The Dark Patterns for the User Interface

Chief Assist. Prof. Dr. Mariya Armyanova
University of Economics - Varna, Varna, Bulgaria
armianova@ue-varna.bg

Abstract

The theory of interaction with user aims to understand the user needs and to develop an interface that optimizes the users work. But some developers use this knowledge to design interfaces that make people inadvertently agree to share more data than they intend, or spend more money than planned, by using various psychological motives and outright deception. These approaches in interface development are defined as dark patterns. They are found in websites, social media platforms, mobile applications and games. The theme remains relevant regardless of the EU's GDPR. The purpose of the report is to identify and detect commonly used dark patterns. The main dark patterns groups and the problems they cause are studied.

Keywords: Dark patterns, User Interface, GDPR, Design patterns

JEL Code: C88

Introduction

Шаблони в разработването на софтуер започват да се използват широко след публикациите на GoF[1]. Целта на шаблоните е да подпомогнат разработката, като представят доказани решения, които са утвърдили своята полезност в практиката. Но има една особена група шаблони, насочени към внасяне на печеливши практики в интерфейса. Те са под английския термин "Dark Pattern", т.е. тъмни или подмолни шаблони. За разлика от анти-шаблоните, с които се означават порочни практики, чието използване води до създаване на некачествен софтуер. Терминът анти-шаблон се използва за означаване на повтарящо се решение на даден софтуерен проблем, което е неефективно, крие рискове и понякога задълбочава проблема. За разлика от тях тъмните шаблони се разработват и използват умишлено. Целта им е да се подведе крайният потребител. Те са интерфейсни шаблони, които са от полза за онлайн услугата, която ги прилага, но те принуждават, заблуждават или объркват потребителите да вземат решения, които те не биха взели, ако са напълно информиране и имат алтернативи (Brignull, 2018). Тъмните шаблони дразнят и разочароват потребителите, но могат да заблуждават и мамят потребителите, като им причинят и финансови загуби, нарушат неприкосновеността на личните им данни или предизвикат пристрастяващо поведение. При създаването им участват, както софтуерни дизайнери, така и специалисти по психология и поведенчески реакции. Прилагането на шаблоните умишлено предизвиква ползвателите на софтуера да извършат определени действия, често противоречащи на интересите им. Те са често срещана техника в областта на електронната търговия, мобилните приложения, социалните мрежи, медии и игрите.

Тъй като използването им е в противоречие с интересите на потребителите и често в противоречие и с правилата, стандартите и законите, те са постоянен обект на изследване в литературата. От друга страна разработчиците непрекъснато се състезават със законодателите, за да продължат да прилагат практиките, които им носят полза. Проучени са групите шаблони, възможностите да бъдат разпознати, последиците от използването им и начините да им се противодейства. Използваната методология е проучване и систематичен анализ на литературата, като и изследване на популярни сайтове. Изследвани са публикации

[1] GOF (Gang of Four) включва Гама, Хелм, Джонсън и Влисидес (Gamma et al., 2004)

в Scopus и Google Scholar. Статиите са анализирани в контекста на изследването.

1. Психологически ефекти, използвани за манипулации от тъмните шаблони

Измамата, която лежи в основата на тъмните шаблони, може да се разглежда, като общочовешко поведение. Хората редовно прибягват до нея, за да извличат лична изгода. Измамата и психологическата манипулация присъстват във всички форми на търговията. В условията на глобална мрежа тъмните шаблони се използват за извличане на печалба. Срещу прилагането им има етични и понякога дори законови съображения. Тъмните шаблони разчитат на когнитивните страсти на потребителите. Всяка група тъмни шаблони използва определени предубеждения на потребителите за манипулации. Основни групи използвани психологически ефекти в търговията са:

