнози. Следва регулярно и устойчиво да се предвижда бюджетен ресурс и за поддържане на информационните системи.

Все още не е изградена националната схема за електронна идентификация, предвидена в Закона за електронната идентификация, което забавя 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 в максимална степен да се разширят средствата за електронна идентификация с наложили се и използвани в държавите членки такива, както и интеграцията с eIDAS възли на същите.

През 2022 г. е увеличен броят на потребителите на облачни услуги, предоставяни от ДХЧО. Продължава развитието на ДХЧО, изразяващо с измерими количествени показатели като предоставено дисково пространство и брой виртуални машини. Нараснал е броят на министерствата и ведомствата, използващи колокация на инфраструктура в центровете за данни

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.

За разлика от 2021 г. в голяма част от администрациите има определен служител или административно звено, отговарящ за мрежовата и информационната сигурност.

Най- голям е процентът на регистрираните инциденти, дължащи се на зловреден код (malware), следвани от измама (phishing). С избухване на войната в Украйна се наблюдава рязко увеличаване на кибератаките срещу държавите-членки на ЕС, в т.ч. и България. Държавно-спонсорираните хакерски групи продължават да се насочват към субекти в държавите-членки, с цел придобиване на чувствителна информация и прекъсване на важни услуги.

В областта на човешките ресурси в ИКТ е необходимо разработването на единна политика за човешките ресурси в държавната администрация. За успешната реализация на политиката за е-управление, за информационната сигурност и за изграждането на ефективна цифрова администрация е необходимо повишаване на капацитета и мотивацията на

служителите, отговарящи за ИКТ в администрацията. Без високо компетентни и мотивирани служители в областта на ИКТ няма как да се посрещнат предизвикателствата, свързани с цифровата трансформация на обществото ни и повсеместното прилагане на съвременни технологични решения в областта на управлението на данни, изкуствен интелект, анализи, прогнози и на тяхна база вземане на максимално обективни решения.

Огромни са предизвикателствата в тази посока, при постигането на които тотално ще се промени качеството на живот и обществени взаимоотношение.

Анализът на данните в Информационната система за извършване на предварителен, текущ и последващ контрол по целесъобразност показва сравнително нисък процент усвояемост, което поставя множество въпроси 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.

ЗАКЛЮЧЕНИЕ

Гарантирането на устойчив модел за дългосрочно е-управление налага продължаване на целенасочената политика за постигане на оперативна съвместимост и системна интеграция на информационните ресурси на администрациите. Въпреки постигнатия напредък във всички области на политиката за електронно управление и мрежова и информационна сигурност все още не можем да говорим за единна информационна и технологична екосистема на държавната администрация.

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

Основните изводи се основават на данните и информацията за състоянието на информационните ресурси на администрациите в 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 2023 г. следва да се работи по тяхното отстраняване.

Приложение № 1:

Най-често заявявани централизирано услуги през 2022 г.

Номер и наименование на услуга	*Администрация предоставящ услугата*	*Брой заявявания*
Издаване на удостоверение за данъчна оценка на недвижим имот и незавършено строителство	*Общински администрации*	*7 876*
Издаване на удостоверение за наличие или липса на задължения по Закона за местните данъци и такси	*Общински администрации*	*5783*
Данъчна декларация по чл.14 от ЗМДТ за облагане с данък върху недвижимите имоти	*Общински администрации*	*3585*
Отпускане на месечни помощи за дете до завършване на средно образование, но не повече от 20-годишна възраст по реда на...	*Агенция за социално подпомагане*	*3515*
2198 Освобождаване на лица от винетни такси при ползване на републиканските пътища	*Агенция за социално подпомагане*	*3 468*
Издаване на удостоверение за наследници	*Общински администрации*	*3 282*
Приемане на заявления и регистрация на търсещи работа лица	*Агенция по заетостта*	*2 841*
Отпускане на еднократна помощ за ученици, записани в осми клас	*Агенция за социално подпомагане*	*2597*

Приложение № 2:

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

с най-голям брой системи, присъединени към

Средата за междурегистров обмен на данни

Консуматор	*Брой системи*	*% системи*
Министерство на електронното управление	*11*	*12*
Национален статистически институт	*10*	*12*
Изпълнителна агенция "Автомобилна администрация"	*6*	*7*
Министерство на външните работи	*2*	*7*
Агенция "Митници"	*6*	*7*
Агенция по заетостта	*4*	*5*
Министерство на правосъдието	*6*	*5*
Община Пловдив	*2*	*5*
Агенция по вписванията	*4*	*4*
Изпълнителна агенция по рибарство и аквакултури	*3*	*4*
Министерство на туризма	*3*	*4*
Районен съд -Поморие	*2*	*4*
Столична община	*3*	*4*
Агенция "Пътна инфраструктура"	*3*	*2*
Агенция за устойчиво енергийно развитие	*2*	*2*
Администрация на Министерски съвет	*3*	*2*
Изпълнителна агенция по околна среда	*2*	*2*
Министерство на здравеопазването	*3*	*2*
Министерство на земеделието	*4*	*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*

СПИСЪК НА ФИГУРИТЕ

Фигура 1. Разпределение на работните станции по година на придобиване 9
Фигура 2. Брой разработени услуги по години 11
Фигура 3. Брой присъединени към Единния модел администрации по години 12
Фигура 4. Справка за посещения на портала за 2022 г., вида устройство и видове операционни системи,..... 13
Фигура 5. Статистика за успешно автентикирани потребители със средства, поддържани от системата..... 14
Фигура 6. Интегрирани системи на доставчици на услуги към системата еАвт 2.0..... 14
Фигура 7. Справка за посещения на системата за електронна автентикация за 2022 г., видове устройства и видове операционни системи 15
Фигура 8. Брой АИС клиенти в системата за е-Плащане..... 16
Фигура 9. Статистика за присъединени АИС клиенти на администрации и преминали трансакции в системата за е-Плащане..... 16
Фигура 10. Справка за посещения на системата за електронно плащане за 2022 г., показатели за ефективност, видове операционни системи 17
Фигура 11. Брой заявявания на ЕАУ по години..... 18
Фигура 12. Брой регистрираните потребители в ССЕВ по години 19
Фигура 13. Справка за обменените съобщения по години 19
Фигура 14. Справка за посещения на системата за сигурно електронно връчване за 2022 г., вид на устойствата и видове операционни системи 20
Фигура 15. Справки и посетени регистри за 2022 г. 21
Фигура 16. Топ 5 посещавани администрации през 2022 г. 21
Фигура 17. Топ 5 „Консуматор“ на справки..... 22
Фигура 18 Справка за посещения на системата за електронно плащане за 2022 г., показатели за ефективност, видове операционни системи 23
Фигура 19 Заетост на продукционната среда за клъстер 1 на ДХЧО..... 29
Фигура 20. Заетост на продукционната среда за клъстер 2 на ДХЧО..... 29
Фигура 21. Използваемост на хранилището за данни за клъстер 1 на ДХЧО 32
Фигура 22. Използваемост на хранилището за данни за клъстер 2 на ДХЧО 33
Фигура 23. Брой услуги от ниво 3 или ниво 4 по години..... 34
Фигура 24. Получени сигнали и регистрирани инциденти 38
Фигура 25. Видове регистрирани инциденти за периода 01.01.2022 г.-31.12.2022 г..... 39
Фигура 26. Сравнителна таблица на видове регистрирани инциденти..... 39
Фигура 27. Сравнителна таблица приоритет на регистрираните инциденти за периода 01.01.2020 г.-31.12.2022 г. 40
Фигура 28. Брой служители в администрацията, ангажирани с ИР 45
Фигура 29. Планирани средства за обновяване на ИКТ ресурси..... 53

СПИСЪК НА ТАБЛИЦИТЕ

Таблица 1. Въведени активи в РИР..... 10
Таблица 2. Разпределение на антивирусния софтуер..... 10
Таблица 3. Администрации, които нямат внедрени информационни системи. Източник ИИСДА... 24
Таблица 4. Списък на държавните организации, ползващи ресурси в ДХЧО 28
Таблица 5. Сравнителни данни за брой засегнати IP адреси и брой изпратени мейли през периода януари - декември 2020 г., 2021 г. и 2022 г. 40