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 2024 г.

СЪДЪРЖАНИЕ

СЪДЪРЖАНИЕ 2
СЪКРАЩЕНИЯ 4
I. ВЪВЕДЕНИЕ 6
II. СТРАТЕГИЧЕСКА РАМКА ЗА РАЗВИТИЕ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ 7
1. Стратегия за развитие на електронното управление в Република България 2019 – 2025 г. 7
2. Единна политика за информационните ресурси 7
3. Архитектура на електронното управление 8
4. Основни източници на информация за състоянието на информационните ресурси 9
5. Референтна архитектура за оперативна съвместимост 9
III. СЪСТОЯНИЕ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ В АДМИНИСТРАЦИЯТА 10
1. Обезпеченост на администрациите с хардуер 10
2. Обезпеченост на администрациите със софтуер и лицензи 12
3. Информационни системи 13
3.1. Хоризонтални системи на електронното управление 13
3.1.1. Портал на електронното управление (egov.bg) 13
3.1.2. Система за е-Автентикация 15
3.1.3. Система за електронно плащане (е-Плащане) 16
3.1.4. Система за проверка валидността на персонален цифров сертификат (е- Валидиране) 18
3.1.5. Система за управление на електронни форми (е-Форми) 18
3.1.6. Система за сигурно електронно връчване (ССЕВ, е-Връчване) 19
3.2. Централизирани системи за е-управление 20
3.3. Информационни системи в администрациите 22
4. Електронна идентификация 23
4.1. Електронна идентификация за нуждите на заявяване на ЕАУ 23
4.1.1. По реда на Закона за електронната идентификация (ЗЕИ). 23
4.1.2. Със средства за електронна идентификация с ниво на осигуреност „високо“, издадено в рамките на удостоверителна услуга за електронна идентификация с национално покритие, вписана в Доверителния списък, воден от Комисията за регулиране на съобщенията по чл. 22 от Регламент (ЕС) № 910/ 2014. 24
4.1.3. С други средства за електронна идентификация, определени с Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги (НОИИСРЕАУ) - квалифициран електронен подпис (КЕП), включително облачен/ мобилен КЕП, персонални идентификационни кодове, издавани от Националния осигурителен институт и от Националната агенция за приходите, както и уникален код за достъп, издаван от Националната здравноосигурителна каса. 24
4.2. Трансгранична електронна идентификация 25
5. Регистри, поддържани от администрацията. 25
6. Споделени информационни ресурси 26
6.1. Държавен хибриден частен облак (ДХЧО) 27
6.2. Единна електронна съобщителна мрежа (ЕЕСМ) 29
6.3. Хранилище за данни на електронното управление 30
7. Предоставяне на електронни административни услуги 30
7.1 Състояние на електронните административни услуги 30
7.2 Осигуряване на институционална идентичност и достъпност на уебсайтовете 31
IV. УКРЕПВАНЕ НА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ 32
1. Състояние на мрежовата и информационната сигурност 32
2. Мерки за повишаване нивото на мрежовата и информационната сигурност 37
2.1. Нормативна уредба 37
2.2. Национален координационен център (НКЦ) 38
2.3. Национален екип за реакция на инциденти в компютърната сигурност 38
V. ЧОВЕШКИ РЕСУРС В ИКТ 38
VI. КОНТРОЛ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ 40
1. Контрол в рамките на бюджетния процес на разходите за е-управление и ИКТ 40
2. Контрол в процеса на утвърждаване на проектни предложения/дейности 41
3. Контрол за спазване на задължителните изисквания при изготвяне на технически спецификации 42
4. Контрол по спазване на изискванията на ЗЕУ, във връзка с осъществяване на административнонаказателната дейност на МЕУ 43
VII. СЪЩЕСТВУВАЩИ ОГРАНИЧЕНИЯ ПРИ ИЗТОЧНИЦИТЕ НА ИНФОРМАЦИЯ 43
1. Интегрирана информационна система на държавната администрация 43
2. Регистър на информационните ресурси (РИР) 44
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 44
IX. ИЗВОДИ 47
X. ЗАКЛЮЧЕНИЕ 49

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*
АУАН	*Акт за установяване на административно нарушение*
ГКПП	*Граничен контролно-пропускателен пункт*
ЗАНН	*Закон за административните нарушения и наказания*
МЕУ	*Министерство на електронното управление“*
ДХЧО	*Държавен хибриден частен облак*
ЕАУ	*Електронни административни услуги*
ЕЕСМ	*Единна електронна съобщителна мрежа*
ЕРИКС	*Екипи за реагиране при инциденти с компютърната сигурност*
ПЕУ	*Портала на електронното управление*
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*
ИСПОДСА	*Информационна система за попълване на отчетите за дейността и състоянието на администрацията*
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*
КЕП	*Квалифициран електронен подпис*
КИН	*Клиентски идентификационен номер*
КПКОНПИ	*Комисия за противодействие на корупцията и за отнемане на незаконно придобитото имущество*
МИС	*Мрежова и информационна сигурност*
МС	*Министерски съвет*
НАП	*Националната агенция за приходите*
НМИМИС	*Наредба за минималните изисквания за мрежова и информационна сигурност*
НКЦ	*Национален координационен център*
НОИ	*Национален осигурителен институт*
НОИИСРЕАУ	*Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги*
ОА	*Областна администрация*
ПИК	*Персонални идентификационни кодове*
РМС	*Решение на Министерския съвет*

РИР	*Регистър на информационните ресурси*
СЕОС	*Среда за електронен обмен на съобщения*
СОСП	*Съобщителен обект със специално предназначение*
ССЕВ	*Система за сигурно електронно връчване*
ЦВПОС	*Централен виртуален ПОС терминал*

I. ВЪВЕДЕНИЕ

В настоящия отчет се разглежда текущото състояние и се очертава годишен план за развитие и обновяване на информационните ресурси в администрацията и информационните ресурси на Единната електронна съобщителна мрежа на държавната администрация, както и за нуждите на националната сигурност.

Въвеждането на технологични иновации и усъвършенстването на информационните системи са от ключово значение за повишаването на ефективността и прозрачността на административните процеси, както и за укрепването на националната сигурност. Развитието на цифровата инфраструктура и подобряването на електронните услуги не само улесняват гражданите и бизнеса в тяхното ежедневие, но и допринасят за по-бързата и ефикасна комуникация между различните нива на управление. С оглед на това, отчетът подчертава важността на планирането и изпълнението на стратегически инициативи, които целят не само поддържането, но и непрекъснатото обновяване и разширяване на информационните ресурси. В отчета е представен анализ на съществуващата инфраструктура, идентифицирани предизвикателствата и очертава конкретни цели за устойчиво развитие, които да бъдат постигнати в следващия планов период. Чрез изложените стратегически насоки и предложения за действие, отчетът служи като основа за вземане на информирани решения и формиране на политики, насочени към модернизацията на административната работа и повишаване на националната сигурност.

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, предизвика бързи промени в технологиите и не на последно място промени в икономическите условия в страната. Вследствие на всичко това през 2023 г., в отговор на нарастващите изисквания, държавните администрации активно продължават да разширяват и оптимизират своите услуги, следвайки стабилен път към по-напреднало електронно управление.

През септември 2023 година са приети промени в ЗЕУ, целящи съществено ускоряване на процеса на развитие на електронното управление в Република България и реални ползи за гражданите и бизнеса, за намаляване на административната тежест и стимулиране на потреблението на електронни административни услуги. Законът за изменение и допълнение на Закона за електронното управление (ЗИД на ЗЕУ, ДВ бр. 80 от 2023 г.) е обнародван на 19 септември 2023 г.

В края на 2023 г. с Решение на Министерския съвет № 797 от 13 ноември 2023 г. бе приет актуализиран Национален план за въвеждане на еврото в Република България и включените като приложение към него „Методически указания за адаптирането на информационните системи на административните органи във връзка с въвеждането на еврото в Република България“. Методическите указания целят да гарантират точното и еднакво прилагане на изискванията за въвеждане на еврото от административните органи при привеждането на информационните им системи към работа с евро. Предвид крайния

срок за адаптиране (не по-късно от три месеца преди датата на въвеждане на еврото в Република България), всички администрации своевременно трябва да предприемат необходимите действия по адаптирането на информационните си системи за работа с евро.

Развитието на процесите на цифрова трансформация и новата реалност за България, свързана с въвеждането на еврото, налагат администрацията да актуализира използваните в дейността си ИКТ решения.

Отчетът представя информация относно състоянието на информационните ресурси (ИР) в администрациите за периода от 1 януари до 31 декември 2023 г.

II. СТРАТЕГИЧЕСКА РАМКА ЗА РАЗВИТИЕ НА ИНФОРМАЦИОННИТЕ РЕСУРСИ

За осъществяване на цялостна координация, сътрудничество и консултация при разработването, провеждането, мониторинга и оценката на държавната политика в областта на цифровата трансформация в Република България, с Постановление № 60 от 19 април 2023 г. за изменение на Постановление № 38 на Министерския съвет от 29 март 2022 г., е създаден Съвет по цифровото десетилетие, като орган на Министерския съвет. Председател на съвета е министърът на електронното управление. Съветът провежда държавната политика във взаимодействие с други органи на изпълнителната власт. Основната му цел е да гарантира ефективното и качествено участие на България в разработването, изпълнението и отчитането на мерките и дейностите, свързани с Европейската политическа програма „Цифрово десетилетие“ до 2030 г.

Европейската политическа програма „Цифрово десетилетие“ до 2030 г. определя пътя за цифрова трансформация на европейските икономики и общества и поставя конкретни цифрови цели за изпълнение до 2030 г. Една от посочените цифрови цели е в основна област цифровизация на обществените услуги, с която се цели гарантиране на възможността за онлайн участие на всеки в демократичния живот. Достъпността в надеждна и сигурна онлайн среда до обществените услуги, услугите в сферата на здравеопазването и социалните грижи за всички, изисква приобщаващи, ефикасни, оперативно съвместими и персонализирани услуги и инструменти с високи стандарти за сигурност и неприкосновеност на личния живот.

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 се предвижда създаването на Единно европейско пространство на данните и прилагането на нови модели за събиране, обработка, използване и преизползване, съхранение и сигурност на данните.

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 с хоризонт 2025 г. Предвид инициативите на европейско ниво, през 2023 г. започна изготвянето на нов стратегически документ за развитие на електронното управление, информационните технологии и информационното общество с хоризонт на действие 2030 г. В допълнение се изготвят нови механизми за наблюдение и оценка на изпълнението на целите и дейностите.

2. Единна политика за информационните ресурси

Единна политика за информационните ресурси, която обединява и стандартизира

управлението на информационните ресурси във всички държавни институции, подобрява ефективността и намалява разходите чрез централизация и оптимизация на ИТ ресурсите и инфраструктурата.

С РМС № 296 от 2 април 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 международен план налагат разработването на политика за развитие на информационните ресурси, която да бъде съобразена и с предизвикателствата, очертани от текущото състояние на ИР в държавната ни администрация. Това налага ЕПИР да бъде допълнена със съответните правила, стандарти и процедури за развитие и управление на ИР, като за прилагането ѝ да бъдат разработени методически указания към администрациите.

В тази връзка, като част от Програмата за управление на Република България юни 2023 г. – декември 2024 г., се изпълнява мярка „20.2.15. Подготвена политика за развитие на информационните ресурси, която включва и политика за развитие и поддръжка на споделените ресурси на електронното управление“. От Министерството на електронното управление е изготвен проект на нова Единна политика за информационните ресурси. В документа е отразен напредъкът и постигнатите цели по провеждане на политиката, заложен е подход към ускоряване на процесите по цифрова трансформация на администрацията и подобряване на качеството на предоставяните услуги чрез целесъобразно разходване на средства и прилагане на единни централизирани подходи за изграждане на информационната инфраструктура. В ЕПИР са отразени и изменения и допълнения в Закона за електронното управление (изм. и доп. ДВ. бр.15 от 22 февруари 2022 г., доп. ДВ. бр.66 от 1 август 2023 г., изм. и доп. ДВ. бр.80 от 19 септември 2023 г.).

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 прилага единния модел за заявяване, заплащане и предоставяне на електронни административни услуги (ЕАУ), както и изграждане и развитие на споделени информационни ресурси и предоставянето им за децентрализирано управление и използване. Архитектурата налага преход от фрагментирани и затворени към цялостни и технологично независими решения и поетапна промяна на модела на съхранение на данните от децентрализиран към централизиран такъв.

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, както и промените в институционалната, стратегическата и нормативната рамка, през 2023 г. стартира работата по актуализиране и развитие на Архитектурата.

За прилагането на националната Архитектура, като задължителен документ и модел, е необходимо да бъдат разработени архитектури по области на политики от съответните компетентни административни органи. Предвидено е създаването на механизъм за осъществяване на ефективна координинация на разработването и одобряването на проектите на архитектури по области на политики и наблюдението на тяхното изпълнение.

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 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 от министъра на електронното управелние 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. В него се въвеждат информационните ресурси на Единната електронна съобщителна мрежа (ЕЕСМ) на държавната администрация и за нуждите на националната сигурност. Администрациите подават в РИР и годишните си планове за обновяване на ИР.

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

Референтната архитектура за оперативна съвместимост (РАОС) е разработена в съответствие с Европейската референтна архитектура EIRA, Европейската рамка за оперативна съвместимост, както и Българската рамка за оперативна съвместимост. Проектът за разработката на Българсктата рамка за оперативна съвместимост е от национално значение, тъй като изграждането и развитието на оперативно съвместими информационни системи в администрациите, следва да бъде в съответствие с РАОС. Чрез Референтната архитектура и Националната рамка за оперативна съвместимост цели създаването на координирана и ефективна система за електронно управление, която да улесни комуникацията и взаимодействието между различните административни структури, бизнеса и гражданите, чрез налагане на стандартизирано описание на информационни обекти, шаблони на споразумения за ниво на обслужване (SLA) в администрациите и други. За постигане на целите и резултатите са ниобходими нормативни изменения. Предложенията за нормативни изменения са подготвени и предстои утвърждаването им.

На Националния портал за оперативна съвместимост https://ros.egov.bg е публикувана информация в помощ на администрациите и ИТ сектора в сферата на оперативната съвместимост.

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 и софтуерни лицензи.