- Ефект на закотвяне (Anchoring Effect) – Той се свързва със склонността на хората да разчитат на първоначално събраната информация, която може и да не е актуална в момента на вземане на решение, но е котвата, която ги задържа при избора им (Tversky et al., 1974).
- Групов ефект (Bandwagon Effect) Това е склонността на хората да придават по-голяма стойност на продукт или услуга, защото е желана от голяма група хора (Sherif, 1936).
- Ефект на предубеждение към недостига (Scarcity Bias 64) Това е тенденцията на хората да предават по-голяма стойност на продукт или услуга, ако са оскъдни или придобиването им е съпроводено с трудности (Mittone et al., 2009).
- Ефект на подразбиране (Default Effect) Той се представя със склонността на хората да се придържат към предложените им опции за избор по подразбиране, поради инерция или мързел (Johnson et al., 2002).
- Ефект на рамкиране (Framing Effect) Склонността на хората да интерпретират по различен начин една и съща информация според начина на представянето ѝ и следователно да вземат различни решение при едни и същи данни (Tversky et al., 1981).
- Заблуда за непоносимите разходи (Sunk Cost Fallacy) Склонността на хората да продължават действие, ако са инвестирали ресурси (пари или време) в него, дори ако това не е най-печелившата стратегия (Arkes et al. 1999).

Тези ефекти се откриват в различни групи шаблони. Понякога даден шаблон може да съчетае няколко ефекта за засилване на влиянието си. Независимо от голямото многообразие на шаблоните, познаването на използваните в тях техники за влияние, може да помогне за по-лесното им разпознаване и избягване.

2. Основни групи шаблони, според особеностите им

Тъмните шаблони са постоянен обект на изследване, заради негативните последици, които нанасят на широк кръг потребителите. Използването на съвременните компютърни технологии, като компютърните мрежи и изкуствен интелект, позволява на онлайн търговията, социалните мрежи и мобилните приложения да имат изключително голяма аудитория, върху която да оказват влияние. Проблемът е глобален, защото почти няма потребител на съвременните технологии, които да не е бил подведен от някоя разновидност на тъмните шаблони. Тъмните шаблони са изследвани в много трудове, които са в основата и на въвеждането на някои законодателни промени. От друга страна създателите на тъмните шаблони непрекъснато се състезават с изследователите и законодателите, за да запазят влиянието си над потребителите. Запознаването на потребителите с използваните техники в тъмните шаблони спомага за пораждане на недоверие и загуба на ефективност на известните тъмни шаблони. Но разработчиците на тъмни шаблони продължават да измислят нови разновидности, с които все още не са се сблъсквали потребителите. Затова само откриването на тъмните шаблони не е достатъчно, за да се намали влиянието им. Необходимо е откриването на общите им механизми за влияние. Изследователите групират, класифицират и обобщават известните тъмни шаблони. Има няколко класификации на тъмните шаблони:

според областта, в която оказват влияние, например електронна търговия, социални медии, мрежи и компютърни игри; или пък според особеностите им; или според вида на щетите, които нанасят. Класификацията на шаблоните според особеностите им позволява лесно да се открият подобни черти в интерфейса, които го определят като манипулативен.

Основните характеристики на тъмните шаблони са определени, в два доклада (Mathur et al., 2019; 2021). Откриването на подобни особености спомага за класифициране на използваните елементи на интерфейса като тъмен шаблон. Най-общо тъмните шаблони могат да се разделят в две големи групи – шаблони, които предрешават избора на потребителя и шаблони, които манипулират информацията. Особеностите на тъмните шаблони са асиметричност, скритост, измама, скриване на информация, ограничаване и различно отношение (Table 1).

Table 1. Особености на тъмните шаблони

Групи	Особеност	Описание
Шаблони, предрешаващи избора на потребителя	асиметричност	Неравномерно акцентиране върху опциите за избор, достъпни за потребителите
	скритост	Скриване на механизма за влияние на потребителите
	ограничаване	Премахване на определени възможности за избор, които трябва да бъдат достъпни за потребителите
	различно отношение	Третиране на определена група потребители различно
Шаблони, манипулиращи информацията	скриване на информация	Неясно или забавено представяне на нужната информация за потребителите
	Измама	Създаване на фалшива представа чрез потвърждаване на грешни или подвеждащи твърдение или пропускане на други

Асиметричните тъмни шаблони предлагат несиметрични възможности за избор на потребителя. Опциите за избор, които са в полза на търговеца са представени на видно място, докато тези от полза за клиента са скрити. За да достигне до тях потребителят трябва да прави няколко допълнителни щраквания или те не са толкова добре видими, заради използвания стил и място на разполагане. Например бутон за съгласие може да е откроен като изпъкнал, а бутон за отказ да е почти неразличим. Често настройки, които позволяват на потребителя да съхрани поверителността на действията и данните си са скрити зад неясни менюта. Този тип шаблони се използват, когато е нужно потвърждение и съгласие на клиента. Например шаблон (Trick Questions) предизвиква съгласие на потребителя чрез използване на трикове в естествения език, като двойно отрицание и използване на объркващи изрази. Друг тъмен шаблон (Confirmshaming) използва емоциите, за да предреши избора, например като свърже чувството за вина с определени опции.

