https://doi.org/10.70265/FGGE7899

СИГУРНОСТ НА ЦИФРОВАТА ИДЕНТИЧНОСТ

Теодора Личева

DIGITAL IDENTITY SECURITY

Teodora Licheva

***Резюме**: Дигиталната ера, в която живеем навлиза във всяка сфера на живота ни, променя вида и формата на информацията. Цифровата идентичност е нашето дигитално копие, и затова е от първостепенно значение е да се гарантира защита на данните и мрежовите устройства.*

***Ключови думи**: сигурност, цифрова идентичност, блокчейн, е-услуги*

***Summary**: The digital age in which we live enters every sphere of our lives, changes the type and form of information. Digital identity is our digital copy, and therefore it is of utmost importance to ensure the protection of data and network devices.*

***Key words:** security, digital identity, blockchain, e-services*

УВОД

Все по-голяма част от живота си прекарване онлайн, светът ни става все по-дигитален и това променя и понятието за идентичност.

Дигиталната трансформация и развитието на технологичните възможности е предпоставка за създаване на цифрова самоличност. В статията са предложени съвременни решения, с които да се гарантира сигурност на цифровото доказателство за самоличност и да се осигури защита на данните и мрежовите устройства.

1. СИСТЕМА ЗА УПРАВЛЕНИЕ НА САМОЛИЧНОСТТА И ДОСТЪПА

Управлението на самоличността и достъпа е ключов момент за организации, политики и технологии. С правилното управление се гарантира контрола на достъпа до чувствителна информация и предотвратяване изтичането на данни (Личева, 2024, с. 56).

Управлението на самоличността и достъпа включва следните инструменти:

- управление на пароли;
- система за единно влизане;
- двуфакторно удостоверяване;
- многофакторно удостоверяване;
- управление на привилегирован достъп;
- управление на привилегирована идентичност.

Използването на тези инструменти гарантира сигурно съхранение на данните и позволява да се споделят само тези, които са необходимите и подходящите.

Причините, които определят важността на управлението на самоличността и достъпа са следните:

1. Подобрява се сигурността на данните. Използването на контрол на потребителския достъп намалява до минимум кражбата на самоличност, изтичането на данни и нерегламентиран достъп до чувствителна информация. Системите за управление на самоличността и достъпа предпазват от кибератаки, фишинг и др. злонамерени действия.

2. Оптимизира се работното време. С актуализиране на политиките на сигурност има възможност да се променят наведнъж всички контроли за достъп.

3. Осъществява се контрол за спазване на законови и нормативни рамки. С въвеждане на управление на самоличността и достъпа се гарантира и сигурност на потребителските данни, особено когато става въпрос за чувствителни данни използвани за е-здравно досие, онлайн банкиране и т.н.

4. Намаляват се до минимум човешките грешки. Елементите за управление премахват напълно ръчните грешки в акаунта на потребителите и неговите разширения. Правата на достъп до данните вече не се контролира ръчно от отдела по сигурност, а процеса става автоматизиран.

5. Осъществяване на ефективен достъп до ресурси. Потребителите се възползват от системите за единично влизане, защото с тях се ограничават възможностите за нерегламентиран достъп до ресурсите на организацията.

6. Гарантиране поверителността на данните. С въвеждането на управлението на самоличността и достъпа се повишава защитата на данните и организациите защитават най-ценните данни, т.нар. чувствителни данни и извършват постоянен мониторинг на свързаностите на потребителите.

7. Подобрява се достъпа между браузъри и устройства. С облачните приложения потребителят има достъп до браузъра от всяко

устройство, което е свързано с интернет. Като недостатък може да се приеме, че повечето приложения означават и повече адреси и пароли.

Инструментите на управление на самоличността и достъпа, които са базирани в облака, дават възможност чрез системи за единично влизане да се използват същите услуги от мобилните устройства на потребителите.

Въпреки изброените предимства и преимущества трябва да обърнем внимание и на рисковете, които крие платформата за управление на самоличността достъпа (фиг. 1).