1. Обезпеченост на администрациите с хардуер

Към 31 декември 2023 г. администрациите разполагат със 125 857 бр. работни станции, (спрямо 125 222 бр. към 31 декември 2022 г.), като от тях 65,56% са в централната администрация и 28,87% – в териториалната администрация, а 5,56% са в администрации на отчет пред Народното събрание. Данните в ИИСДА показват, че 44,56% от работните станции са придобити преди повече от 5 г., 26,37% са на възраст между 3 и 5 г., а 29,07% са на възраст до 3 години. Данните показват, че 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.



Източник: Администрация на Министерския съвет, ИИСДА
Фигура 1: Разпределение на работните станции по година на придобиване

По данни на администрациите броят на местата, в които има разположени сървъри в края на 2023 г. са:

- Общ брой сгради, в които има разположени сървърни помещения, използвани от администрацията е 1 115 бр.;
- Общ брой сървърни помещения във всички сгради (локации) – 1 223 бр.;
- Общ брой сървърни помещения във всички сгради (локации), в които има осигурено непрекъснато токозахранване с UPS – 1 128 бр.;
- Общ брой сървърни помещения във всички сгради (локации), в които има

осигурено аварийно токозахранване от дизел-генератор – 255 бр.;

- Общ брой сървърни помещения във всички сгради (локации), в които има осигурена климтизация (охлаждане) в режим 24/7 – 920 бр.

По отношение на сървърите в държавната администрация, по данни в ИИСДА, състоянието им е следното:

- Общият брой на използваните сървъри за 2023 г. е 9 498, като броят на физическите сървъри, които се използват за виртуализация е 1 727, виртуалните сървъри са 7 635, а облачните сървъри са 136.
- Общият обем на физическата памет (RAM) на хостовете за виртуализация е 5 312 132,18. Общият обем на виртуалната памет за всички виртуални сървъри е 6 173 21,03, а на облачните сървъри е 892,78.
- Общият брой физически процесорни ядра на хостовете за виртуализация е 26 165. Общото процесорно натоварване на всички виртуални сървъри (GHz) е 39 346,88, а на всички облачни сървъри (GHz) е 15 337,5.

Общият капацитет за съхранение на данни, предоставен за виртуални машини в TB е 10 096,96. Общият капацитет за съхранение на данни в облачното пространство е 15 892,4.

Общият обем на локалните дискове във всички сървъри (TB) е 36 901,27 (33%), от които:

- Броят на споделените дискови масиви (FC/iSCSI) е 904,4 (1%).
- Общият брой механични твърди дискове във всички споделени дискови масиви е 29 460,4 (26%).
- Общият брой SSD дискове във всички споделени дискови масиви е 13 898 (12%).
- Общият капацитет за съхранение на данни на споделените дискови масиви (TB след RAID) е 30 820,93 (28%).

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

Вид актив	*Брой*		*Стойност, лв.*	
	2022	*2023*	*2022*	*2023*
Запаметяващи устройства	*1 103*	*509*	*7 100 876*	*1 933 549*
Поддържащи системи	*7 671*	*1 906*	*17 802 628*	*8 071 737*
Мрежово оборудване	*12 624*	*6 927*	*44 746 194*	*38 165 350*
Периферни устройства	*105 372*	*52 649*	*83 531 182*	*135 312 164*
Физически сървър	*3 265*	*1 480*	*54 625 465*	*57 099 931*
Сървърен/комуникационен шкаф	*1 682*	*560*	*9 016 141*	*8 109 574*
Система за съхранение	*373*	*191*	*21 043 949*	*14 860 429*
Виртуална машина	*668*	*486*	*467 657*	*528 994*

Източник: Министерство на електронното управление, РИР
Таблица 1: Въведени активи в РИР

Предоставената информация показва значителни промени в броя на активите в РИР през разглеждания период. Наблюдава се намаление в обема на хардуерните активи, което може да се дължи на няколко фактора, включително надграждане или подмяна на остаряло оборудване, консолидация на ресурси и преминаване към нови технологии.

Един от най-значимите спадове със 75% между 2022 г. и 2023 г. е в категорията „Поддържащи системи“. Подобно намаление се наблюдава и при сървърните/комуникационни шкафове - с 67%. Значително е намалението и в броя на запаметяващите устройства с 54%, което е в следствие на прилагането на ефективни методи за съхранение. По подобен начин броят на физическите сървъри намалява с 54%.

Въпреки тези спадове, продължава тенденцията при работните станции, сървърите и мрежовото оборудване да се наблюдава голямо разнообразие от производители. Тази ситуация създава рискове, свързани с увеличените разходи за поддръжка и намалената ефективност. С допълването на ЕПИР със съответните правила, стандарти и процедури за развитие и управление на ИР по отношение на вида и типа хардуер, който трябва да се използва за изпълнение на еднакви функции и дейности в различните администрации, този риск може да бъде преодолян.

2. Обезпеченост на администрациите със софтуер и лицензи

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

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.

По данни в ИИСДА 8,61% от операционните системи на работни станции са с остарели версии, които вече не се поддържат от основния доставчик, като се наблюдава понижение на тази стойност в сравнение с миналия отчетен период над 50%. Въпреки предприетите мерки от администрациите, ползването на версии на софтуер извън поддръжка, представлява сериозен риск за информационната сигурност.

По отношение на антивирусните решения, на база информация в ИИСДА, най-използвани от администрациите са антивирусните решения на ESET, както и друг безплатен софтуер.

	ESET Antivirus	*Panda Antivirus*	*F-Secure Business*	*Kaspersky Antivirus*	*Symantec Antivirus*	*Друг безплатен антивирусен софтуер*
2022, %	*30,42%*	*6,66%*	*8,56%*	*4,60%*	*3,80%*	*13%*
2022	*192*	*42*	*54*	*29*	*24*	*82*
2023, %	*35,7%*	*6,09%*	*5,41%*	*3,72%*	*3,21%*	*45,85%*
2023	*211*	*36*	*32*	*22*	*19*	*247*

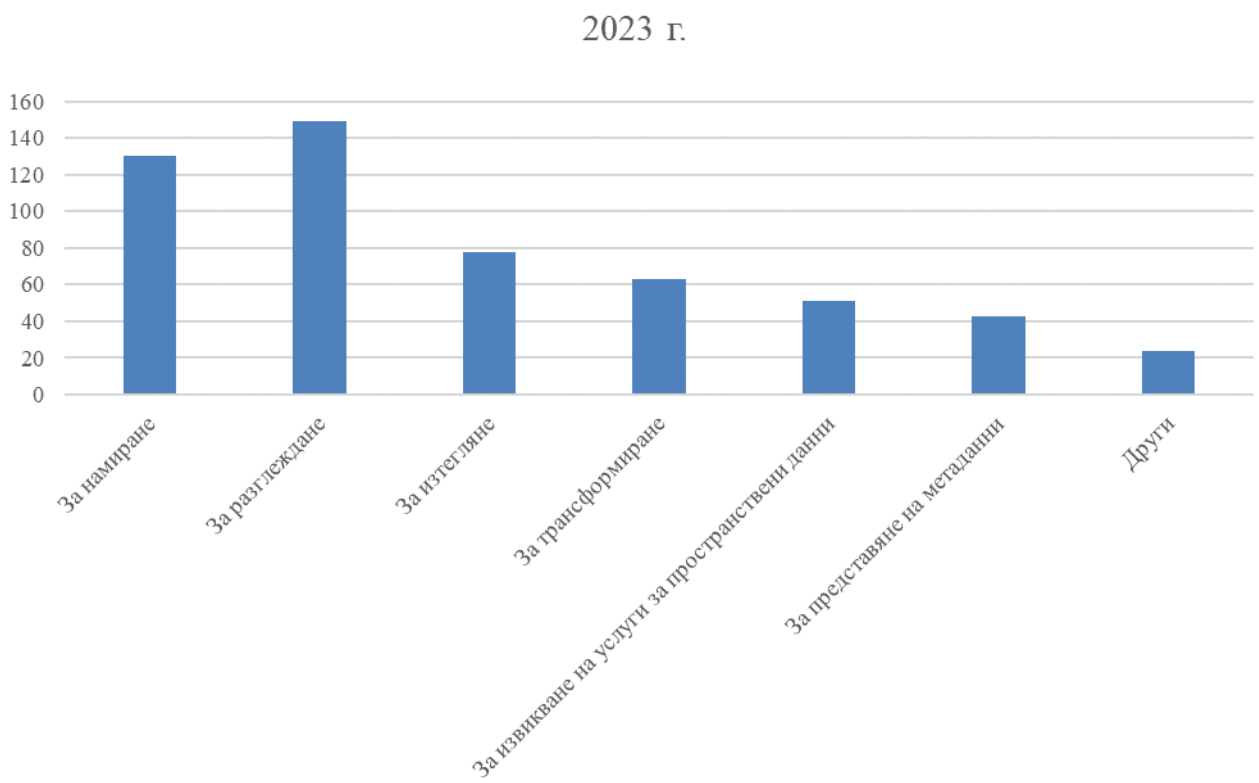
Източник: Администрация на Министерския съвет, ИИСДА

Таблица 2: Разпределение на антивирусния софтуер

През отчетната 2023 г. по данни от ИИСДА в администрацията са инсталирани 48 940 броя софтуерни програми за киберзащита на софтуерни продукти.

Сървър приложение за географска информационна система (ГИС) се използва от 68 администрации, ползващи десктоп приложение са 100 и уеб приложение – 72.

Администрациите, които обменят информация между ГИС системата и други информационни системи са 56, а 120 са посочили, че не обменят.



Източник: Администрация на Министерския съвет, ИИСДА
Фигура 2: Видовете ГИС услуги предоставяни в администрациите през 2023 г.

От графиката по-горе е видно, че администрациите използват ГИС услуги предимно за намиране и разглеждане.

По данни от ИИСДА, 130 администрации са хармонизирали услугите, предоставяни от тяхната ГИС, съгласно изискванията на Закона за достъп до пространствени данни (ЗДПД) и регламентите към Директива 2007/2/ЕО INSPIRE0, а 73 са посочили отговор „не“.

3. Информационни системи

От гледна точка на ресурсите на е-управление информационните системи са системите на е-управление (хоризонтални и централизирани) и системите на администрациите.

3.1. Хоризонтални системи на електронното управление

3.1.1. Портал на електронното управление (egov.bg)

Порталът на електронното управление (ПЕУ) е реализиран като единна точка за достъп до електронни административни услуги (ЕАУ). Към края на 2023 г. на ПЕУ е публикувана информация за 1 846 електронни услуги, от тях 1 215 ЕАУ са реализирани чрез централизирано и унифицирано заявяване. За заявяването им са разработени над 1 800

електронни форми.

За 2023 година новите ЕАУ за централизирано заявяване, публикувани на ПЕУ са 83. Публикувана е и информация за 631 ЕАУ, предоставяни децентрализирано чрез разработени портали на администрациите – Министерство на правосъдието, Министерство на вътрешните работи, Агенция по геодезия, картография и кадастър, Агенция „Митници“, Национален осигурителен институт, Национален център за информация и документация и др.



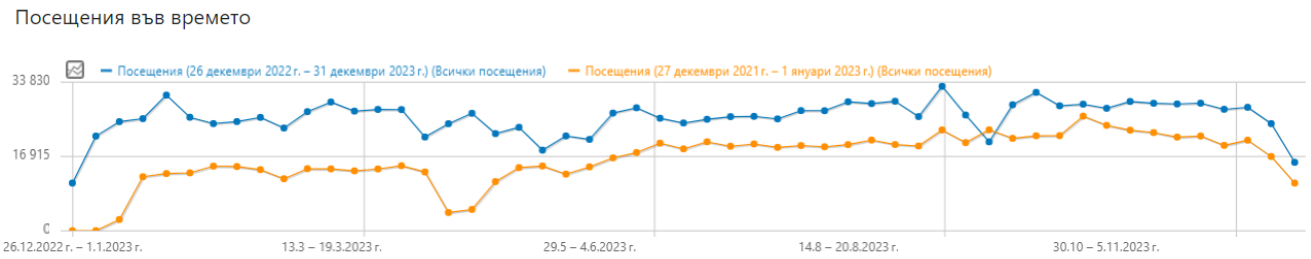
Източник: Министерство на електронното управление
Фигура 3: Брой разработени услуги по години

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.

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 се предоставят 21 услуги от областните администрации и 197 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 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. Регистрираните потребители към края на 2023 г. в „Моето пространство“ са над 75 000, като за отчетния период броят им е нараснал с над 45%.

Интересът от страна на гражданите и бизнеса непрекъснато нараства, което е видно от представената графика. Приблизително два пъти са нараснали посещенията от потребители.



Източник: Министерство на електронното управление,https://analytics.egov.bg/
Фигура 4: Справка за посещения на портала за 2023 г.

С цел намаляване на разходите на администрациите при прилагането на политиките за е-управление, е създадената 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 Портала на електронното управление.

Данните от ИИСДА показват, че от 587 администрации 160 имат изграден уебстайт в инфраструктурата на ПЕУ.

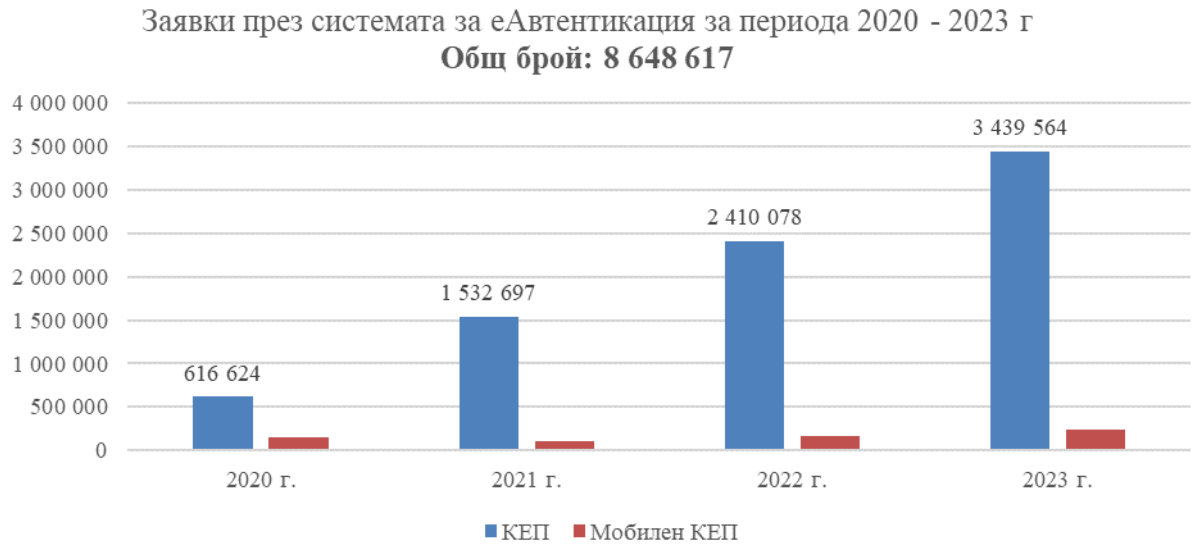
3.1.2. Система за е-Автентикация

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. Нормативно установените средства за идентификация са Квалифициран електронен подпис (КЕП), мобилен КЕП, Персонален идентификационен код (ПИК) на НАП и ПИК на НОИ.