Тъмните шаблони, които се се характеризират със **скритост**, подтикват потребителя към определени решения, като скриват механизмите за влиянието му. Манипулациите могат да се базират на когнитивни пристрастия или да са чисто интерфейсни чрез цвят и стил. Потребителят може да бъде погрешно насочен чрез скрити елементи. Например към пазарската количка в сайт за търговия се добавя ненужен безплатен подарък, като абонамент за списание, и така да се увеличи размера на отстъпката. За клиента остава скрит начинът, по който е получена видимата отстъпка. Подобни шаблони използват ефекта на примамката, за да направят по привлекателен избора и така да повлияят на решенията на клиентите.

Тъмните шаблони, които използват **измами**, предизвикват фалшиви вярвания в потребителите чрез потвърждаване на грешни или афиширане на подвеждащи твърдение, или допускане на пропуски. Те се използват най-често в сайтове за търговия. Такъв е

шаблонът Таймер за обратно броене (Countdown Timer), който включва фалшив краен срок за офертата. Обаче над 40% от всички използвани таймери се нулират при опресняване на страницата или след изтичане на срока, или изобщо не са свързани с рекламираната оферта (Mathur et al., 2019). Това притиска потребителя да вземе импулсивно решение.

Тъмните шаблони, които **скриват информация**, не представят явно или забавят представянето на необходимата информация на потребителите. Такъв е шаблонът Скриване (Sneaking). Например сайт може да скрива допълнителните такси, които се налагат на потребителя, до изплащането им. Или пък да скрива абониране за услуга, като подвежда потребителите, че правят еднократно плащане. Понякога потребителят може да не забележи допълнителните разходи, но дори и когато малко преди транзакцията е уведомен, вече е малко вероятно да се откаже от покупката.

Тъмните шаблони, които налагат **ограничение**, се стремят да премахнат или намалят възможностите за избор на потребителите. Например сайт може да изисква от потребителите да се регистрират с акаунтите си в социалните мрежи, за да събира лесно и повече информация за тях. Например шаблонът Принудително действие (Forced Action) изисква от потребителите едновременно да се съгласят не само с условията на използване на сайта, но и с получаването на маркетингови имейли. Шаблонът Трудна отмяна (Hard to Cancel) улеснява потребителите да се регистрират за определена услуга, но не представя на потребителите онлайн опция да анулират услугата.

Някои тъмни шаблони поставят в неизгодно положение или третират определена група потребители по **различен начин**. Те най-често се използват в игрите (Zagal et al., 2013). Такъв е тъмният шаблон Плати, за да избегнеш (Pay to Skip). Той позволява на потребителите с повече ресурси да получат предимство пред потребителите, които не могат да си позволят да плащат. Някои шаблони работят без да са предварително обявени и потребителите могат да не разберат причината за предоставения им ограничен набор от възможности (Hannak et al., 2014).

3. Основни групи шаблони, според щетите, които нанасят

Тъмните шаблони нанасят щети на потребителите в няколко направления: намаляват индивидуалното благосъстояние, колективното благосъстояние, подкопават индивидуалната автономия и противоречат на регулативните политики (Mathur et al., 2021).

Един от факторите шаблоните да се определят като тъмни е, че прилагането им намалява индивидуалното благосъстояние на потребителите. Аспектите на **индивидуалното благосъстояние** са различни финансови, материални или емоционални. Тъмните шаблони вредят на потребителя, нарушават интересите му или му създават отрицателно изживяване. Затова аспектите на тъмните шаблони са финансови, нарушаване на поверителността, изразходване на време, енергия и внимание.

