



# Тема 2.6. Управление на дигиталната идентичност

МУЛТИМЕДИЕН ТЕКСТ (ПОМАГАЛО) ТИП ЛЕКЦИЯ (УЧЕБНИК)

## СЪДЪРЖАНИЕ

---

1	Тук ще научите .....	1
1.1	Нови понятия.....	1
2	Дигитална идентичност .....	1
3	Данни, генерирани чрез дигитални инструменти или в дигитални среди.....	2
3.1	Рискове от оставяне на електронни следи .....	2
3.2	Как работят бисквитките (Cookies)? .....	3
4	Защита на репутация в интернет и изграждане на дигитална идентичност в различни среди.....	5



## 1 ТУК ЩЕ НАУЧИТЕ

---

- Какво представлява дигиталната идентичност и как може да я идентифицирате.
- Какви данни генерирате чрез дигитални инструменти или в дигитални среди.
- Как да защитите своята репутация в интернет и как да прилагате добри практики за изграждане на дигитална идентичност в различни среди.

### 1.1 НОВИ ПОНЯТИЯ

Понятие	Описание
Дигитална идентичност	Съвкупност от данни, които представят уникално лице или организация онлайн.
Лични данни	Лична информация, свързана с лице, което може да бъде идентифицирано.
Рискове в интернет	Възможни рискове при ползване на интернет.

## 2 ДИГИТАЛНА ИДЕНТИЧНОСТ

---

Дигиталната идентичност е информация, използвана от компютърните системи за представяне на лице, организация, приложение или устройство. Дигиталните идентичности позволяват да се автоматизира достъпът до услуги, предоставяни с компютри, и правят възможно компютрите да посредничат в отношенията.

Използването на дигитални идентичности днес е широко разпространено. На практика цялата колекция от информация, генерирана от онлайн дейността на дадено лице, се нарича *Дигитална идентичност*. Това включва потребителски имена, пароли, история на търсенето, дата на раждане, история на покупките и др. Когато тази информация е публично достъпна и не е анонимизирана, тя може да бъде използвана от други лица за определени цели. В този по-широк смисъл дигиталната идентичност е аспект на социалната самоличност на дадено лице и се нарича още *Онлайн самоличност*.

Критичен проблем в киберпространството е да се знае с кого се взаимодейства. Използвайки само статични идентификатори като парола и имейл, няма начин да се определи точно самоличността на дадено лице в киберпространството, тъй като тази информация може да бъде открадната или използвана от много лица, действащи като едно. Дигиталната идентичност обаче, базирана на динамични връзки между субектите, уловени от историята на поведението в множество уебсайтове и мобилни приложения, може да провери и удостовери самоличността с точност до 95%.



Чрез сравняване на набор от взаимоотношения между същности между ново събитие (напр. влизане в дадена система) и минали събития, подходящ модел може да провери или удостовери идентичността като легитимна или като опит за маскиране на идентичността. Данните, използвани за дигитална идентичност, обикновено се анонимизират, като по този начин се избягват опасенията за неприкосновеност на личния живот. Тъй като се основава на история на поведението, дигиталната идентичност е много трудна за фалшифициране или кражба.

Цифровата идентичност включва демографска и поведенческа информация, включително проследени онлайн действия.

### 3 ДАННИ, ГЕНЕРИРАНИ ЧРЕЗ ДИГИТАЛНИ ИНСТРУМЕНТИ ИЛИ В ДИГИТАЛНИ СРЕДИ

---

Всеки онлайн субект, включително любимата ви платформа за социални медии и търсачка, се е превърнал в доставчик на идентичност, което означава, че има власт над достъпа и споделянето на вашите онлайн данни. Почти всички онлайн платформи днес използват различни методи за проследяване и масово събиране на данни, за да натрупат склад с потребителски данни, които след това могат да обявят за собствена информация. След това те продават тези данни на рекламодатели, които от своя страна примамват потребителите чрез увзимостите, разкрити от техните онлайн взаимодействия.

#### 3.1 РИСКОВЕ ОТ ОСТАВЯНЕ НА ЕЛЕКТРОННИ СЛЕДИ

*Електронният отпечатък* (или *електронната сянка*) се отнася до уникалния набор от проследими дигитални дейности, действия, приноси и комуникации, които се проявяват в интернет или на дигитални устройства. Електронният отпечатък може да бъде класифициран като пасивен или активен. Първият тип се състои от активността на потребителя при сърфиране в интернет и информацията, съхранявана като бисквитки (от англ.ез. – *cookies*). Вторият тип често се пуска умишлено от потребителя, за да сподели информация в уебсайтове или социални медии. Въпреки че терминът обикновено се отнася за човек, електронен отпечатък може да се отнася и за бизнес, организация или корпорация.