Интеграцията със системата позволява на потребителите да се автентикират с всяко средство за идентификация, предоставяно от интегрираните с еАвт 2.0 доставчици на идентификация. Възможно е и обратното, при интеграция на доставчик на идентификация чрез предоставяното от него средство, да се автентикират потребители пред всички интегрирани с еАвт 2.0 системи.

Общият брой успешни автентикации е 8 648 617, като само за 2023 г. успешните автентикации са 3 671 637, от които 3 439 564 са с физически КЕП, а 232 073 са с мобилен КЕП.

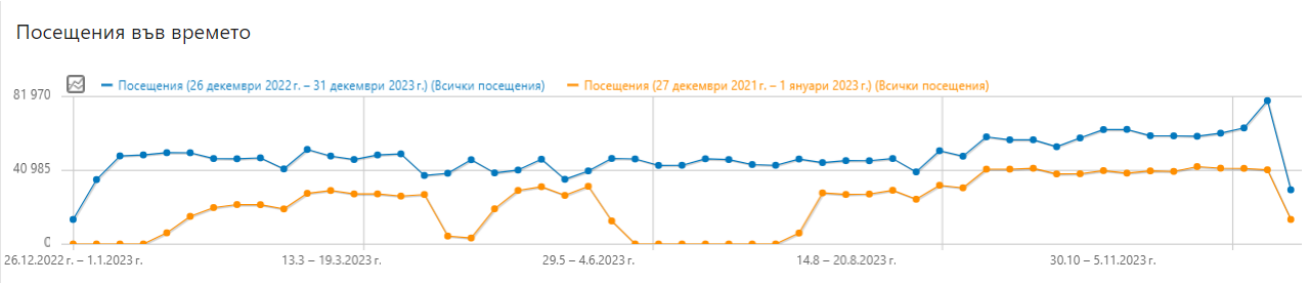
В сравнение с предходния отчетен период увеличението е 43%, когато автентикациите чрез физически КЕП са били 2 410 078 бр., а с мобилен – 162 645 бр.



Източник: Министерство на електронното управление
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.

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



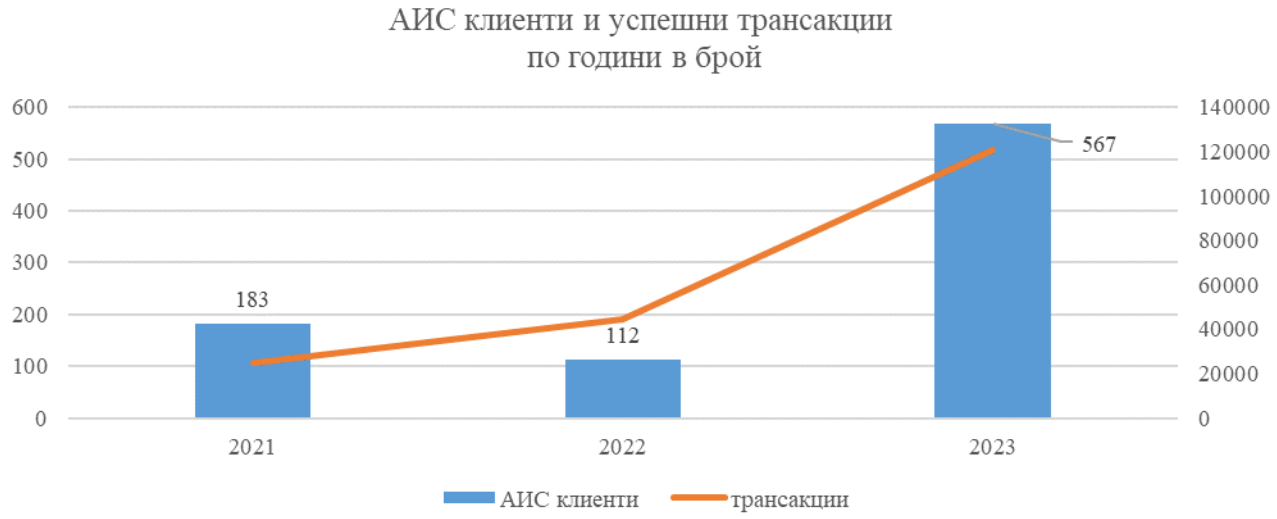
Източник: Министерство на електронното управление,https://analytics.egov.bg/
Фигура 6: Справка за посещения на системата за електронна автентикация за 2023 г.

3.1.3. Система за електронно плащане (е-Плащане)

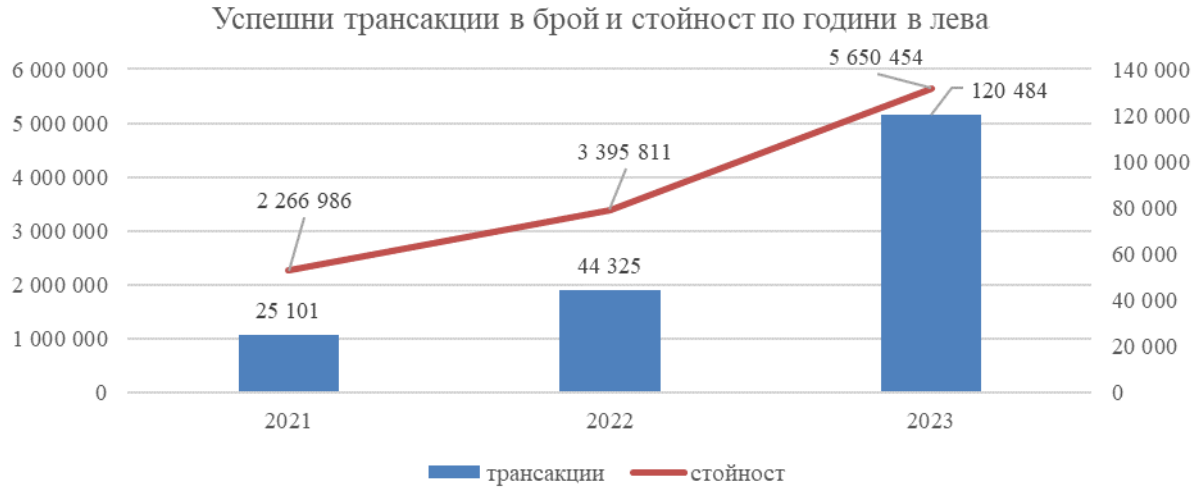
Системата предоставя възможност на задължените лица да заплатят своите задължения към администрациите чрез платежна карта през Централен виртуален ПОС терминал, чрез системата за електронни плащания ePay, както и с код за достъп, предоставен от администрацията, предоставяща услугата. Чрез системата могат да се заплатят услуги към присъединените централни, специализирани териториални и всички областни и общински администрации, както и техните райони. Система за електронно плащане предоставя удобството на гражданите и бизнеса да извършват плащания без да заплащат допълнителни такси или комисиони и допълнително улеснява извършването на трансакции от всяка точка на света, посредством платежна карта.

Съгласно данни от системата е-Плащане през 2023 г. са присъединени 567 бр. АИС клиенти от 127 администрации. Нарастването спрямо предходната година е четири пъти.

Извършените трансакции и общата им стойност по години са показани на фигура 7 и фигура 8.



Източник: Министерство на електронното управление
Фигура 7: АИС клиенти и преминали трансакции в системата за еПлащане

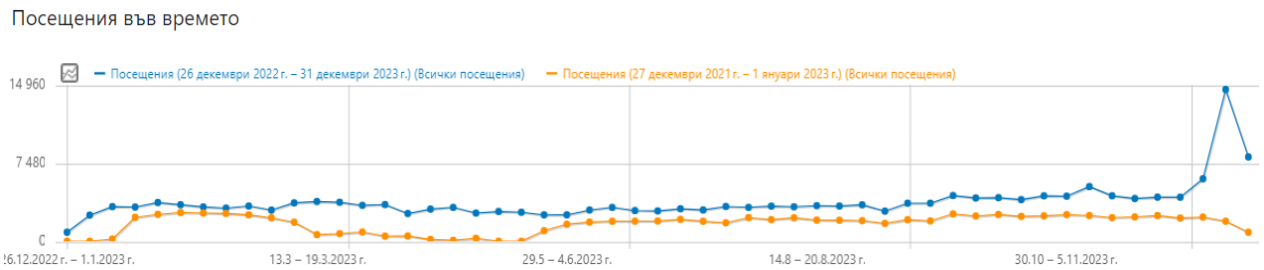


Източник: Министерство на електронното управление
Фигура 8: Успешни трансакции в системата за еПлащане – стойност в лв.

През 2023 г. са реализирани следните функционалности:

- Изпращане на уведомления за регистрирани нарушения - съгласно промените в чл. 189 ал. 4а от Закона за движение по пътищата, бе предоставен канал за уведомяване за регистрирани нарушения.
- Проверка за задължения за регистрирани нарушения на фиш, електронен фиш или наказателно постановление и заплащането им по електронен път чрез Централен Виртуален ПОС терминал;
- Извличане на справка за дължими местни данъци и такси и други публичноправни задължения и плащането им по електронен път чрез Централен Виртуален ПОС терминал, като за трансакцията не се дължат такси и комисионни.

Потреблението на системата за електронно плащане непрекъснато нараства, което е видно от фигура 9.



Източник: Министерство на електронното управление,https://analytics.egov.bg/
Фигура 9: Справка за посещения на системата за електронно плащане за 2023 г.

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

Системата е средство в реално време за проверка и потвърждаване на валидността на квалифициран електронен подпис, удостоверение за време (time stamp), електронно подписан документ.

Към системата са добавени над 700 удостоверителни (Root) сертификата от доверителния списък[1], администриран от Европейската комисия относно валидиране на електронен подпис.

Системата е интегрирана със Системата за сигурно електронно връчване (ССЕВ), като за отчетния период е проверена валидността на 7 054 361 персонални цифрови сертификата. Повишението на ползваемостта на системата в сравнение с 2022 г. е близо 57%, когато броят на проверените цифрови сертификати е бил 4 125 461.

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, както и подаване ѝ към административния орган, доставчик на услугата.

През прототипа на системата за електронни форми се предоставят за централизирано заявяване 1 215 ЕАУ. Борят заявявания на ЕАУ за отчетния период са общо 91 591, отчита се нарастване с 34% на заявените услуги през 2023 г. спрямо 2022 г. Формите са разработени по стандарт с цел унифициране на формуляри. Най-често заявяваните услуги през 2023 г. са към Агенцията за социално подпомагане, Агенцията по заетостта и общинските администрации.

От създаването на прототипа на системата статистика на заявените ЕАУ по години е представена на фиг. 10.

[1] https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home



Източник: Министерство на електронното управление
Фигура 10: Брой заявявания на ЕАУ по години

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 края на 2023 г. са 285 515, от които 260 715 на физически лица, 11 887 на административни органи, техни структури и лица, предоставящи обществени и публични функции и 12 913 юридически лица. За 2023 г. в системата са регистрирани 3 514 организации, от които 2 735 са юридически лица, а 779 са лица по чл. 1 от ЗЕУ.

Справка за броя на регистрирани потребители в ССЕВ по години е представена на фигура 11.



Източник: Министерство на електронното управление
Фигура 11: Брой регистрираните потребители в ССЕВ по години

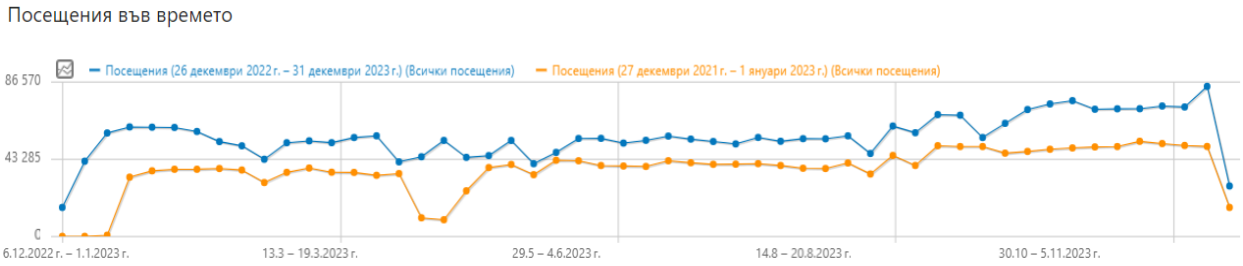
Обменените съобщения чрез ССЕВ към края на отчетния период са общо 5 449 408, като за 2023 г. броят на изпратените съобщения е 2 553 545, което е с над 55% увеличение в сравнение с 2022 г.

Справка за обменените съобщения по години е представена на фигура 12.



Източник: Министерство на електронното управление
Фигура 12: Справка за обменените съобщения по години

Потреблението на ССЕВ, осигуряваща обмена на съобщения между граждани, бизнес и административни органи непрекъснато нараства, което е видно от на фигура 13.



Източник: Министерство на електронното управление,https://analytics.egov.bg/
Фигура 13: Справка за посещения на системата за сигурно електронно връчване за 2023 г.