Фигура 1. Рискове при внедряване на система за управление на самоличността и достъпа

С централизираното управление се поставя една цел – ограничаване и спиране на недоброжелателите и на опитите за нерегламентиран достъп до данните и затова трябва да се полагат повече грижи за правилното осигуряване на платформата с мрежови инструменти за сигурност. Неправилното управление на достъпа може да доведе до неправилно разпределение на задълженията и да наруши контрола на достъп до данните в организацията. При изготвяне на правила за достъп изниква въпросът: Кой трябва да ги направи? – служителите по сигурност или ръководителите на организацията. Препоръчва се създаването на политика, с която ясно се определя кой до какви приложения има достъп и дали има нужда от тях в сферата на своята дейност. Процесите по управление на достъпа не са достатъчно автоматизирани. Рутинните и повтарящи се процеси трябва да са

автоматизирани и да не губят време на администраторите да се ангажират и с тях. Няма визия за мабащируемост на платформата, за да може да отговори на новите изисквания. Администраторите трябва да бъдат обучени да настройват стъпките за автоматизация и да осигурят правилното им функциониране. Задължително е да се изискват редовни одити на управлението на самоличността и достъпа, за да се са актуализирани правилата и те да са в синхрон с използването на новите данни или приложения.

Анализираните рискове са част от най-често срещаните предизвикателства пред организациите, които внедряват системата за управление на самоличността и достъпа. Защитните стени, системата за предотвратяване на заплахи и строгата политика за достъп са част от ефективните процеси, които гарантират правилно използване на платформата с точен и ясен достъп до данни, само на служители, които се нуждаят от нея за дейността си.

Съвременните инструменти за управление на идентичността и достъпа работят в синхрон с екипите по сигурност, за да могат да управляват контрол над данните и използването от служители, клиенти и оторизирани групи. Пандемичната обстановка от Covid 19 направи тези инструменти още по-ценни и необходими, за да може правилно и сигурно да функционира организацията.

Основна цел на управлението на идентичността и достъпа е да определи кой иска достъп до данните на организацията и да се потвърди дали наистина трябва да се даде пълномощно на идентифицираните потребители. Условно могат да се определят следните общи характеристики на платформите за управление на самоличността и достъпа:

1. Управление на идентичността. Това е ръководния подход, с които платформата доказва, че е в синхрон със спецификата за съответствие.

2. Централизирано управление на достъпа. Без значение къде се намира приложението, то се управлява централизирано с контролите за достъп и оторизирано използвано, важат за цялата инфраструктура.

3. Система за единично влизане. Тази система е поредица от действия, с които потребителите могат да се удостоверяват еднократно, чрез централизирания портал, и да имат пълен достъп до базата данни на организацията.

4. Обезпечаване на потребителя. Инструмента включва дейности по създаване на акаунт и определяне на роля за оторизация.

5. Многофакторно удостоверение. Този процес гарантира повече от един метод за удостоверяване на потребител или устройство.

6. Мащабируема рамка за удостоверяване и контрол на достъпа. Тази платформа е централизирана, по-лесна и лека за управление.

7. Синхрон на дейността на потребителя. Това е процес по контрол на съответствието. Той спомага да защитата и идентифицирането на рисковете за дейността по отношение на защита на данните.

8. Достъп до портална услуга. Това е самообслужване в портала. Служители и клиенти спестяват време и могат да се саморегистрират, управляват профили и нулират пароли за достъпа.

9. Код на приложно програмен интерфейс (*англ*. Application Programming Interface)[1]. Той може да създаде персонализиран край и да позволи приложението да удостоверява и контроли достъпа. След като този код насочва задачите към системата за управление на идентификацията и достъпа той може правилно да идентифицира потребите и да предостави или откаже достъп.

10. Анализ на риск. Част от платформите събират удостоверявания, както и потреблението на акаунта, както и данни за местоположение, часови диапазон и искания достъп. С тези събрани данни може да се открият аномалии и нетипично поведение на потребителите и да насочат вниманието на екипите по сигурност към атаки или нерегламентиран достъп.

Системата за управление на идентичността и достъпа е първият и последен етап на защита срещу нерегламентиран достъп и атака, базирани на идентификационни данни. В тази връзка идентичността се определя като същината на сигурността в облака и неприкосновеността на личните данни.

2. БЛОКЧЕЙН И УПРАВЛЕНИЕ НА ИДЕНТИЧНОСТТА

Съвременното ни ежедневие е така устроено, че по-голяма част от него минава в режим онлайн, затова удостоверенията кои сме в дигиталната среда са от първостепенно значение за хората и организациите. Хората искат да контролират самоличността си и с кого споделят личната си информация, а организациите са изправени пред нови предизвикателства за сигурността, автоматизация на работните процеси и подобряване на живота на служители и клиентите.