Използването на електронен отпечатък има както положителни, така и отрицателни последици. От една страна, той е предмет на много въпроси, свързани с неприкосновеността на личния живот. Например, без разрешението на дадено лице, непознати лица могат да съберат информация за него само с помощта на търсачките. Корпорациите също така могат да създават персонализирани реклами въз основа на историята на сърфиране. От друга страна, други могат да извлекат ползи, като се възползват от своя електронен отпечатък като влиятелни личности в социалните медии. Освен това работодателите използват електронния отпечатък на кандидата за работа или



служителя като средство за онлайн проверка и оценка на пригодността му поради по-ниските разходи и достъпността му. Между двама равностойни кандидати за работа, този с „положителен“ електронен отпечатък може да има предимство. Тъй като използването на технологиите става все по-широко разпространено, дори децата генерират по-голям електронен отпечатък с потенциални положителни и отрицателни последици, като например при приема в дадено училище. Тъй като е трудно да нямаш електронен отпечатък, в най-добър интерес е да създадеш положителен такъв.

### 3.2 КАК РАБОТЯТ БИСКВИТКИТЕ (COOKIES)?

Бисквитките са текстови файлове с малки части от данни – като потребителско име и парола – които се използват за идентифициране на компютъра ви при използване на компютърна мрежа. Специфични бисквитки, известни като HTTP бисквитки, се използват за идентифициране на конкретни потребители и за подобряване на вашето сърфиране в уеб.

Данните, съхранявани в бисквитка, се създават от сървъра при свързването ви. Тези данни са обозначени с идентификатор, който е уникален за вас и вашия компютър.

Когато бисквитката се обменя между вашия компютър и мрежовия сървър, сървърът прочита идентификатора и знае каква информация да ви предостави конкретно.

С някои вариации бисквитките в дигиталния свят биват два вида: *сесийни* и *постоянни*.

Сесийните бисквитки се използват само по време на навигация в даден уебсайт. Те се съхраняват в паметта с произволен достъп и никога не се записват на твърдия диск. Когато сесията приключи, сесийните бисквитки се изтриват автоматично. Те също така помагат за работата на бутона *Back (назад)* в браузера ви или приставките за анонимизиране. Тези *плъгини* (от англ. ез. – *добавки*) са предназначени за работа на конкретни браузъри и помагат за запазване на поверителността на потребителя.

Постоянните бисквитки остават на компютъра за неопределено време, въпреки че много от тях включват дата на изтичане и се изтриват автоматично при достигане на тази дата.

Постоянните бисквитки се използват за две основни цели:

- 1) *Удостоверяване*. Тези бисквитки проследяват дали даден потребител е влязъл в системата и под какво име. Те също така рационализират информацията за влизане, така че на потребителите да не се налага да помнят паролите на сайта.
- 2) *Проследяване*. Тези бисквитки проследяват многократните посещения на един и същ сайт във времето. Онлайн търговците използват бисквитки за проследяване на посещенията на определени потребители, включително разглежданите страници и продукти. Получената информация им позволява да предлагат други продукти, които биха могли да заинтересуват посетителите.



Постепенно се изгражда профил въз основа на историята на сърфиране на даден потребител в този сайт.

Бисквитките могат да бъдат незадължителна част от работата ви в интернет. Ако желаете, можете да ограничите броя на бисквитките, които се намират на вашия компютър или мобилно устройство.



Ако разрешите бисквитките, това ще рационализира сърфирането ви. За някои потребители липсата на риск за сигурността на бисквитките е по-важна от удобното използване на интернет.

Премахването на бисквитките може да ви помогне да намалите рисковете от нарушаване на поверителността. То може също така да предотврати проследяването и персонализирането на браузъра ви.

Различните интернет браузери имат различни настройки за включване или изключване на бисквитките, които сами по себе си се различават и за устройствата, от които се ползва съответния браузър.

За да включите или изключите бисквитките в браузъра Chrome, когато става дума за мобилно устройство с операционна система Android, отворете приложението Chrome, после в горния десен ъгъл от трите точки изберете *Settings* (*Настройки*), после *Site settings* (*Настройки за сайтове*), след това *Cookies* (*Бисквитки*) и срещу надписа *Allow cookies* (*Разреша бисквитките*) изберете *On* за пускане или *Off* – за спиране (Фиг. 1).

### In the Chrome app

1. On your Android phone or tablet, open the Chrome app .
2. At the top right, tap More  > **Settings**.
3. Tap **Site settings** > **Cookies**.
4. Turn **Allow cookies** on or off.

Фигура 1: Настройки на браузъра Chrome за мобилно устройство за позволяване или спиране на бисквитките.