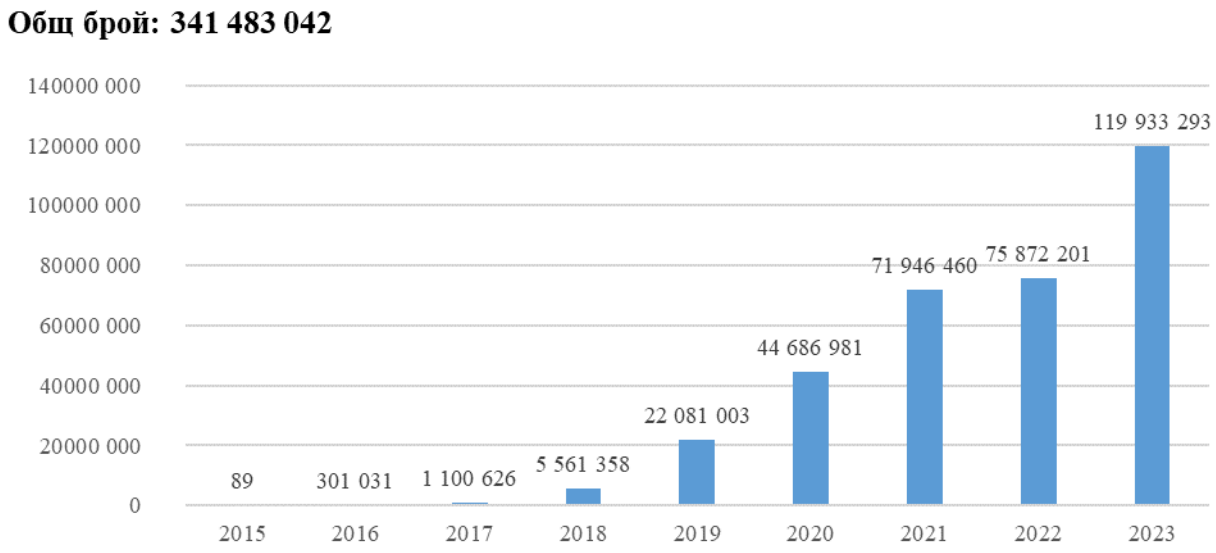
3.2. Централизирани системи за е-управление

Централизираните системи са предназначени да подпомагат администрациите при взаимодействието им с гражданите и бизнеса. В голямата си част те позволяват с една инсталация на системата да работят множество администрации (multi-tenant решения). На този етап функционира информационната система за обмен на справочна и удостоверителна информация (RegiX).

През 2023 г. продължават усилията за разширяване на възможностите за служебен обмен на данни като вътрешни електронни административни услуги (ВЕАУ) между административните органи чрез RegiX. Общият брой консуматори на справки е 1 119. Към системата са свързани 84 основни регистъра, администрирани от 30 централни администрации и са реализирани 232 справки към регистрите.

Към края на 2023 г. общият брой направени заявки към регистри е 341 483 042, като за

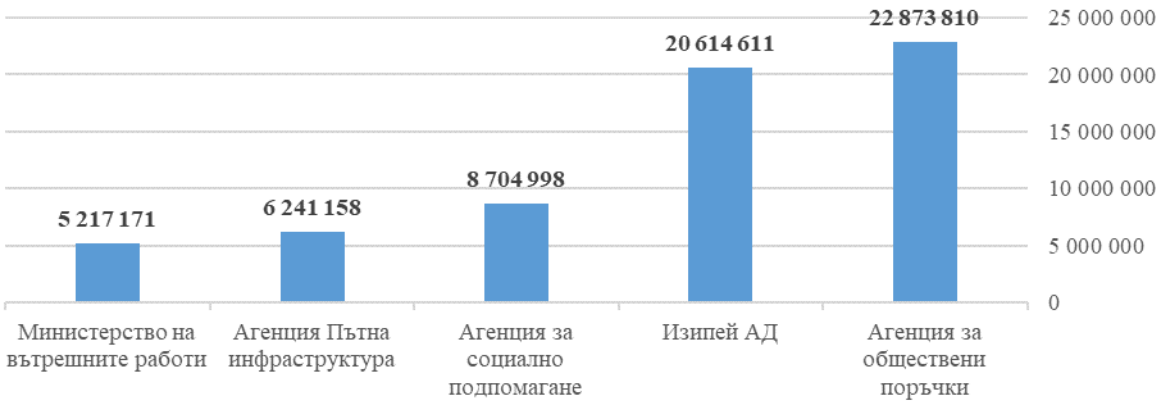
отчетния период са извършени 119 933 293 справки. По данни от логовете на системата за 2023 г. най-големият консуматор е Агенцията по обществени поръчки, която е заявила 22 873 810 справки. Министерството на вътрешните работи е първичен администратор на данни, предоставил най-много справки – 42 136 836, като само от Регистър „Български документи за самоличност“ са 38 234 072.



Източник: Министерство на електронното управление
Фигура 14: Брой предоставени вътрешни електронни административни услуги за периода 2017 - 2023 г.



Източник: Министерство на електронното управление
Фигура 15: Топ 5 „Консуматор“ на вътрешни електронно административни услуги през 2023 г.



Източник: Министерство на електронното управление
Фигура 16: Топ 5 посещавани администрации през 2023 г.

На електронен адрес: https://info-regix.egov.bg/main са публикувани данните за присъединените регистри и операциите за достъп до тях, както и статистическа и справочна информация за използването на системата.

Към информационната система за обмен на справочна и удостоверителна информация са присъединени всички общински администрации. Засиленото използване на RegiX се дължи както на популяризирането ѝ сред консуматорите, така и на законовите изисквания, задължаващи административните органи и лицата по чл. 1 от ЗЕУ да предоставят ВЕАУ с цел намаляване на административната тежест за гражданите и бизнеса.

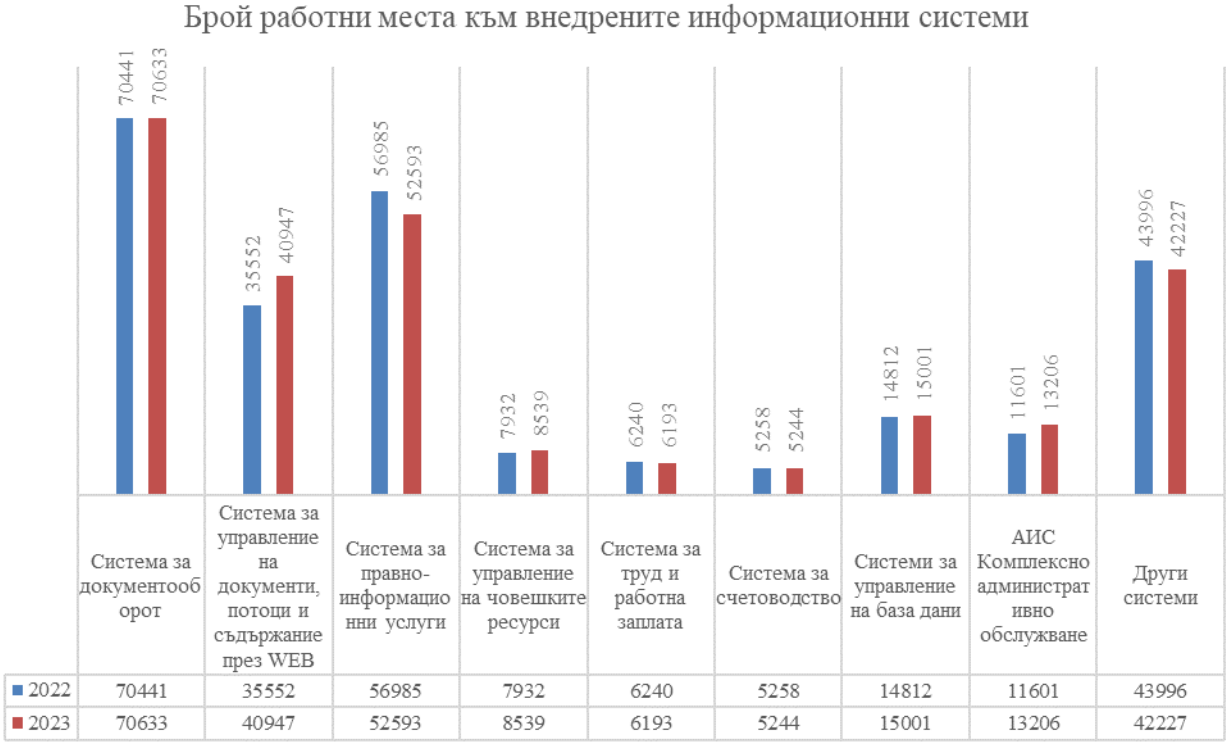
3.3. Информационни системи в администрациите

Информационните системи в държавната администрация се явяват важна предпоставка за автоматизиране на вътрешно-административните процеси и за изпълнение на оперативните дейности. Данните показват леко покачване във всички категории на броя на администрациите, които нямат внедрени информационни системи, като най-значително е нарастването при системите за управление на база данни (близо 2%).

Администрации, които НЯМАТ внедрени информационни системи	*2022 г. %*	*2023 г. %*
Административни информационни системи/ Система за документооборот	*3.10*	*3.9*
Система за управление на човешките ресурси	*22.4*	*23.2*
Система за труд и работна заплата	*1.20*	*2.4*
Система за счетоводство	*0.00*	*1.5*
Система за управление на база данни	*41.90*	*44.8*
Системи за управление на документи, потоци и съдържание през WEB	*43.20*	*44.8*
АИС за комплексно административно обслужване	*66.70*	*67.5*
Система за правно-информационни услуги	*15.80*	*17.0*

Източник: Администрация на Министерския съвет, ИИСДА
Таблица 3: Администрации, които нямат внедрени информационни системи.

Внедрените информационни системи, които се използват в администрацията са общо 5 283. В сравнение с предишната отчетна година 2022 г., където общия брой на работните места към внедрените информационни системи в администрацията е 252 817 бр., през 2023 г. се наблюдава ръст с 0,69% на работните места, които са 254 583 броя.



	Система за документооборот	Система за управление на документи, потоци и съдържание през WEB	Система за правно-информационни услуги	Система за управление на човешките ресурси	Система за труд и работна заплата	Система за счетоводство	Системи за управление на база дани	АИС Комплексно административно обслужване	Други системи
2022	70441	35552	56985	7932	6240	5258	14812	11601	43996
2023	70633	40947	52593	8539	6193	5244	15001	13206	42227

Източник: Администрация на Министерския съвет, ИИСДА
Фигура 17: Внедрени информационни системи и брой работни места

4. Електронна идентификация

4.1. Електронна идентификация за нуждите на заявяване на ЕАУ

Действащата нормативна уредба в Република България предвижда, че лицата по чл. 1 от ЗЕУ са длъжни да осигурят възможност на гражданите и организациите при заявяването на ЕАУ да се идентифицират:

4.1.1. По реда на Закона за електронната идентификация (ЗЕИ).

Националната държавна схема за електронна идентификация, предвидена в ЗЕИ все още не е изградена, което в определена степен ограничава достъпа на гражданите и бизнеса до ЕАУ, в т.ч. и трансгранични такива. Липсата на схема по ЗЕИ се явява стимул за частния сектор за разработването на различни решения за електронната идентификация.- със средства за електронна идентификация в рамките на уведомени схеми за електронна идентификация по реда на чл. 9 от Регламент (ЕС) № 910/ 2014 на Европейския Парламент и на Съвета от 23 юли 2024 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО, наричан по-нататък Регламент (ЕС) № 910/ 2014.

Създадени са подходящи условия за трансгранично признаване на средствата за електронна идентификация, издадени в различни държави – членки на Европейския съюз (ЕС) – чрез национален eIDAS възел.

С проекта за развитие на националния eIDAS възел, интеграцията му с eIDAS възлите на другите държави - членки на ЕС, както и осигуряването на достъп до ЕАУ, се изпълняват задълженията на Република България по Регламент (ЕС) № 910/2014 г. във връзка с

трансграничната електронна идентификация. Проектът включва актуализиране на текущата версия на възела спрямо последната актуална техническа спецификация, предоставена от ЕК. Възелът представлява точка на свързване, която е част от архитектурата за оперативна съвместимост на електронната идентификация и участва в трансграничното удостоверяване на автентичността на лица, като е в състояние да разпознава и обработва или препраща предавания на данни към други възли, с което дава възможност на националната инфраструктура за електронна идентификация на една държава членка да се свързва с националната инфраструктура за електронна идентификация на други държави членки.

През отчетния период успешно са преминали тестовете за свързаност с 16 държави – членки на ЕС (Австрия, Белгия, Германия, Дания, Италия, Естония, Лихтенщайн, Люксембург, Малта, Португалия, Словакия, Словения, Франция, Хърватска, Чешка република, Испания); с 8 държави е осъществена свързаност и в продукционна среда (Белгия, Италия, Лихтенщайн, Люксембург, Малта, Словакия, Словения, Чешка република).

Чрез eIDAS възела е осигурена технологична възможност за взаимно признаване на средствата, но процесът се затруднява, тъй като на национално равнище и през 2023 г. продължава тенденцията за критично нисък брой ЕАУ, които да могат да се заявяват трансгранично.

4.1.2. Със средства за електронна идентификация с ниво на осигуреност „високо“, издадено в рамките на удостоверителна услуга за електронна идентификация с национално покритие, вписана в Доверителния списък, воден от Комисията за регулиране на съобщенията по чл. 22 от Регламент (ЕС) № 910/ 2014.

В МЕУ е създаден механизъм, чрез който при поискване от страна на доставчиците на услуги за електронна идентификация и след проверка, че същите отговарят на изискванията на чл. 7-9 от Регламент (ЕС) № 910/2014, разработените от тях решения за електронна идентификация могат да бъдат признати с Решение на Министерския съвет за национални схеми за електронна идентификация.

В рамките на посочения механизъм с Решение на Министерския съвет от 29 май 2023 г. е призната първата българска национална схема за електронна идентификация с нива на осигуреност „значително“ и „високо“. Схемата е публикувана в Официалния вестник на ЕС на 05 юли 2023 г., след нотифицирането ѝ пред Европейската комисия (ЕК) от МЕУ. Чрез нея се осигурява възможност на гражданите и организациите за достъп до онлайн услуги, предоставяни от органи от публичния сектор в други държави – членки на ЕС със средство за електронна идентификация, издадено в Република България.

През отчетния период е в ход процедура по извършване на проверка за съответствие с изискванията на чл. 7-9 от Регламент (ЕС) № 910/2014 на втора българска схема за електронна идентификация, разралотена от доставчик на услуги за електронна иидентификация. В проверката участва междуведомствен екип, назначен със заповед на министъра на електронното управление. Проверката предшества процеса по нотификация на схемата пред ЕК.