Управлението на самоличността и достъпа е ключов елемент за управление и удостоверяване на цифровите самоличност (TechTarget, 2021).

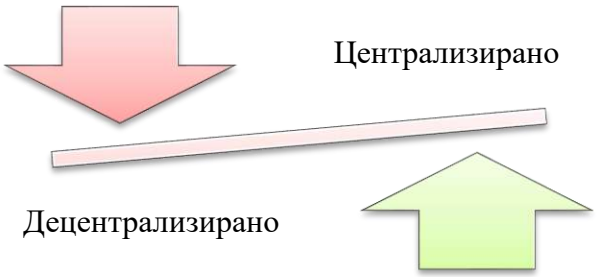
Блокчейн се различава от системите за управление на идентичност и достъп, защото той е децентрализиран и позволява записване на трансакциите и удостоверяванията (Личева, 2023, с. 19). Те се записват и проверяват от мрежа, а не от един централен орган.

Дигиталната среда предполага и нарастване на киберпрестъпленията и както хората, така и организациите имат

[1] Интерфейс за приложно програмиране. Това са механизми, които позволяват на два софтуерни компонента да комуникират едни с друг, използвайки набор от дефиниции и протоколи

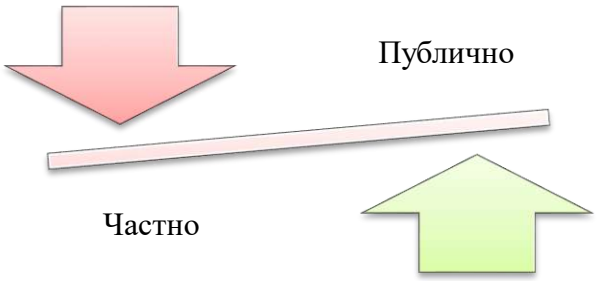
решаваща роля да защитят чувствителните данни, сигурността на устройствата и оперативната инфраструктура и не на последно място цифровата идентичност на хората.

Използването на децентрализиран регистър в процесите по управление на самоличността и достъпа са в различи аспекти – правни, технически, бизнес.



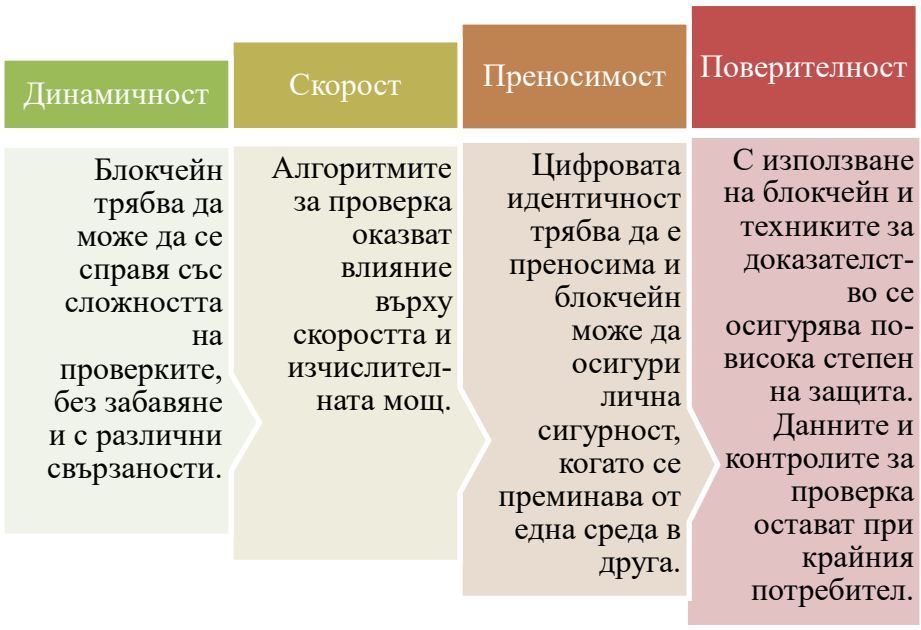
Фигура 2. Децентрализиран или централизиран регистър

Организациите работят с централизирана и собствена инфраструктура за съхранение на данни. Това от своя страна изостря отношението на притежателя на данните и онези, които ги използват. Използването на блокчейн, като децентрализирана инфраструктура, дава възможност за ефективни и индивидуални ползи.