Една от очевидните последици от тъмните шаблони е *финансова загуба*. Това е характерно за сайтовете за търговия, екскурзии или пътувания, които целят да убедят потребителя да похарчи повече от първоначално планираната сума. Такива са шаблоните Промъкване в пазарната кошница (Sneak into Basket), Скрит абонамент (Hidden Subscription) и Прикрити реклами (Disguised Ads). Те печелят като добавят продукти към пазарската количка на потребителите без тяхно съгласие или ги подвеждат да се регистрират за еднократна оферта или безплатен пробен период, докато всъщност потребителите се регистрират със скрит абонамент да плащат периодични такси. По подобен начин действат и скритите реклами, като убеждават потребителите да закупят продукти, които иначе не представляват интерес за тях.

Друга последица за благосъстоянието на потребителите *е нарушаването на поверителността на данните им* чрез тъмен шаблон. Потребителите се подвеждат да изберат опция за уведомяване, която намалява поверителността на данните им (Gray, 2018).

Примери са шаблоните Лоши настройки (Bad Defaults), шаблонът на Цукеринг (Privacy Zuckering), Смущения в интерфейса (Interface Interference), Обструкция (Obstruction), Обвиняване на индивида (Blaming the Individual), Пораждане на срам (Confirmshaming), Поставяне на рамки (Framing). При такива тъмни шаблони на потребителите са предложени по подразбиране настройки, които разкриват потребителските данни или изборът на други настройки е скрит чрез труден достъп. Някои шаблони използват човешките емоции – страх, вина, срам, за да отблъснат потребителите от вземане на решения, зачитащи поверителността.

Тъмните шаблони, които нарушават *неприкосновеността на личните данни*, са най-обсъждания тип в литературата. Срещу тях се приемат и законови мерки. Обаче част от шаблоните успяват да заобиколят правилата, като изискват регистрация и избор на определени опции, които са на границата на законните за поверителност (Waldman, 2020). Някои шаблони събират лична информация за клиентите, която се продава на трети лица. Темата за поверителността остава дискусионна, заради различни бизнес интереси. Някои възгледи представят личната информация като обществено благо, други като човешко право или като аспект на индивидуална автономия.

Друга последица за благосъстоянието е свързана с излишно *изразходване на време, енергия и внимание*. Потребителите избират най-лесния за реализация избор, за да си спестят излишните усилия, заложени от дизайнерите. Примерни шаблони са Трудно отменяне (Hard to Cancel), Заяждане (Nagging), Скрити правни условия (Hidden Legalese Stipulations). Такива интерфейси възпрепятстват потребителите да отменят абонаменти, чрез обаждане в определени часове, несъответствия между упътванията на различни отдели, страници и служители. Други многократно подтикват потребителите към определени действия с изпращане на съобщения, позвънявания, реклами или скриват законово изисквана уведомяваща информация. Има тъмни шаблони, които не се преследват от закона, като диалоговите прозорци за съгласие с бисквитки без опция за отказ или с усложнено достигане до такава. Трудностите при определяне на този тип тъмни шаблони се състои в липсата на стандарт за определяне на благосъстоянието на потребителите. Индивидуалните желания и предпочитания са трудни за измерване, защото са динамични и варират при различните индивиди. Маркетингът по своята същност се базира на оформяне на предпочитанията на потребителите и е трудно да се различат доброкачествените и поносими начини за влияние от тъмните шаблони. Прието е, че при свободните пазари потребителите наказват недобросъвестните практики, като ги изоставят или сриват репутацията им. Не се отчитат и разходите за прилагане на различни видове маркетингови практики.

Друга група шаблони засягат **колективното благосъстояние**. За разлика от индивидуалното благосъстояние, изследванията върху колективното благосъстояние са ограничени. То е свързано с обществото и свободните пазари. Основно тъмните шаблони влияят върху конкуренцията, прозрачността на цените, доверието в пазара и имат неочаквани обществени последици.