4.1.3. С други средства за електронна идентификация, определени с Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги (НОИИСРЕАУ) - квалифициран електронен подпис (КЕП), включително облачен/ мобилен КЕП, персонални идентификационни кодове, издавани от Националния осигурителен институт и от Националната агенция за приходите, както и уникален код за достъп, издаван от Националната здравноосигурителна каса.

Посочените средства са временно решение, обусловено от липсата на национална схема за електронна идентификация по ЗЕИ. Тяхното използване е регламентирано в параграф 5 от Преходните и заключителни разпоредби на НОИИСРЕАУ.

Общинската администрация предоставя ЕАУ основно чрез Портала на електронното управление и потребителите на тези услуги се идентифицират чрез средствата, които изисква портала. Това са КЕП, включително облачен/мобилен КЕП и ПИК на НАП/НОИ. Средства, които не са правно регламентирани, но все още спорадично се използват са КИН (клиентски идентификационен номер) и ПИН (персонален идентификационен номер). Гражданите се идентифицират чрез тях предимно пред общинската администрация.

В изпълнение на заложените законодателни мерки в Програмата за управление на Република България за периода юни 2023 – декември 2024 г. (ЗМ-20.1.3) е изготвен проект на Закон за изменение и допълнение на Закона за електронната идентификация (ЗИД на ЗЕИ). Чрез него се регулира признаването на схеми за електронна идентификация, разработени и администрирани от частноправни субекти. Законопроектът ясно дефинира субектите, които могат да изграждат схеми за електронна идентификация и условията, на които тези схеми трябва да отговарят, за да бъдат използвани за достъп до електронни услуги, предоставяни от органите от публичния сектор. Разписано е административното производство, в рамките на което се признават горепосочените схеми; органът, които извършва признаването и който осъществява надзора над схемите. Предвидена е и възможността за схемите да бъде извършено уведомяване пред ЕК съгласно чл. 9 от Регламент (ЕС) № 910/2014, което има за цел да осигури възможност за заявяване на електронни административни услуги на територията на ЕС със средствата, издадени в рамките на тези схеми.

И през 2023 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.

Съгласно данните, публикувани в ИИСДА за 2023 г. средствата за електронна идентификация, които администрациите поддържат за подаване на документи по електронен път и заявяване на ЕАУ от гражданите и бизнеса са, както следва: КЕП – 95 %; ПИК/ПИН – 29 %; потребителско име и парола – 20 %. Около 5 % са посочили друго средство. През отчетния период 586 администрации са заявили, че приемат, обработват и изпращат електронно подписани документи.

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.

5. Регистри, поддържани от администрацията.

По данни от ИИСДА регистри – електронни или на хартия, свързани с предоставяне на електронни услуги за граждани и бизнеса, поддържат 185 от администрациите.

Регистрите, свързани с предоставянето на ЕАУ за гражданите и бизнеса са:

	Брой регистри	*В т.ч. първични регистри*
Регистри, които се поддържат на хартиен носител и подлежат на електронизация	*200*	*182*
Регистри, за които закон предвижда да се водят на ръка (не подлежат на електронизация)	*141*	*116*
Регистри, които се поддържат в електронен вид	*2 309*	*1 725*
Регистри, които се поддържат в електронен вид и са част от информационна система	*674*	*615*

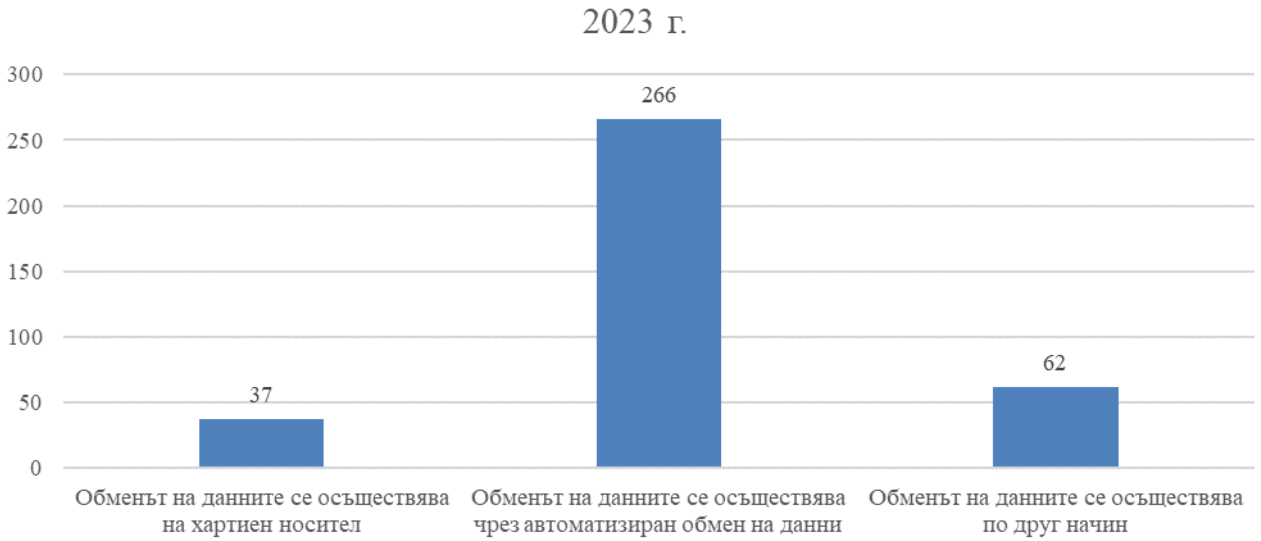
Източник: Администрация на Министерския съвет, ИИСДАю
Таблица 4: Регистри, свързани с предоставянето на ЕАУ за гражданите и бизнеса

Регистрите, които се поддържат в електронен вид са:

	Брой регистри
Първични регистри, които предоставят данни на други административни органи, лица, осъществяващи публични функции или организации, предоставящи обществени услуги, които въз основа на закон също обработват тези данни	*1 028*
Регистри, които предоставят програмни интерфейси за достъп до данните	*526*
Регистри, които поддържат интерфейси за отворени данни, по реда на ЗДОИ	*851*

Източник: Администрация на Министерския съвет, ИИСДА
Таблица 5: Регистри, които се поддържат в електронен вид

От регистрите, за които през 2023 г. е отбелязано, че имат обмен и интеграция на данни с други регистри разпределението е следното:



Източник: Администрация на Министерския съвет, ИИСДА
Фигура 18: Регистри с обмен и интеграция на данни

6. Споделени информационни ресурси

Споделени информационни ресурси на електронното управление са техническата инфраструктура, единната електронна съобщителна мрежа, информационните центрове, защитеното споделено информационно пространство 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 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:

ОСНОВНИ СИСТЕМИ В ЦЕНТРОВЕТЕ ЗА ДАННИ
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

Източник: Министерство на електронното управление
Таблица 6: Инсталирани основни систем в центровете за данни

Информационните компоненти на инфраструктурата на споделените ресурси на е-управлението са разположени в Основния център за данни в СОСП „Ботевград 2“, в

Контролно-техническия център за данни Бояна, в резервния център за данни, за който предстои издаване на акт 16 и Центъра 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 са предоставени следните облачни услуги:

- „Инфраструктура като услуга“ – 44 организации;

- Web електронна поща – 95 организации и дадени около 3 200 пощенски кутии;

- Услуга „Back up“ – 38 организации.

На над 100 министерства и ведомства са предоставени 1 329 броя виртуални машини и 1 420 ТБ дисково пространство.

Има 1 349 потребителя (министерства, агенции и общини) на Системата за електронен обмен на съобщения (СЕОС).

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

През 2023 г. броят на държавните организиции, ползващи ресурсите на ДХЧО са е увеличил с 37%. В таблицата са показани държавните организации, ползващи ресурси в ДХЧО към края на 2023 г.

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
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
Столична община
Община Мизия
Национален осигурителен институт
Държавна комисия по сигурност на информацията
Министерство на финансите
Висш съдебен съвет
Министерство на външните работи
Държавна агенция за закрила на детето
Българска агенция по безопасност на храните
Министерство на младежта и спорта
Информационен Център на Министерство на Отбраната
Главна дирекция „Гражданска въздухоплавателна администрация“
Комисия за защита на потребителите
Министерство на правосъдието
Национален център за информация и документация
Министерство на отбраната
Държавна комисия по сигурността на информацията
Министерство на културата
Агенция по геодезия, картография и кадастър

Източник: Изпълнителна агенция „Инфраструктура на електронното управление“
Таблица 7: Списък на държавните организации, ползващи ресурси в ДХЧО към 2023 г.

През отчетната година е осигурена разширена извънгаранционна поддръжка на техническите средства в ДХЧО 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 2023 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.

Същевременно е осигурена работоспособността на ЕЕСМ и в допълнение са реализирани услуги и дейности към администрацията:

- Изградени са 28 нови възли за достъп и са преконфигурирани други такива, по заявки на ползвателите на ЕЕСМ.
- Изградена е нова оптична свързаност към ГКПП Кардам, СОССП Плевен 2, Община Долна Митрополия, ВВВУ Долна Митрополия, БУЛРИС Русе, Българска

национална филмотека, РЗПАБ Разград, КПКОНПИ Видин, Военно разузнаване Варна, ГД „Мерки и измервателни уреди“ Велико Търново.

- Изградени 38 бр. L2/L3 нови услуги по заявки през ЕЕСМ.
- Увеличен е преносният капацитет на 172 бр. възли за достъп.
- Общ брой администрации, използващи Интернет зад Защитения Интернет възел – 131 бр., като за 2023 г. са присъединени 8 администрации.

През 2023 г. се изпълнява проект „Широкомащабно разгръщане на цифрова инфраструктура на територията на България“ по Националния план за възстановяване и устойчивост. Разработва се документация за изготвяне на Технически спецификации по отношение на кабелната инфраструктура. Проведени са срещи с Министерството на транспорта и съобщенията и с кабелните оператори (Виваком, А1 ЕАД и Цетин) за определяне на кабелните магистрали, необходими за привързване на 140 общини.

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.

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

7. Предоставяне на електронни административни услуги

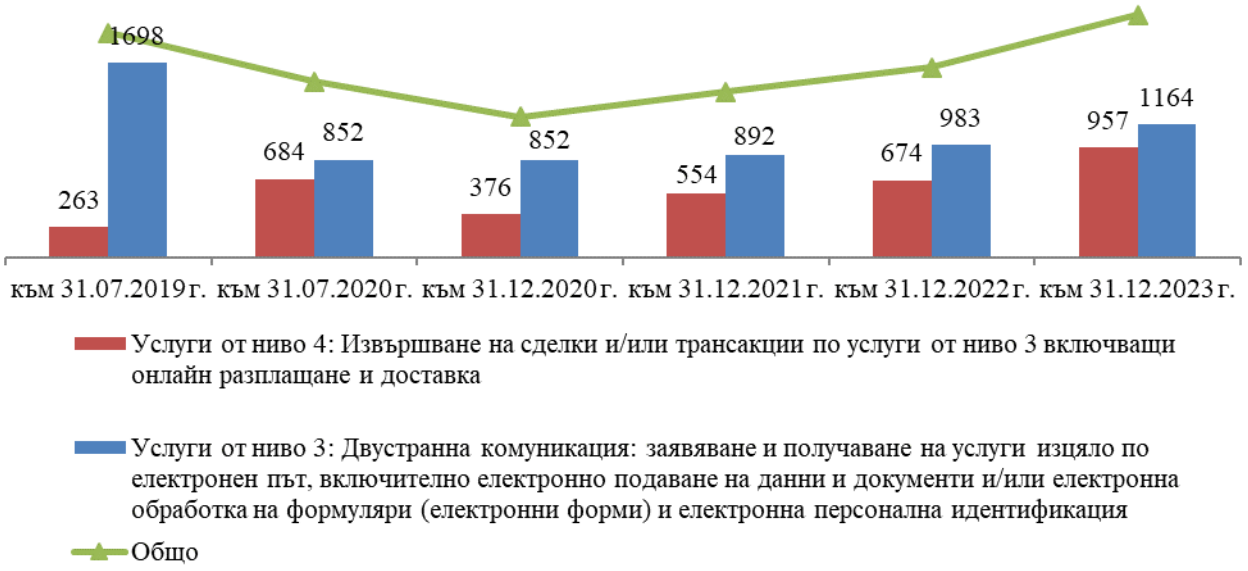
В изпълнение на Регламент (ЕС) 2018/1724[2] на Европейския парламент и на Съвета от 2 октомври 2018 г. (Single Digital Gateway) през 2023 г. България взе участие на европейско ниво в координационните срещи и събития по създаването и функционирането на единна цифрова платформа. Платформата освен информация и услуги за оказване на помощ ще позволява национален и трансграничен обмен на доказателства по процедури, като посредническа платформа.

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.

7.1 Състояние на електронните административни услуги

Общият брой услуги[3], вписани в АР към 31.12.2023 г., е 2 605, от които 2 121 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. Невъзможността да бъдат агрегирани данните по еднотипни услуги води до разминаване в броя на услугите по нива и до затруднения в интерпретацията на информацията що се касае до ЕАУ, предоставяни от повече от една администрация.

[2] https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32018R1724
[3] *https://iisda.government.bg/adm_services/services*



Източник: Администрация на Министерския съвет, ИИСДА
Фигура 19: Брой услуги от ниво 3 или ниво 4 по години

Запазва се тенденцията да нараства делът на административните услуги, предоставяни на нива 3 и 4 спрямо общия брой предлагани 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 и ниво 4. 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.

7.2 Осигуряване на институционална идентичност и достъпност на уебсайтовете

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

През 2023 г. са утвърдени актуализирани Правила за институционална идентичност на интернет страниците и портали на държавната администрация[4], които отразяват Препоръките за подобряване на обявяваната на интернет страниците на администрациите информация за контакти по телефона, на базата на Аналитичен доклад „Изследване и препоръки за информацията за контакти по телефона на интернет страниците на администрациите“, изготвен от Института по публична администрация.