Сравнително сходни са стъпките и при Chrome за компютър: отворете браузъра Chrome, в горния десен ъгъл от трите точки изберете *Settings* (*Настройки*), след това вляво щракнете на *Privacy and security* (*Поверителност и сигурност*). По средата малко по-долу ще откриете *Cookies and other site data* (*Бисквитки и други данни от сайтове*). Щракнете там, след това ще видите опциите за позволяване на бисквитките (*Allow all cookies*) или блокирането им (*Block*, Фиг. 2).



### In Chrome

1. On your computer, open Chrome.
2. At the top right, click More  $\text{⋮}$  > **Settings**.
3. Under "Privacy and security," click **Site settings**.
4. Click **Cookies and site data**.
5. From here, you can:
  - Turn on cookies: Next to "Blocked," turn on the switch.
  - Turn off cookies: Turn off **Allow all cookies**.

Фигура 2: Настройки на браузъра Chrome за компютър за позволяване или спиране на бисквитките.

## 4 ЗАЩИТА НА РЕПУТАЦИЯ В ИНТЕРНЕТ И ИЗГРАЖДАНЕ НА ДИГИТАЛНА ИДЕНТИЧНОСТ В РАЗЛИЧНИ СРЕДИ

Ако възнамерявате да наемете някого, да отидете на среща с него или дори просто искате да разберете повече за него, вероятно първата ви стъпка ще бъде да го потърсите в Google. Ето защо е толкова важно да поемем контрола върху онлайн репутацията си: тя се отразява вече в почти всеки аспект на живота ни – от наемането на работа до получаването на потенциален договор, но и в личния ни живот.

Ето някои съвети за това как да създадем положителна онлайн репутация и да се справим с проблематичните резултати в Google.

- 1) *Създавайте съдържание.* Създаването на съдържание е чудесен начин за изграждане на лична марка онлайн. Например, ако сте сладкар и искате да се рекламирате като най-добрия сладкар, можете да направите свой блог, в който да обясните как правите най-добрия шоколадов кроасан, а след това да сложите описание стъпка по стъпка и видеоклипове, в които да покажете на хората как да го приготвят. Това е чудесен начин да покажете, че сте експерт. Вие сте добри в това, което правите. Също така може да направите и публикации в социалните медии по темата – още един начин да споделите публично експертните си познания.
- 2) *Осъзнайте, че това е дългосрочен проект.* Няма бърз начин за изграждане на отлична онлайн репутация. Трябва да го правите (публикации в блог или споделяне на мисли онлайн) последователно в продължение на шест месеца до една година, преди хората да започнат да забелязват, че сте навсякъде, че имате добро влияние и че помагате на другите.
- 3) *Не се притеснявайте за резултати в търсачките.* Търсачките днес са усъвършенствани и знаят кое съдържание трябва да бъде по-добре видимо. Това, върху което трябва да се съсредоточите, е просто да пишете страхотно съдържание. Не се притеснявайте за ключовите думи. Това,



което наистина е от съществено значение, обаче, е използването на социалните медии за разпространение на информацията. След като създадете дадено дигитално съдържание (текстове, снимки, видео), трябва да се съсредоточите върху получаването на споделяния в социалните мрежи. Независимо дали ще го поставите в профила си във Facebook, Instagram или Twitter, помолете приятелите си да го популяризират, други хора от бранша ви също. По този начин ще получите повече посетители на страницата, ако съдържанието е добро. Повече от тези посетители действително ще поставят връзки към статията ви и на своите профили и това ще доведе до по-високо класиране на съдържанието ви в търсачките.

- 4) *Малко ежедневно присъствие в социалните медии предпазва от лоши резултати в търсачките.* Какво ще стане, ако се появи отрицателен резултат, когато някой напише името ви в Google? В повечето случаи не можете да поискате премахване на резултата от търсачките. Трябва да ги изтласкате надолу с други, по-добри резултати. (Европейските закони за „правото да бъдеш забравен“ все пак позволяват някои резултати да бъдат премахнати от търсачките, но не и от интернет.) Изграждането на силна онлайн репутация може да изглежда като херкулесова задача, но малките усилия всеки ден наистина се натрупват. Ако има негативна информация, трябва да участвате във всички социални сайтове. Така това последователно съдържание ще се появява при търсене на името ви и ще ви помогне да се предпазите от негативно съдържание, което може да е вече налично или да се появи в бъдеще.

Всеки, с малко време и усилия, може да създаде солидно онлайн присъствие и добра репутация. Но въпреки важността на този въпрос, мнозина не си правят труда. Големият проблем, който се среща при повечето хора, е, че те просто са твърде мързеливи, за да положат усилия в създаването на добра онлайн репутация. Но ако вие сте изключение, това е вашето конкурентно предимство.