Част от тъмните шаблони позволяват на доминиращите фирми да злоупотребят с властта си и *да елиминират конкуренцията*, като представят избора на потребителите, като самостоятелно взето решение, а не като резултат от тъмни шаблони, които вредят на конкурентите. Такива са шаблоните Предварителен подбор (Preselection), Поставяне на рамки (Framing). Те представят на потребителите форма с избрани по подразбиране опции за отметка или използват емоции и страх, които да насочат избора. Те позволяват да се обвържат несвързани продукти и така да пласират и продукт с неголям пазарен дял. Тъмните шаблони особено от групата на ограниченията препятстват възможностите на потребителите да използват продукти на конкурентите и създадат бариери пред навлизането на конкуренти. Използването на тъмните шаблони позволява на платформите да ограничава възможностите на потребителите да действат рационално, което им позволява да изграждат пазарна сила и

да трупат богатство, нарушавайки пазарните принципи (Day et al., 2020). Когато шаблонът е предназначен да генерира разходи за превключване, които не могат да се компенсират от конкурентите, това изкривява пазара. Шаблоните от групата целят да се засили пристрастяването, като същевременно се предоставя на потребителите по-некачествен продукт.

Прозрачността на цените позволява на потребителите да вземат информирани решения и по този начин се създава ефективен пазар. Конкуренцията по отношение на цените не винаги е изгодна и тъмните шаблони прикриват истинската цена на продуктите от потребителите, като използват различни наименования за един и същ продукт. Такива са шаблоните Скрити цени (Hidden Costs) и Предотвратяване на сравнението на цените (Price Comparison Prevention). Липсата на прозрачно ценообразуване причинява потенциални финансови загуби на потребителите, които биха могли да изберат по-ниска ценова оферта, но също така и намалява конкуренцията на пазара. Често конкурентите престават да разкриват непрозрачните цени на конкурентите си, а им е по-изгодно да копират и използват същите шаблони, които изкривяват пазара.

Тъмните шаблони могат да *подкопаят доверието на потребителите* в пазара и да навредят на компаниите, които се придържат към принципите на честната конкуренция. Потребителите започват да разпознават тъмните шаблони и елементи на интерфейса, които напомнят на тях се възприемат скептично от потребителите. Например потребителите разпознават шаблона Недостиг (Scarcity). Скептицизмът, който потребителите изпитват при подобни оферти, може да навреди на търговци на дребно, които предлагат ограничени бройки. Потребителите, подведени от сайт с тъмен шаблон, са склонни да съобщят за отрицателното си изживяване и така да накажат недобросъвестните практики. Въпреки, че се предполага, че тъмните шаблони в крайна сметка са самоунищожителни, не винаги страда само бизнесът, прилагащ нечестни практики.

Прилагането на тъмен шаблон понякога има *непредвидени последици* от разработчика. Например социалните мрежи натрупват огромни бази с лични данни, които могат да се използват за целите на рекламата. Но информацията може да се използва и за влияние върху обществените ценности, за политически кампании и др.

Тъмните шаблони, които влияят върху общественото благосъстояние не винаги влияят на индивидуалното благосъстояние, но могат да повлияят непряко върху други потребители. Типичен пример са приложенията за игри, които позволяват на участниците да изпращат спам на приятелите си и да ги подтикват да се регистрират. Трудно е да се открият и съпоставят всички ползи и вреди, още повече, че за някои групи последиците са косвени. И отново темата е дискусионна – интерфейсът трябва да е добър за максимален брой хора или пък трябва да защитава по-уязвимите групи в обществото.

Голяма част от тъмните шаблони се опитват да подкопаят **индивидуалната автономия**. Под индивидуална автономия се разбира правото на индивида сам да взема информиране решения, в съответствие със собствените си цели и принципи, като не е задължително целите му да са финансова ефективност. Но всеки опит да се скрие информация или да се намалят опциите за избор подкопава индивидуалната автономия. Такива са и шаблоните, които допускат пристрастяване. Онлайн услугите имат стимули за максимално ангажиране на потребителите с платформата си, което противоречи на автономията на потребителите. Тъмните шаблони, които водят до пристрастяване, имат редица негативни последици, както психологически, така и физически. Те могат да водят до разсейване, нарушаване на съня и т.н. Много от онлайн услугите са създали техники в съответствие с подходи, използвани от хазартната индустрия (Schüll, 2014). Например Кутии с плячка (Lootboxes), които дават предимства на потребителите пред другите във видеоигрите и така ангажират непрекъснато потребителите си. Проблемът с автономията е в трудността да се определи, кога нарушаването ѝ носи ползи за индивида и обществото. Освен това тя трудно се реализира в реалния живот, при наличието на ограничена информация за вземане

на решения. Трудно е да се разграничи и допустимата реклама от тъмния шаблон, тъй като и двете могат да доведат до промяна в поведението на потребителя. Няма начин да се измери и степента на нарушаване на автономията от потребителския интерфейс.