Фигура 3. Частна или публична инфраструктура

Публичните блокови вериги не се предпочитат от институциите, защото се изисква поверителност и допълнителни разрешения за добавяне и управление на блоковата система. Важно място заема гарантиране на сигурността, изчисленията и скалируемостта.



Фигура 4. Предизвикателства пред блокчейн за цифрова идентичност

От гледна точка на стандартите има затруднение, поради несъществуващи стандарти за блокчейн технологии и оперативна съвместимост през веригата. За преминаване от централизирана към децентрализирана система е необходимо да има взаимосвързаност, координация на данни и системи за управление. Необходимо е да се синхронизира и нормативна уредба за база данни и регламента за лични данни и тук се получава противоречие с неизменността на регистрите данни. Нововъзникващите данни се генерират и употребяват в по-голям мащаб и трябва да се вземат предвид текущи и дългосрочни рискове за съответствие и поверителност.

3. ВНЕДРЯВАНЕ НА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ИДЕНТИЧНОСТТА И ДОСТЪП ДО ДАННИ НА УСТРОЙСТВА

Правилното управление на процеси на достъп до идентичността дава разрешение на оторизирани потребители и на устройствата по подходящ, ролеви достъп. Тези устройства са мобилни устройства, сървъри, софтуери, виртуални машини, всички свързани с интернет на нещата устройства.

Машините също се нуждаят от удостоверение, което се постига с криптографски ключове и цифрови сертификати.

Криптографските ключове за сигурност и интернет протоколите удостоверяват самоличността на устройството и то може да се свързва с други машини, да получи достъп до мрежите, ресурсите и данните им. Роля на организацията е да следи идентичността на машините и да

контролира подходящ достъп. Ако ключовете са с изтекъл срок и валидност, това ще доведат до грешки и прекъсване на дейност и услуги.

Самоличността на машините също е поставена под постоянни хакерски атаки, защото чрез нея ще получат достъп до ресурси и данни на организацията и могат да използват нерегламентирано чувствителните ѝ данни.

Много трудно е управлението на идентичността на машините. Основна причина на това е постоянно нарастващия брой от устройства, с различни спецификации, и ключове. От друга страна валидността на цифровите сертификати също намалява. Transport layer security (TLS)[2] сертификата вече е с валидност до 398 дни (TechTarget, 2021).

За да успеят да гарантират сигурно управление на идентичността на устройствата компаниите трябва да извършват постоянни обучителни процеси на експертите от отделите за сигурност и да прилагат най-добрите практики за валидиране на ключовете. Постоянен мониторинг и видимост в цялата инфраструктура на компанията на системата за управление на идентичност е добро решение за правилното ѝ експлоатиране. Ръчното управление на сертификати и настройки не се препоръчват, поради възможност за човешка грешка и нерегламентиран достъп.

Друг акцент е правилно да се съхранява списъкът на сертификати и ключове. Автоматизиран инструмент за сканиране в мрежата ще определи както употребата на всеки ключ, така и местоположението му. Инструментът за сканиране трябва да действа и извън устройствата и да може да открива ключове в облака и Интернет на нещата. Ключовете трябва да се съхраняват на централизирано и сигурно място, с ограничен и контролиран достъп.

Постоянния мониторинг ще успее да набележи невалидни ключове, фалшиви сертификати и слабите пароли.

Поради много процеси, които изпълнява централизираното управление за идентичност, има вероятност да се забави разработването и издаването на сертификати. За да се разреши този проблем може да се позволи на отделни отдели да предоставят, подновяват и анулират сертификати за самообслужване, но с необходимите ограничения.

Въпреки всички действия по осигуряване на сигурност на идентификацията и достъпа на устройствата все пак има вероятност да се стигне до инциденти и затова трябва да се създаде план за реакция и ограничаване на зловредния и нерегламентиран достъп. Предпочитан

[2] Сертификат, който осигурява защита на информацията в мрежова среда. Той се прилага за криптиране на данни, удостоверяване на самоличността на сайта и потвърждава целостта и достоверността на данните (бел.авт.)

вариант е да се създаде и внедри автоматизиран инструмент за управление на ключове, който да реагира при заплаха и да направи групови промени на всички засегнати устройства.