В изпълнение на функциите по наблюдение и прилагане на изискванията на Директива (ЕС) 2016/2102 относно достъпността на уебсайтовете и мобилните приложения

[4] *Утвърдени със Заповед МЕУ-10828/ 12.07.2023 г. на министъра на електронното управление. Актуализацията на Правилата се осъществява по реда на определянето им в съответствие с чл. 40, ал. 1 на НОИИСРЕАУ.*

на организациите от обществения сектор, МЕУ извършва регулярни проверки за достъпност на уебсайтове (интернет страници) и мобилни приложения на лицата по чл. 1 от ЗЕУ, съгласно чл. 60а от ЗЕУ. Контролът се осъществява в съответствие с Методология за наблюдение и проверки на достъпността на съдържанието на интернет страниците и мобилните приложения[5] на лицата по чл. 1 от ЗЕУ, съобразена с Решение за изпълнение (ЕС) 2018/1524 от 11 октомври 2018 г. и на основата на хармонизирания стандарт EN 301 549 Изисквания за достъпност на ИКТ продукти и услуги, разработен в подкрепа на Директивата.

В рамките на 2023 г. са извършени проверки на 273 уебсайта (от тях 126 – на държавни администрации) и 13 мобилни приложения (от тях 7 – на държавни администрации), а резултатите от проверките, с включени разяснения по установените несъответствия и срок за отстраняването им, са предоставени на организациите. Информацията, получавана в МЕУ, показва, че се предприемат необходимите действия за отстраняване на несъответствията и за поддържане на достъпно съдържание чрез прилагане на хармонизирания стандарт. Някои от организациите планираха и създадоха изцяло нови уебсайтове, съобразени с изискванията за достъпност, вкл. изграждане на федериран портал в инфраструктурата на Портала на електронното управление.

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. През 2023 г. са извършени 14 бр. присъствени и 50 бр. дистанционни проверки на административните органи за оценка за съответствие с изискванията за мрежова и информационна сигурност, определени с Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС) по Закона за киберсигурност, като резултатите показват, че се запазва тенденцията по-голяма част от администрациите да привеждат документацията си съобразно изискванията на НМИМИС – разработени са вътрешни правила, но все още липсва регулярност при обновяване на политиките за сигурност.

От резултатите на извършените проверки се наблюдава негативна практика класификацията на информацията да не се прилага 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

[5] https://egov.government.bg/wps/portal/ministry-meu/home/web-accessibility/monitoring

организацията. На процеса на управление на риска все още не се обръща достатъчно внимание.

Вследствие на проведени в предходни отчетни периоди проверки за спазване задълженията на административните органи от Закона за киберсигурност се регистрира повишаване на сигурността на уебсайтовете на институциите, като голяма част от тях са приложили изискванията на законодателството. При установените нарушения в обхвата на извършените проверки, на съответните организации са издадени надлежни протоколи и са уведомени отговорните лица.

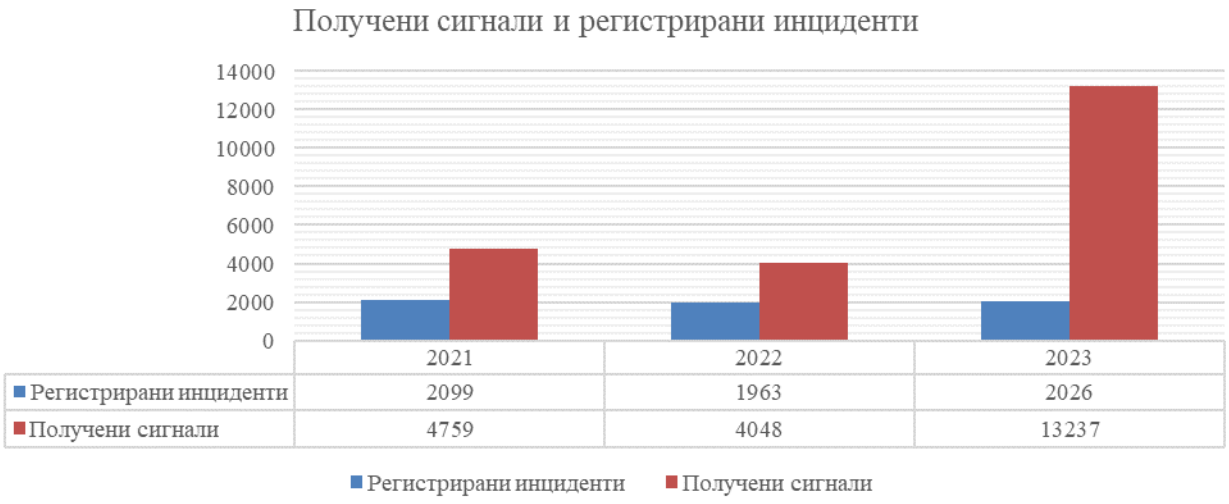
За определяне нивото на мрежовата и информационната сигурност в административните органи администрациите попълват въпросник. На база получен отговор от 322 административни органа се констатира:

	Брой административни органи
По чл. 8 от НМИМИС – не поддържат актуализирани схемите на ИК инфраструктурата и описа на информационните активи.	*75*
По чл. 8 от НМИМИС – не поддържат опис на дейностите и услугите, които се предлагат чрез ИК инфраструктурата на администрацията.	*144*
По чл. 10 от НМИМИС – нямат определени клаузи в договорите за реакция при инциденти и време за възстановяване работоспособността на системите.	*173*
По чл. 10 от НМИМИС – нямат актуален списък с контакти на всички, от които зависи работоспособността на ИК системите, обезпечаващи дейността и услугите, които предоставя администрацията.	*72*
По чл. 10 от НМИМИС – не са провели консултация с доставчици на достъп до Интернет, относно какви мерки могат да предприемат за смекчаване на потенциални кибератаки срещу ИК инфраструктура на администрацията.	*96 (28 са планирали до края на месец ноември)*
По чл. 22 от НМИМИС – не са направили преглед на предприетите мерки за защита на всяко приложение, сървър и мрежово устройство в ИК инфраструктурата на администрацията и не са приложили последните актуализации на използвания софтуер, операционни системи и фърмуер.	*37*
По чл. 23 от НМИМИС – не са направили проверка на актуалността и работата на антивирусните програми.	*19*
По Приложение 6 от НМИМИС – са направили тестване за уязвимости в сигурността и отстраняване на констатираните слабости.	*29*
По чл. 5 от НМИМИС – не са направили преглед на достъпитедо ИКТ ресурси.	*72*
По чл. 32 от НМИМИС – не са направили проверка на резервиране и/или архивиране на информацията и тестване на последните архиви.	*56*
По чл. 32 от НМИМИС – не съхраняват копие на архива офлайн.	*22*

	Брой административни органи
По чл. 4 от НМИМИС (вътрешни правила, заповед, процедури, инструкции) – нямат утвърдена политика за информационна сигурност.	*14*
По чл. 30 от НМИМИС – не са правили проверка на плановете за действие при инциденти.	*43*
По чл. 30 ал. 4 от НМИМИС – имат стратегия за комуникация в случай на инциденти със значително увреждащо въздействие и/или киберкриза.	*23*
По Приложение 6 от НМИМИС – са провели обучения на служителите относно киберхигиената и добрите практики за мрежова и информационна сигурност.	*24*
Нямат списък на отговорните лица от администрацията и фирмите, осъществяващи поддръжка по договор.	*101*
Използват Security Information Event Management (SIEM).	*4*
Използват външни услуги като SIEM, SOC, IaaS, PaaS и др.	*6*

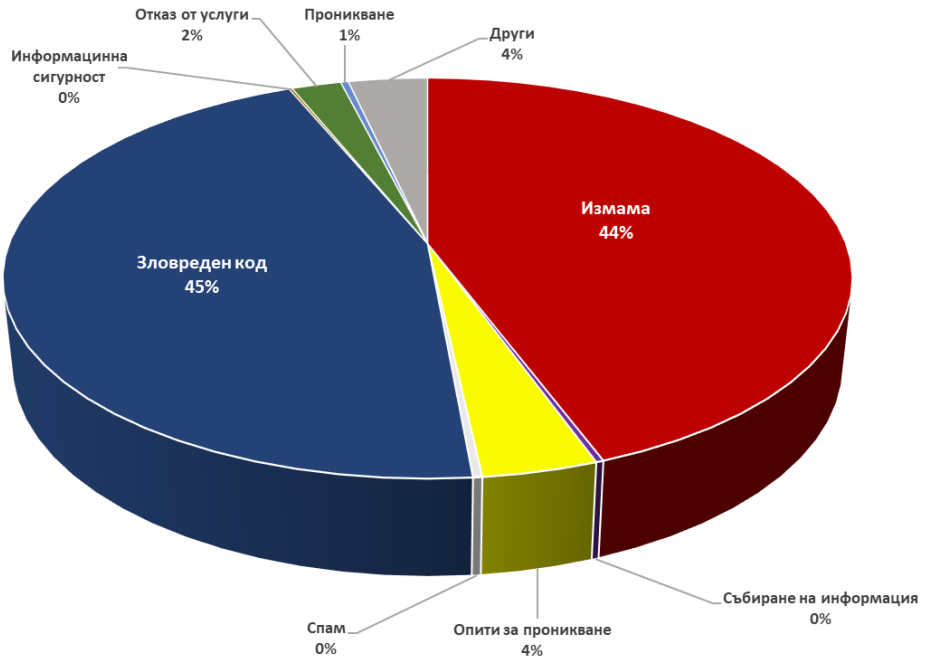
Източник: Министерство на електронното управление
Таблица 8: Получени сигнали и регистрирани инциденти

В периода януари – декември 2023 г. Националният екип за реагиране при инциденти с компютърната сигурност констатира непрекъснато усложняване на обстановката в киберсигурността на страната, като са регистрирани 13 237 сигнала. От тях като инциденти, съгласно таксономията на Европейската агенция за киберсигурност – ENISA, са регистрирани 2 026 бр., което представлява увеличение над три пъти на получените сигнали спрямо същия период през изминалата година.

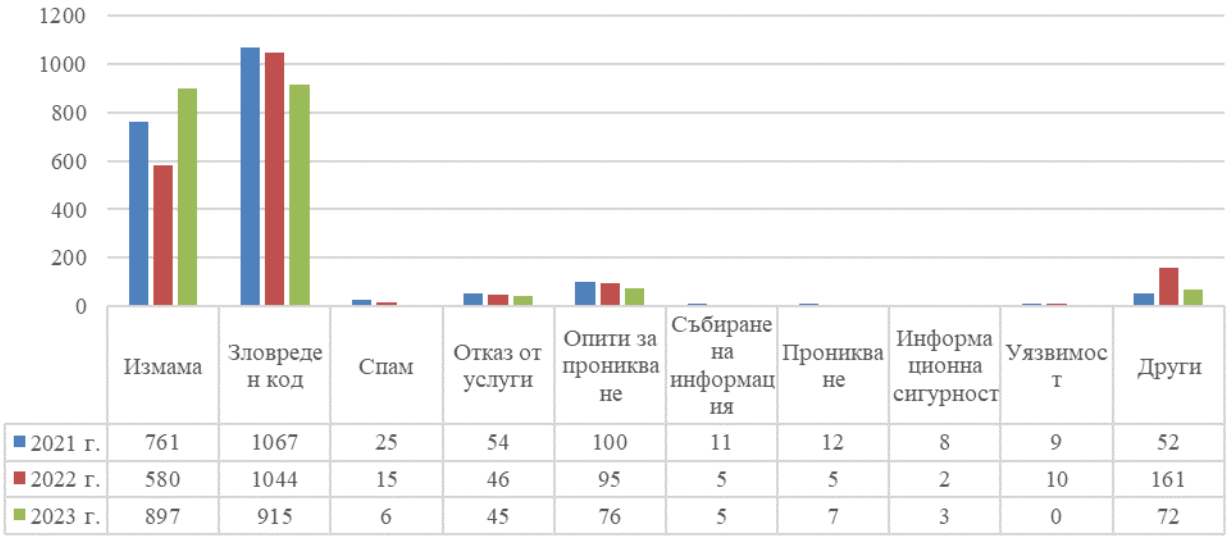


Източник: Министерство на електронното управление
Фигура 20: Получени сигнали и регистрирани инциденти

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 10 363 имейла. На графиките по-долу са показани видовете регистрирани инциденти за отчетния период.



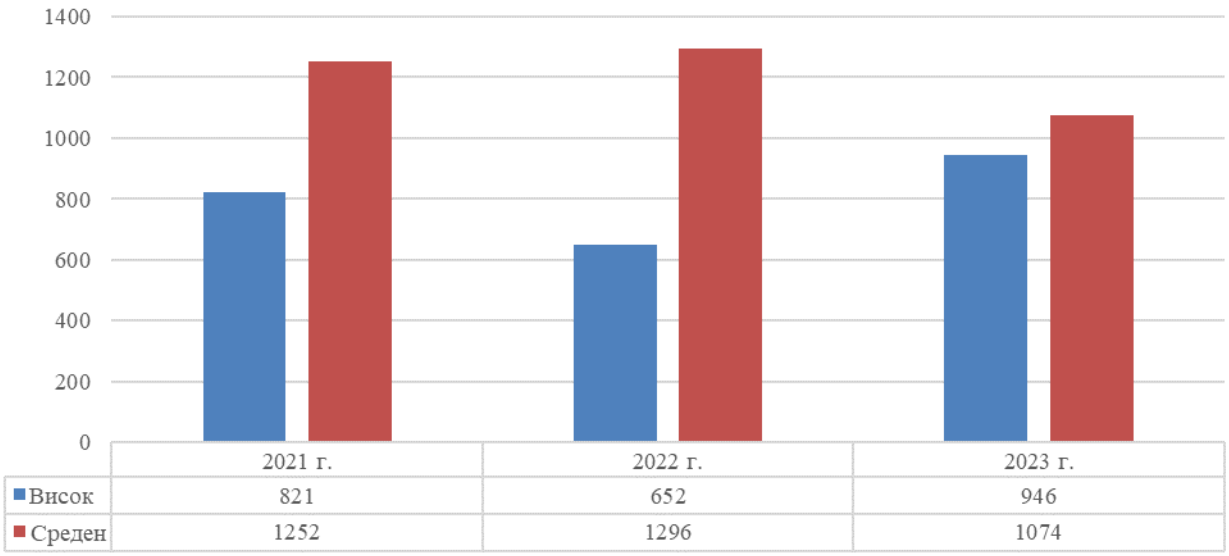
Източник: Министерство на електронното управление
Фигура 21: Видове регистрирани инциденти за периода 01.01.2023 г.-31.12.2023 г.