Регулаторните политики използват правила и стандарти, за да установят индивидуални или колективни щети, които намаляват финансовото благосъстояние на индивидите и подкопават пазарните принципи. Според този регламент за тъмен шаблон се определя всеки интерфейс, който променя възможностите за избор, за да пречи или ограничи дефинираните правила и стандарти. Например шаблони, които пропускат съществена информация или представят невярна информация, противоречат на законите за защита на потребителите. Обаче регулаторните органи нямат единен стандарт и решават за всеки случай по отделно. Приемат се закони за регулиране на некоректни практики такъв е новият Общ регламент за защита на личните данни (General Data Protection Regulation GDPR). Той е в сила от 25 май 2018 г. във всички страни, които са членки на Европейския съюз (ЕС) и е за регулиране на поверителността. В ЕС властите са склонни да приемат закони и наредби, дефиниращи допустимо и непозволено поведение, докато регулаторните органи на САЩ се придържат към подход, основан на принципи (Soe et al., 2020).

Въпреки приетият регламент от ЕС GDPR, все още се използват шаблони, които намаляват сигурността. Независимо, че събирането на лични данни, цифрови самоличности и съответните им идентификатори е риск, те продължават да се събират от редица услуги. Доставчиците на услуги продължават да не приемат псевдонимен или анонимен достъп. Именно проблемът с осигуряването на сигурността и неприкосновеността на личния живот е един от най-сериозните в условията на глобална мрежа. Той е обект на специално разглеждане по отношение на заобикаляне и дори нарушаване на регламентите и етичните норми.

4. Използвани тъмни стратегии, които подкопават сигурността

В основата на приетите в GDPR ограничения стоят принципите, предложени от Хофман (Hoepman, 2014). Той предлага осем стратегии, които да гарантират сигурността на данните. Това са Минимизиране, Скриване, Разделяне, Обобщаване, Информиране, Контролиране, Изискване и Демонстриране. От друга страна (Bösch et al, 2016) тъмните шаблони съпоставят свои стратегии, които са точни обратните: Максимизиране, Публикуване, Централизиране, Запазване, Неяснота, Отказ, Нарушаване и Фалшифициране (fig. 1). Наличието на подобна стратегия позволява лесно да се идентифицира тъмен шаблон, нарушаващ сигурността.

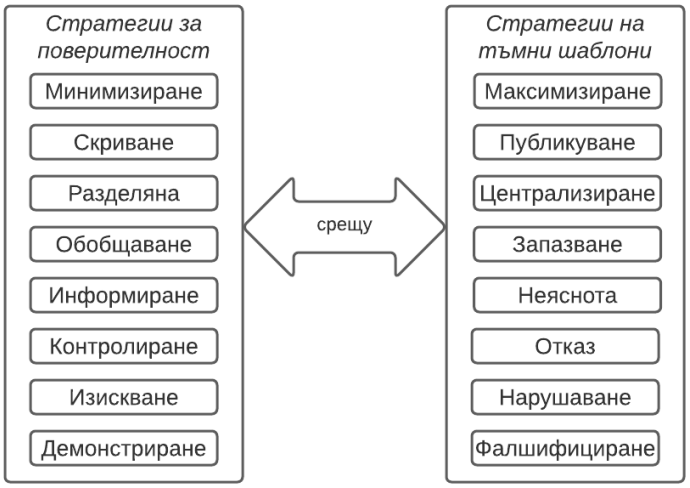

Figure 1. Стратегиите за сигурност и противоположните им в тъмните шаблони.
(Bösch et al, 2016)

Минимизирането изисква свеждане до минимум на използването на лични данни. Данни, които не са изрично необходими не трябва да се събират. Стратегията на максимизирането е противоположна. При нея се съхраняват и обработват възможно най-много данни, което често води до загуба на поверителност. Стратегията обикновено не е преднамерено злонамерена, а цели да извлече конкурентно предимство. С допълнителна лична информация може да се изпратят подходящи персонални реклами. Често събирането, обработването и използването на данните е възложено изцяло на изкуствен интелект с неизяснен докрай алгоритъм. Такива шаблони изискват попълването на обширни формуляри, които не са необходими за функционирането на услугата, при това със задължителни полета. Тъмни шаблони са изискванията за създаване на акаунт за използване на услугата или задължителното избиране на по-слаби настройки за сигурност, за да може да се използва услугата.