Изграждането и внедряването на система за управление на идентичността и достъпа до данни е голямо предизвикателство за организациите, но тя е от ключово значение за правилната употреба и достъп до ресурсите на структурата. Новите методи за сключване на сделки, бизнес процеси и споразумения изискват и нови и дигитални услуги, които да отговорят на съвременните технологични възможности. За да могат да се защитят организациите трябва да са поне една крачка през киберпрестъпниците и да имат изработен план срещу недоброномерените действия.

Част от промените, които са наложителни, за да бъде конкурентно способна и сигурна една структура, са свързани с изготвяне на анализ, който да определи силните и слаби страни на организацията, да оцени състоянието на системите за сигурност, да се дефинират идентичностите – на служители и на устройства, стриктно спазване на политиките на сигурност и избор на най-подходящите решения от технологична гледна точка. Данните са най-важната част от организацията и тяхната сигурност и поверителност ще определят и бъдещето на структурата.

4. ЛИЧЕН ЦИФРОВ ПОРТФЕЙЛ

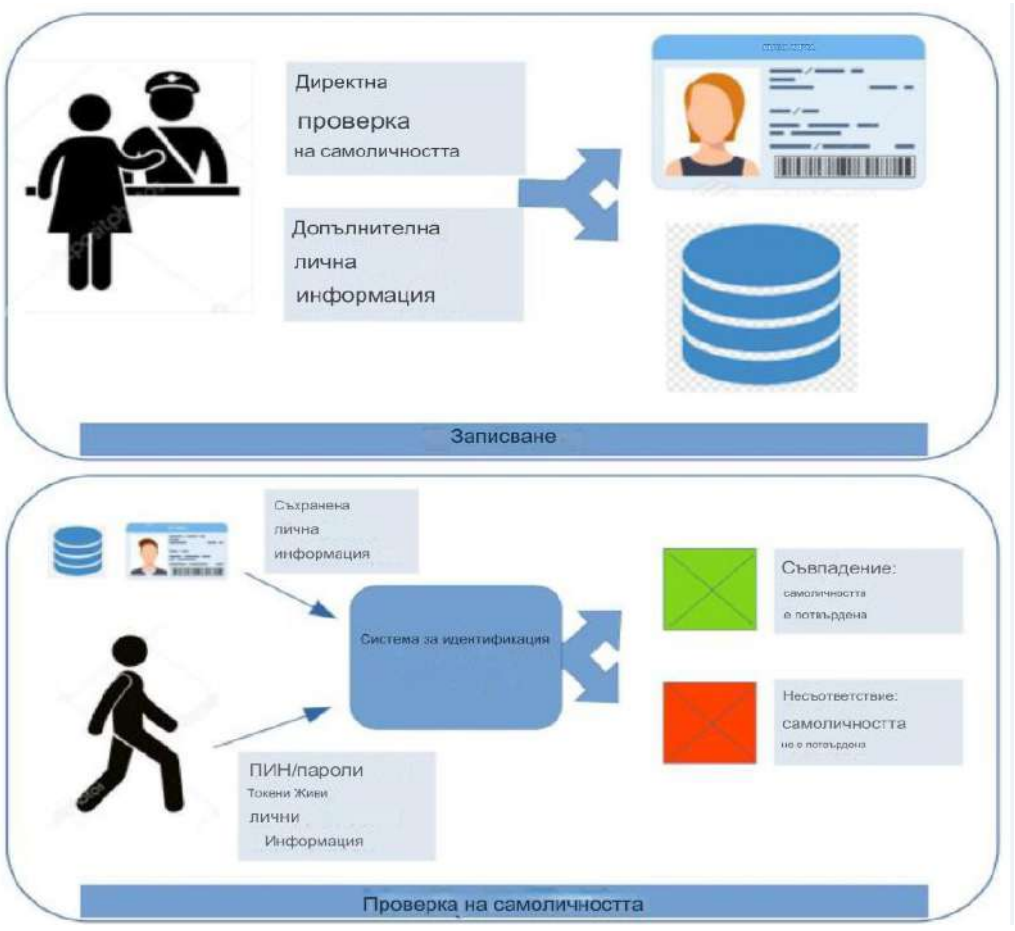
Цифровият личен портфейл е дигиталното ни доказателство за самоличност. Технологичният напредък върви с много бързи темпове и липсват регулаторни рамки, използват се личните и чувствителните ни данни по нерегламентиран и не достатъчно сигурен начин. Всичко това е процес по бързото развитие на технологии и забавено законодателство в областта.