	Измама	Зловреден код	Спам	Отказ от услуги	Опити за проникване	Събиране на информация	Прониквaне	Информационна сигурност	Уязвимост	Други
2021 г.	761	1067	25	54	100	11	12	8	9	52
2022 г.	580	1044	15	46	95	5	5	2	10	161
2023 г.	897	915	6	45	76	5	7	3	0	72

Източник: Министерство на електронното управление
Фигура 22: Сравнителна таблица на видове регистрирани инциденти за периода 01.01.2021 г.-31.12.2023 г.

През отчетния период се наблюдава намаляване на относителният дял на инцидентите със значително увреждащо въздействие в мрежовата и информационната сигурност със средна степен на опасност.



Източник: Министерство на електронното управление
Фигура 23: Сравнителна таблица приоритет на регистрираните инциденти за периода 01.01.2021 г.-31.12.2023 г.

С избухване на войната в Украйна се наблюдава рязко увеличаване на кибератаките срещу държавите-членки на ЕС. 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 173 463 IP адреса, което е с близо 11% по-малко от 2022 г. В таблицата по-долу са представени данни за последните три години, които включват брой засегнати IP адреси и съответно брой изпратени имейли.

	2023 год.	*2022 год.*	*2021 год.*
Засегнати IP адреси	*173463*	*193270*	*276 970*
Изпратени имейли	*10363*	*15023*	*18 103*

Източник: Министерство на електронното управление
Таблица 9: Сравнителни данни за брой засегнати IP адреси и брой изпратени мейли през периода януари - декември 2021 г., 2022 г. и 2023 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. Причините за успешните атаки най-често са уязвимости в системата или човешка грешка, породена от любопитство, незнание или неволно кликване върху зловреден 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 за сигналите, обработени от CERT България за нарушения в и от българското интернет пространство за предходния месец, актуална информация и препоръки за добри практики.

Продължено е сътрудничеството между Трой Хънт и Министерство на електронното

управление (от 29.03.2022 г.) за използване на ресурсите на Have I Been Pwned – платформа за проверка на компрометираност на online акаунти. С помощта на предоставената услуга бяха извършени поредица от проверки 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. На засегнатите потребители своевременно са изпратени уведомителни имейли с информация за компрометиране на регистрирания акаунт, както и стъпки за предприемане с цел защитата му от неоторизиран достъп.

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

Директива 2022/2555 (ЕС) 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)[6] разширява и обхваща по-голяма част от секторите на икономиката. Разширяването цели да се осигури пълно включване на сектори и услуги от жизненоважно значение за ключови обществени и икономически дейности във вътрешния пазар. 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.

През септември 2023 г. се сформира междуведомствена група с цел транспониране Директивата МИС 2 в българското законодателство, като до 17 октомври 2024 г. да бъде транспонирана.

Създадена е Междуведомствена експертна работна група (МВЕРГ) „Сертификационна рамка на киберсигурността“ към МЕУ и ИА Българска служба за акредитация. Търси се партньорство с други организации, които да се включат в сертификационната рамка на киберсигурността в България.

Европейската агенция по киберсигурност – ENISA продължава да развива Европейска рамка за умения за киберсигурност (ECSF)[7]. 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.

На 19 януари 2023 г. бе проведено редовно заседание на Съвета по киберсигурността (СКС). От съображения за сигурност и по предложение на председателят на Съвета заседанието 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.

На 07 февруари 2023 г. бе проведено изнесено редовно заседание на СКС в дом № 3 в комплекс Бояна. Заседанието се проведе в разширен състав с участието на областните управители с цел да се координират действията на отговорните институции при организиране и провеждането на честни избори за Народно събрание. Подчертана бе важността от функциониране на СКС, който дава насоки при изпълнение на задачи по организацията, управлението и контрола на киберсигурността, която включва мрежова и информационна сигурност, противодействие на киберпрестъпността и киберотбрана. След

[6] Директива - 2022/2555 - EN - EUR-Lex (europa.eu)
[7] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

официалната част на заседанието бе направена демонстрация на придобитите по киберзащита способности чрез Защитения интернет възел (ЗИВ) и на изградените лабораториите и зала за обучение по проект „Изграждане на капацитет и подобряване на услугите, предоставяни от CERT България“.

2.2. Национален координационен център (НКЦ)

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 е необходимо да се осигури финансиране. На 15 февруари 2023 г. НКЦ подаде проектно предложение, което беше одобрено през месец май 2023 г. по Програма „Цифрова Европа“ (Digital Europe Programme). С изпълнението на проекта „Изграждане на Национален Координационен Център“ ще се реализира и предоставяне на безвъзмездна финансова помощ за българските малки и средни предприятия в двугодишния план на проекта „Разгръщане на мрежата от Национални координационни центрове с държавите членки – Bulgarian NCC Project: DIGITAL-JU-SIMPLE , Number: 101128086“, програма „Цифрова Европа.

2.3. Национален екип за реакция на инциденти в компютърната сигурност

Министерството на електронното управление, в качеството 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)[8] 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 е повишаване капацитета на екипите, които се занимават с превенция и реагиране на инциденти.

През 2023 г., във връзка с повишаването на нивото на мрежовата и информационна сигурност, бяха организирани и се проведоха четири срещи със секторните ЕРИКС, извършиха се 50 сканирания за уязвимости в web сайтове и сървъри с публични IP адреси, изготвени бяха 50 доклада с констатирани уязвимости в web сайтове и сървъри с публични IP адреси и препоръки за отстраняването им, също така бе взето участие в 2 национални и международни киберучения. При подготовката и провеждането на парламентарните избори през 2023 г. бяха изготвени и изпратени Указания за повишаване нивото на МИС.

V. ЧОВЕШКИ РЕСУРС В ИКТ

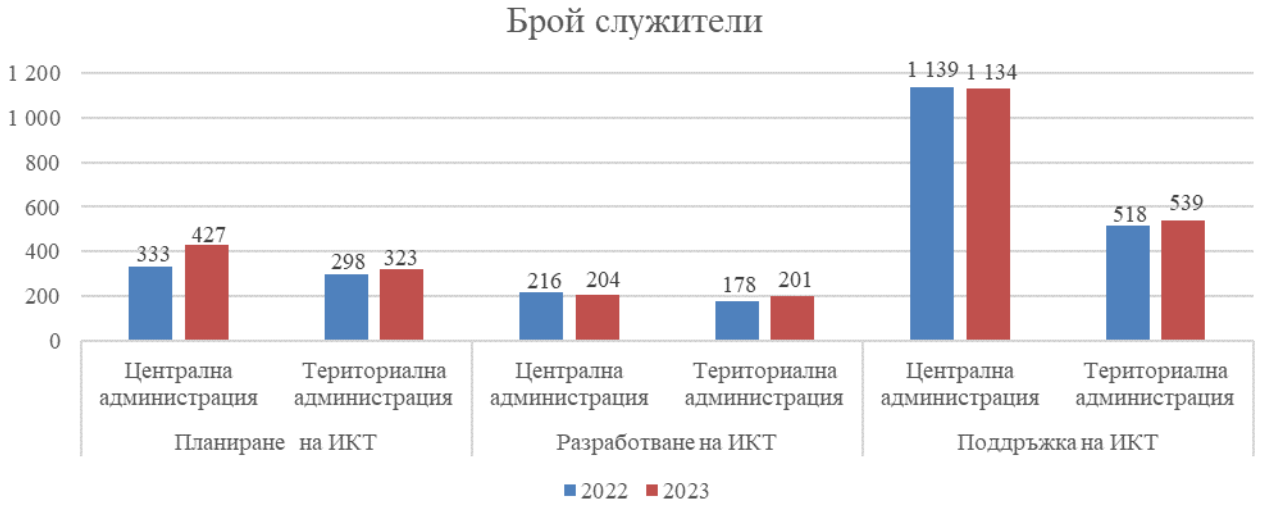
За 2023 г. малко повече от 34% от администрациите разполагат с вътрешен ресурс – вътрешна структура (дирекция, отдел, звено) или отделни специалисти, които да отговарят и извършват поддръжка на информационните ресурси. 182 администрации или 30% от всички през 2023 г. разчитат изцяло на външни изпълнители за поддръжката на своите ИКТ. Макар и малък (19 администрации) се запазва броят на администрациите, които не ползват никакви механизми за поддръжка на своите информационни ресурси.

За 2023 г. се запазва тенденцията малко над 50% от централната администрация да

[8] https://egov.government.bg/wps/portal/ministry-meu/home/programs.projects/finished-projects/cef

ползва външен изпълнител или смесен подход (вътрешен ресурс и външен изпълнител) за поддръжката на информационните ресурси, както и при структурите на териториалната администрация, където по-голямата част близо 60% също разчитат на външен или смесен тип. 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. Като резултат по отношение на поддръжката 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 2023 г. общият брой на служителите в администрацията, занимаващи се с планиране, разработка или поддръжка на информационни ресурси е 3 205 или с 204 повече спрямо 2022 г. Забелязва се увеличаване на служителите в териториалните с близо 7% и в централните администрации с близо 5%. Детайлна разпределение на служителите по вид функция и вид администрация е представено в фигурата по-долу:



Източник: Администрация на Министерския съвет, ИИСДА
Фигура 24: Брой служители в администрацията, ангажирани с ИР

Остава необходимостта от разработването на единна политика за човешките ресурси в държавната администрация в областта на ИКТ, която да цели:

- въвеждане на централизиран подбор на специалисти, като чрез централизирани политики да се насърчават стандарти в държавната администрация. Това е особено важно в области като ИКТ, където сигурността и поверителността са ключови;
- 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 2023 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 са длъжни предварително да съгласуват с министъра на електронното управление разходите в областта на електронното управление и за използваните от тях информационни и комуникационни технологии, като предоставят документи и информация за тригодишните бюджетни прогнози, проектобюджетите за следващата година, утвърдените годишни бюджети и извършените промени по бюджетите си в тази област, текущите и годишните отчети..

Проверките се извършват в съответствие със Задължителни 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). ИСБК и Регистърът на проектите (РП) представляват обща уеб-базирана информационна система.

ИСБК покрива процесите на подаване на информация за контрола на целесъобразността на разходите в областта на е-управлението и ИКТ от административните органи в Република България. Това са всички централни административни органи, първостепенни и второстепенни разпоредители с бюджет, както и всички общини в държавата.

В изпълнение на задълженията в процеса на извършване на предварителен, текущ и последващ контрол по целесъобразност в областта на електронното управление и използването на информационните и комуникационните технологии, в рамките на бюджетния процес за 2023 г., извършените проверки по чл. 7г от ЗЕУ са 707.

По данни от ИСБК, на база постъпилите отчети за касовото изпълнение на утвърдения бюджет, за е-управление и ИКТ за 2023 г., административните органи са изразходвали общо 319 773 322 лв.

Отново по данни от ИСБК, във връзка с подготовката и представянето на проектобюджетите на първостепенните разпоредители с бюджет от централната администрация за 2024 г. и актуализираните им бюджетни прогнози за 2025-2026 г. са съгласувани по целесъобразност целеви средства за е-управление и ИКТ за 2024 г. в размер на 601 608 200 лв.

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.

През 2023 г. от експертите в МЕУ са извършени 625 проверки на проектни предложения и дейности, като по 32 от тях е направен отказ за утвърждаване. За сравнение, за цялата 2022 г. проверките на проектни предложения и дейности са били 221. С измененията на ЗЕУ от 19 септември 2023 г. беше стеснен обхвата на проектни предложения, които се утвърждават от министъра на електронното управление, до тези с прогнозна стойност, по-голяма или равна на стойността на прага по чл. 20, ал. 4, т. 2 от Закона за обществените поръчки.

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 необходимия 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.

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.

Подаването на информация за произнасяне по реда на чл. 58б от ЗЕУ се осъществява чрез Регистъра на проектите, модул „Технически спецификации“. Общият брой на проверените за съответствие с изискванията на чл. 58а от ЗЕУ технически спецификации за 2023 г. е 82.

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, например:
  - много често в техническите спецификации за надграждане или изграждане на информационни системи, чрез които предоставят ЕАУ, администрациите не поставят изискванията, които следват от това, т.е. в техническите спецификации не се предвижда използване на Единния модел за заявяване, заплащане и предоставяне на ЕАУ, както и не се предвижда заявяване на ЕАУ през Портала на електронното управление;
  - 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;
  - 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.
- 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.).
- В технически спецификации, предмета, на които е надграждане на информационни системи, не се представя изчерпателно текущото състояние на системата (т. 4 Образеца по чл. 38 от НОИИСРЕАУ), така, че както проверяващия екип, така в последствие и изпълнителят на надграждането не получават достатъчно добра представа за обхвата на дейността.
- В повечето случаи в техническите спецификации (в т. 8 Образеца по чл. 38 от НОИИСРЕАУ) са представени минимални изисквания към надграждата или изграждана система, а голяма част от спецификата ѝ се предвижда да бъде изяснена от Изпълнителя по време на етапи анализ и детайлизация, което крие риск Възложителя да не получи продукт, който отговаря на истинските му нужди.

4. Контрол по спазване на изискванията на ЗЕУ, във връзка с осъществяване на административнонаказателната дейност на МЕУ

В изпълнение на Годишния план за 2023 г. на МЕУ са извършени 34 бр. планови проверки на административни органи за спазване на разпоредбата на чл. 7г, ал. 4, във връзка с чл. 7г, ал. 2 от ЗЕУ. По шест от тях не бяха установени нарушения или установените нарушения са били с давност, съгласно чл. 34, ал. 1, б. в от Закон за административните нарушения и наказания (ЗАНН), поради което не е образувано административнонаказателно производство. Връчени са общо 50 бр. актове за установяване на административно нарушение (АУАН). Съставени, но невръчени поради невъзможност да се издири нарушителя са 4 бр. АУАН.

Извършени са 5 планови проверки на административни органи от централната администрация за спазване на разпоредбата на чл. 7д, ал. 3 от ЗЕУ. По 4 от тях са установени нарушения, а по 1 установените нарушения са с давност, съгласно чл. 34, ал. 1, б. в от ЗАНН, поради което не е образувано административно-наказателно производство. Връчени са 10 АУАН.

VII. СЪЩЕСТВУВАЩИ ОГРАНИЧЕНИЯ ПРИ ИЗТОЧНИЦИТЕ НА ИНФОРМАЦИЯ

1. Интегрирана информационна система на държавната администрация

Идентифицираните проблеми и пропуски в ИИСДА, които не са решени от 2022 година насам, силно ограничават целесъобразността на системата и интегритета на данните в нея:

- недостатъчно адекватно представяне на административните структури, като множество административни единици не регистрират всички необходими данни в съответствие с регулациите;
- липса на данни относно свързаните услуги, като кой изисква документите, издадени като резултат от услугата, кой ги използва и др.