Европейският съюз отбелязва значителна преднина от гледна точка на нормативната база с въвеждането на Общ регламент за защита на данните (Регламент (ЕС) 2016/679) и Регламентът за услугите за електронна идентификация, удостоверяване и доверие (Регламент (ЕС) № 910/2014). Европейската регулаторна рамка поставя в центъра си биометричните характеристики и въвеждането им в електронни карти за национална самоличност[3], но все още тези данни не се използват за идентификация и удостоверяване на лице в цифров формат (Ruiu, Saiu, & Grosso, 2024).

[3] Италианските eID са пример за използване на биометричните данни в съответствие с регламентите на ЕС. Използването на тази двойна автентификация ще подобри значително сигурността и надеждността на системите. Ще се повиши доверието в системите за електронна самоличност и ще стимулира навлизане в употреба, като добра практика. (бел.авт.)

Използването на биометрични данни е от ключово значение за справяне с предизвикателства като сигурност, лична идентификация и достъп до електронни услуги. Все още събирането и използването на биометрични данни поставя под въпрос неприкосновеността на личния живот на гражданите, достъп и контрол при употребата им и възможността за нерегламентираното им използване. Въпреки, че машинното обучение и алгоритмите на изкуствения интелект могат да подобрят достоверността и надеждността на биометричните системи остават проблемите от гледна точка на нормативната уредба.

Електронната идентификация е възможността за достъп до публични и частни услуги, но в повечето случай тези услуги не отговарят на обща схема за цифрова самоличност.



Фигура 5. Схематично изразяване на двете фази за цифрова идентичност (Адаптирано по: Ruiu, Saiu, & Grosso, 2024)

Първата фаза на записване включва дейности проверка на самоличност и лична информация. Много често тази информация е съхранена в електронен носител, като лична карта с микрочип или в защитена база данни. Това всъщност е средството за електронна

идентификация. Втората фаза включва самата електронна идентификация и достъп до услуги и ресурси.

Схемите за цифрова идентификация са голямо предизвикателство от гледна точка на правно-нормативната уредба и интеграция на информационните технологии. Съществуващите схеми гарантират високо ниво на сигурност, но избягват биометричните данни, поради чувствителността им. Друг проблем е оперативната съвместимост и управлението на данните от наднационално ниво.

5. ЕВРОПЕЙСКИ ЛИЧЕН ЦИФРОВ ПОРТФЕЙЛ

Предвижда се европейската цифрова самоличност да може да се използва онлайн и офлайн за предоставяне на услуги в съюза. С нея гражданите от страни членки на Европейския съюз (ЕС) ще могат да се идентифицират, както и да потвърдят свои данни.

Всички граждани на ЕС, които отговарят на условията за издаване на национална лична карта ще могат да:

- притежават лична карта, която е призната цифрова самоличност и валидна в ЕС;
- контролират кои лични данни да споделят с услуги, за които са необходими лични данни;
- управляват, чрез цифровия портфейл, приложения и платформи за онлайн и офлайн идентифициране, съхранение и обмен на данни от държавния апарат, които са надеждни източници и доказателство за пребиваване, обучение, работа и др. в страни членки на ЕС.

Въвеждането на цифрова идентификация е затруднено, защото не е достъпно за цялото население на съюза, с труден трансграничен достъп и често услугите, за които е достъпен, са само онлайн.

Важно е да се отбележи, че само 14 % от доставчиците на е-услуги позволяват трансгранично удостоверяване на самоличността (Европейска комисия, 2021).

Най-важно за гражданите на ЕС е да ми гарантират правилно и сигурно обработване на данните, при използване на социалните медии, както и да имат сигурна и единна цифрова лична карта, с която да могат да използват всички онлайн услуги на общността.

Ключови елементи		
Достъпност за всички граждани и организации в ЕС.	Идентификация или потвърждение на лични данни, необходими за предоставяне на цифрови услуги в ЕС.	Контрол, сигурност и проследимост на данните, сертификатите и елементите, които гражданите споделят в трети лица с ЕС.

Фигура 6. Основни принципи на европейския личен цифров портфейл

Въвеждането на европейски електронен цифров портфейл дава възможност по дигитален начин да се докаже самоличността на гражданите в целия съюз. Важна характеристика е, че те сами ще могат да избират с коя конкретна лична информация да споделят, без да се налага да се разкрива пълната им самоличност или други лични и чувствителни данни.

Основно преимуществото е, че гражданите ще имат контрол върху данните си. Те ще са защитени и ще може да се проследяват и споделят само регламентирано.

Таблица 1. Услуги за идентификация и удостоверителни услуги за граждани и организации (Европейска комисия, 2021)

		Граждани	Предприятия
	Електронен подпис Изразяване в електронен формат на съгласието на дадено лице със съдържанието на документ. Функцията ще бъде интегрирана в портфейла.	Ще позволи подписването на правни документи и електронна поща без отпечатване на хартия	Ще намали разходите и сроковете чрез рационализиране на процесите и ще допринесе за иновации по отношение на бизнес процедурите
	Електронен времеви печат Електронно доказателство за съществуването на набор от данни в определен момент	Ще представлява доказателство за закупуване на билети за концерт	Ще подобри проследяването на документи и ще спомогне за по-добра отчетност
	Електронна лична карта (eID) Начин за предприятията и потребителите да доказват самоличността си по електронен път	Ще позволи откриване на банкова сметка в друга държава с национална лична карта	Ще разшири клиентската база, ще спести разходи и време и ще изгради доверие в трансграничните сделки
	Квалифицирано удостоверение за автентичност в интернет Гарантира надеждността на уебсайтовете	Ще потвърждава, че използваните уебсайтове и приложения са надеждни и безопасни	Ще укрепи доверието на потребителите и ще спомогне за избягване на фишинг, като защитава репутацията на предприятието
	Електронен печат Гарантира произхода и целостта на даден документ	Ще гарантира, че билетите за футболен мач са истински, а не фалшификат	Ще намали разходите и сроковете чрез рационализиране на процесите и ще насърчи доверието в произхода на документа
	Услуга за електронна препоръчана поща Защита срещу риск от загуба, кражба, повреда или промени при изпращане на документи	Ще гарантира, че подаръкът за рождения ден на дете пристига без проблеми	Ще намали разходите и сроковете при обмен на документи, ще повиши ефективността и доверието и ще подобри проследяването на документи

ЗАКЛЮЧЕНИЕ

Навлизането на все повече технологии в ежедневието ни предполага и повишаване на количеството и качеството на информацията. Това води до подобрено ѝ използване от хората, свързано с климатичните промени и околната среда, енергийната устойчивост, просперитет и развитие на обществото.

Дигиталната среда предполага и нарастване на киберпрестъпленията и както гражданите, така и институциите са изправени пред предизвикателството да защитят чувствителните данни, сигурността на устройствата и оперативната инфраструктура и не на последно място цифровата идентичност на хората.

ЛИТЕРАТУРА:

Европейска комисия. (2021). *Европейска цифрова самоличност*. Генерална дирекция „Комуникации“. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_bg

Европейска комисия. (2024, април 4). *Регламент относно електронната идентификация и удостоверителните услуги (eIDAS)*. Генерална дирекция „Съобщителни мрежи, съдържание и технологии“. https://digital-strategy.ec.europa.eu/bg/policies/eidas-regulation

Европейският парламент и Съвет на Европейския съюз. (2016). *Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (Текст от значение за ЕИП)*. OB L 119, 4.5.2016, p. 1–88 (BG). https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32016R0679

Личева, Т. (2023). *Модерна сигурност в управлението*. Научно-технически съюз по машиностроене „Индуктрия-4.0.

Личева, Т. (2024). Сигурност на данните. В Сборник от XII Международна научна конференция „Техника. Технологии. Образование. Сигурност” – 2 – 5 сеп. 2024 г., с. 54-56.

Ruiu, P., Saiu, S., & Grosso, E. (2024). Digital Identity in the EU: Promoting eIDAS Solutions Based on Biometrics. *Future Internet*, *16*(7), 228. https://doi.org/10.3390/fi16070228

TechTarget. (2021). *Digital identity strategies to enhance data privacy and protect networks (E-guide)*. ComputerWeekly.com. https://media.bitpipe.com/io_10x/io_102267/item_1306461/E-guide_Identity_Management.pdf