Отчивайки значимостта на ИИСДА за процесите в администрацията, е неотложно да се предприемат подходящи мерки за преодоляване на тези проблеми.

ИИСДА също е интегрира с Информационната система за попълване на отчетите за дейността и състоянието на администрацията (ИСПОДСА), която е основен инструмент за създаване на годишни доклади за дейността и състоянието на администрацията. Въпреки че тази система улеснява подаването на информация чрез анкети, липсва гъвкавостта

администрациите да създават и публикуват свои анкети за попълване от съответните компетентни органи.

2. Регистър на информационните ресурси (РИР)

Административните органи са длъжни да вписват информация за своите информационни ресурси в РИР в рамките на един месец след тяхното въвеждане в употреба или изваждане от експлоатация. Въпреки това, често се случва те да не добавят данни за новите си ресурси навреме или да обновяват съществуващата информация адекватно. Това води до поддържане на неактуална информация за наличните ресурси, което представлява проблем при управлението и контрола на ИКТ средствата и електронното управление.

Основната роля на РИР е да функционира като инструмент за подпомагане на планирането на информационните ресурси в администрацията. Поради лошото качество на въведените данни и недостатъчните функционалности за тази цел, реализацията на тази функция е затруднена. Това се дължи на липсата на въведени механизми за проверка и стандартизирани критерии за въвеждане на информация, позволяващи попълването на задължителни полета с непроверени данни.

Регистърът работи като самостоятелна система и липсва интеграция със системата за бюджетен контрол на електронното управление, особено в аспекта на годишното планиране на ресурсите. Интеграция между РИР и системата за бюджетен контрол би могла значително да улесни и оптимизира процесите на планиране, бюджетиране и разходване на средства за обновление и поддръжка на информационните ресурси в администрацията.

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

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 (чл. 55 от НОИИСРЕАУ).

Към 31 декември 2023 г. 447 административни органа са въвели информация 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 хардуерен и мрежови информационен ресурс и за закупуване или подновяване на софтуер. 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 за необходимите за обновяване на ИКТ ресурси средства за текущия четиригодишен период възлиза на 3 410 765 847 лева. Разпределението съответно за 2023 г., 2024 г., 2025 г. и 2026 г. е представено на фиг. 25.



Източник: Министерство на електронното управление, РИР
Фигура 25: Планирани средства за обновяване на ИКТ ресурси

В раздел Годишен план в РИР за 2024 г. 447 административни органа са подали информация относно годишните си планове и планираните средства за обновяване на ИР, като са въвели 6 498 записа. Бройките Годишни планове за обновяване са разпределени по следния начин: 68,45% от тях са на централната, специализираната териториална и областната администрация, а 31,55% – на общинските администрации. Планираните средства за обновяване са на стойност 1 044 990 887 лв., като по-голямата част от тях 97,38 % – в централната, специализираната териториална и областната администрация, а 2,62% – в общински администрации.

Годишните планове за 2024 г. за група „хардуерен и мрежови информационен ресурс“ са на стойност 193 747 408 лв. като 94,79% от тази сума е заложена от централната, специализираната териториална и областната администрация, а 5,21% – от общинските администрации.

Планираните средства за 2023 г. за група „софтуер“ са на стойност 146 799 284 лв. като 97,62% са заложени от централната, специализираната териториална и областната администрация, а 2,38% – от 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 2024 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.

Очертаните през предходния период по отношение на развитието на ИР стъпки са претърпели развитие и въз основа на анализа на данните от отчетеното за 2023 г. през 2024 г. следва да се извърши:

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 приеме с акт на Министерския съвет актуализирана Архитектурата на електронното управление, с включени 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 приеме с акт на Министерския съвет Единна политика за 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. Да бъдат предприети мерки за извеждане от експлоатация на ИР, които представляват риск за мрежовата и информационна сигурност.
6. Да бъде предоставена централизирано възможност на административните органи за създаване и водене на регистри изцяло в електронен вид, в съответствие с изискванията за сигурност, надеждност и оперативна съвместимост.
7. Да бъдат надградени РИР и ИИСДА, както и ЦАИС ЕОП, с оглед на получаване на необходимата актуална и достоверна информация за ИР. недостатъци във функционалностите, ограничават възможността за точна оценка и анализ на информационните ресурси;
8. Да бъде разработена единна политика за човешките ресурси в областта на ИКТ в държавната администрация.
9. Да бъдат преосмислени механизмите за финансиране на дейности за е-управление и ИКТ.
10. 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.
11. Да бъдат предприети действия за преминаване към оценка на бюджетите на проектните предложения на принципа TCO – Total Cost of Ownership.
12. Да бъдат въведени проверки за съответствие със ЗЕУ на поръчки за готови софтуерни продукти (напр. системи за документооборот).

IX. ИЗВОДИ

Изводите се базират на анализ на състоянието на информационните ресурси в администрациите регистрирани в ИИСДА и РИР, както и от справки, извлечени от хоризонтални системи на електронното управление.

Постигането на интегрирана технологична екосистема, подпомагаща цифровата трансформация на държавната администрация, предвид състояние на информационните ресурси в държавната администрация на България, налагат актуализирането и допълването на Единната политика за информационните ресурси и на Архитектурата на електронното управление.

През 2023 г. се отчита значително намаление в обема на хардуерните активи, което се дължи на надграждане или подмяна на остаряло оборудване, консолидация на ресурси и преминаване към нови технологии. Един от най-значимите спадове е в категорията „Поддържащи системи“. Същата тенденция се наблюдава и в категории „Сървърни/комуникационни шкафове“, „Запаметяващи устройства“ и „Физически сървъри“. Отчетеният спад се дължи на преминаване към централизирани решения за поддръжка, консолидиране на ресурсите в администрациите, прилагането на по-ефективни методи за управление на данните, както и преминаването към виртуализация и облачни решения.

Промяната в броя на активите в РИР се дължи на технологичния напредък и промените в бизнес стратегиите. Въпреки това за оптимизирането на ИР, продължаващата липса на стандартизация във видовете и типовете използвани хардуерни ресурси, е предизвикателство.

Запазва се тенденция все повече администрации да използват в своите административни процеси и в комуникацията с гражданите, бизнеса и помежду си хоризонталните и централизираните системи на електронното управление. Пример за това е значителният ръст в броя на изпратените съобщения чрез Системата за сигурно електронно връчване, както и в броя на предоставяните вътрешни електронни административни услуги.

Предоставената възможност за цялостното цифрово взаимодействие с администрациите чрез Системата за електронно връчване все повече се предпочита, за което говори нарастналия брой на потребители през 2023 г.

Унифицираният модел за централизирано подаване на заявления, извършване на плащания и получаване на електронни административни услуги, осигуряващ възможност за предлагане на все повече електронни услуги изцяло онлайн през единна входна точка, допринася за повишаване на качеството и стандартизацията на услугите, генерира икономии за бизнеса и гражданите и способства за подобряване на бизнес климата в България.

Все по-често като ефикасен механизъм за граждански контрол над институциите и за подобряване на качеството на данните в основните държавни регистри при защита на личните данни се използва услугата за „Персонална справка на физическо лице за достъп до лични данни по идентификатор (ЕГН) и период“, предоставена от Министерството на електронното управление.

Основните регистри и системи на централната администрация вече са интегрирани чрез информационната система за обмен на справочна и удостоверителна информация (RegiX). Над 340 милиона са генерираните заявки към регистри и са извършени над 119 милиона справки до края на 2023 г. Отпадането от необходимостта от физическо посещение в администрации и предоставяне на документи на хартиен носител води до икономии за обществото. Продължава развитието на RegiX чрез присъединяване на нови регистри,

справки и данни.

През 2023 година системата за електронни плащания въведе подобрения и функционалности, включващи уведомления за регистрирани нарушения, в съответствие с измененията в Закона за движение по пътищата, онлайн проверки и плащания на задължения, произтичащи от регистрираните нарушения, както и плащане на местни данъци и такси, което доведе до значителен ръст в потреблението ѝ. Тези разработки подчертават ефикасността и удобството на системата и улесняват взаимодействието между гражданите, бизнеса и държавата.

За да се гарантира непрекъснатото и защитено функциониране на системите за електронно управление, административните органи е необходимо при разработването, поддръжката и развитието на информационните си системи да се ръководят от общоприети стандарти за разработка, управление и поддръжка. За постигането на интегрирана технологична екосистема интеграцията между системите на различните администрации и централизираните и хоризонталните системи за електронно управление е задължителна. За осъществяването на тези цели е необходимо и стратегическо планиране, както на дейностите, така и на бюджета, обхващащо период от три години, което да гарантира не само разработването, но и последващата поддръжка на тези системи.

Все още не е изградена националната държавна схема за електронна идентификация, предвидена в ЗЕИ, 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. В условията на лисваща схема по ЗЕИ, през 2023 г. е призната първата българска национална схема за електронна идентификация с нива на осигуреност „значително“ и „високо“, издавана от частноправен субект. Схемата осигурява възможност както за национално, така и за трансгранично заявяване на електронни услуги със средство за електронна идентификация, издадено в Република България. Продължава работата по разширяване на кръга от нормативно признати средства за електронна идентификация с цел осигуряване на надеждно взаимодействие по електронен път между гражданите, бизнеса и публичните органи.

През 2023 г. е увеличен броят на потребителите на облачни услуги, предоставяни от ДХЧО, като ползващите ресурси администрации са нараснали значително. Продължава развитието на ДХЧО, изразяващо с измерими количествени показатели като предоставено дисково пространство и брой виртуални машини.

В областта на мрежовата и информационна сигурност 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. През 2023 г. в голяма част от администрациите има определен служител или административно звено, отговарящ за мрежовата и информационната сигурност.

В областта на човешките ресурси в ИКТ разработването на единна политика за човешките ресурси в държавната администрация в тази област би допринесло за успешната реализация на политиката за е-управление, за постигането на информационната сигурност и за изграждането на ефективна цифрова администрация. Без компетентни и мотивирани служители в областта на ИКТ няма как да се посрещнат предизвикателствата, свързани с цифровата трансформация на обществото ни и прилагането на съвременни технологични решения в областта на управлението на данни и изкуствения интелект.

Постигнато е 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. Нарасналият в пъти брой на представените за съгласуване данни в Информационната система за бюджетен контрол и Регистъра на проектите, говори за постигнатите резултати от контролната

дейност на МЕУ.

X. ЗАКЛЮЧЕНИЕ

До октомври 2024 г. следва Директивата МИС 2 да бъде транспонирана в българското законодателство и да се определят мерки за управление на риска в областта на киберсигурността, както и национални рамки за управление на кризи. Предстои актуализация и на националната стратегия за киберсигурност „Киберустойчива България 2023“.

Националната схема за електронна идентификация, предвидена в Закона за електронната идентификация, досега не е реализирана, което затруднява развитието на електронното управление и ограничава възможностите на гражданите и бизнеса за достъп до електронни административни услуги.

За осигуряване на дълготраен и устойчив модел на електронно управление, е необходимо продължаване на стратегическите усилия за осигуряване на оперативна съвместимост и ефективна интеграция на информационните ресурси. Въпреки значителните подобрения в областите на електронното управление, както и на мрежовата и информационната сигурност, все още липсва цялостна и интегрирана технологична екосистема в рамките на държавната администрация.

СПИСЪК НА ФИГУРИТЕ

Фигура 1: Разпределение на работните станции по година на придобиване 10
Фигура 2: Видовете ГИС услуги предоставяни в администрациите през 2023 г. 13
Фигура 3: Брой разработени услуги по години 14
Фигура 4: Справка за посещения на портала за 2023 г. 15
Фигура 5: Статистика за успешно автентикирани потребители със средства, поддържани от системата 16
Фигура 6: Справка за посещения на системата за електронна автентикация за 2023 г. 16
Фигура 7: АИС клиенти и преминали трансакции в системата за еПлащане 17
Фигура 8: Успешни трансакции в системата за еПлащане – стойност в лв. 17
Фигура 9: Справка за посещения на системата за електронно плащане за 2023 г. 18
Фигура 10: Брой заявявания на ЕАУ по години 19
Фигура 11: Брой регистрираните потребители в ССЕВ по години 19
Фигура 12: Справка за обменените съобщения по години 20
Фигура 13: Справка за посещения на системата за сигурно електронно връчване за 2023 г. 20
Фигура 14: Брой предоставени вътрешни електронни административни услуги за периода 2017 - 2023 г. 21
Фигура 15: Топ 5 „Консуматор“ на вътрешни електронно административни услуги през 2023 г. 21
Фигура 16: Топ 5 посещавани администрации през 2023 г. 22
Фигура 17: Внедрени информационни системи и брой работни места 23
Фигура 18: Регистри с обмен и интеграция на данни 26
Фигура 19: Брой услуги от ниво 3 или ниво 4 по години 31
Фигура 20: Получени сигнали и регистрирани инциденти 34
Фигура 21: Видове регистрирани инциденти за периода 01.01.2023 г.-31.12.2023 г. 35
Фигура 22: Сравнителна таблица на видове регистрирани инциденти за периода 01.01.2021 г.-31.12.2023 г. 35
Фигура 23: Сравнителна таблица приоритет на регистрираните инциденти за периода 01.01.2021 г.-31.12.2023 г. 36
Фигура 24: Брой служители в администрацията, ангажирани с ИР 39
Фигура 25: Планирани средства за обновяване на ИКТ ресурси 45

СПИСЪК НА ТАБЛИЦИТЕ

Таблица 1: Въведени активи в РИР 11
Таблица 2: Разпределение на антивирусния софтуер 13
Таблица 3: Администрации, които нямат внедрени информационни системи. 22
Таблица 4: Регистри, свързани с предоставянето на ЕАУ за гражданите и бизнеса 26
Таблица 5: Регистри, които се поддържат в електронен вид 26
Таблица 6: Инсталирани основни систем в центровете за данни 27
Таблица 7: Списък на държавните организации, ползващи ресурси в ДХЧО към 2023 г. 29
Таблица 8: Получени сигнали и регистрирани инциденти 34
Таблица 9: Сравнителни данни за брой засегнати IP адреси и брой изпратени мейли през периода януари - декември 2021 г., 2022 г. и 2023 г. 36