Скриването предполага защитаване на личните данни, като те не са обвързани и са добре защитени от възможността да станат публично достояние. То започва след събирането на данните, което следва да е минимално. Необходимо е отговорно боравене с личните данни. При работата с тях разработчиците следва да се придържат към стандарти и процедури. Противоположната стратегия за публикуване всъщност означава, че обикновено не се използва или се използва слаб механизъм за скриване на личните данни от неоторизиран достъп. Политиките за криптиране или контрол на достъпа са неадекватни. В социалните мрежи тази стратегия е особено важна, като личните данни са достъпни за всички. В тях се насърчава споделянето на лични неща, което удовлетворява психологическата нужда на човек да принадлежи и повишава използването на платформата.

Разделянето предполага отделяне на обработката на личните данни от останалите обработки. Всички лична данни се обработват поотделно и така се намаляват взаимовръзките между тях, за разлика от централизираната обработка. Централизирането е стратегия на тъмните шаблони. При нея личните данни се събират, съхраняват и обработват централизирано. Запазват се връзките между различните потребителски данни, за да се позволи изследване в дълбочина на навиците и използването на услугата. За целите на рекламите при синхронизиране на бисквитките се споделят псевдоними на потребителските идентификатори. Друга тъмна стратегия са флаш бисквитките, които се съхраняват централно във файловата система на приложението и не са ограничени до конкретен браузър.

Обобщаването се състои в ограничаването на детайлите по обработването на личните данни. Нивото на обобщаване трябва да е максимално високо, така че да се скрият максимално личните данни. Например статистическа обработка, която да премахне детайлите за самоличността. При тъмната стратегия за запазване взаимовръзките между различните елементи от данни не трябва да се изгубят при обработката. Данните се съхраняват в първоначалната си форма за подробен анализ, който често не е предварително известен. Типичен пример са съхранените данни в телекомуникационните компании, по които може да възстанови трафика между потребителите.

Информирането е стандарт, който предполага, че при всяка обработка на лични данни, субектите трябва да бъдат информирани своевременно и адекватно. Стратегията за неяснота ограничава възможностите на субектите да открият начините за събиране, съхраняване и обработване на личните им данни. Постига се под формата на политики за поверителност, използващи сложна техническа и правна терминология. За реализацията на неяснотата активно се използват интерфейси, които заблуждават и объркват потребителя.

На субектите трябва да се предоставят адекватни възможности за контрол върху обработката на личните им данни. Обаче Хофман (Hoerman, 2014) заявява, че не познава услуги, които да прилагат тази стратегия. Стратегията за отказ се състои в манипулирането на потребителя така, че той да загуби контрола върху личните си данни. Така потребителите не могат да предприемат действия, които противоречат на интересите на доставчика на услуги. Например липсата на възможност да се изтрие акаунт или липсата на опции за контрол върху

споделянето на информация.

Поверителност изисква да има приета политика за сигурност, която да се прилага и да се носи съответната отговорност. Стратегията за нарушаване е използвана в случаите, когато има умишлено нарушаване на политиката за сигурност, т. е. има политика за сигурност, но тя не се спазва. Потребителят няма да узнае за нарушенията и не променя доверието си в услугата, докато нарушенията не се разкрият. Тази стратегия е в противоречие със закона и е трудно доказуема.

Демонстрирането е изискване за осигуряване на възможност за показване, че обработката на личните данни съответства на политиката за сигурност и законовите изисквания, например чрез одити. Стратегията за фалшифициране се състои в имитирането на прилагане на ефективна защита за сигурността. Подобен пример са самостоятелно проектиране на елементи в интерфейса, като икони или печати, които имитират различни сертификати. Те създават фалшиво чувство за сигурност на потребителя. Друг пример са различни маркетингови твърдения за „криптиране от военен клас“ или неправилни твърдения за размера на криптиращия ключ.

Освен използваните в сайтовете за търговия и мобилните приложения шаблони има и няколко специфични типа, нарушаващи поверителността, използвани в социалните медии и игрите. Социалните медии недвусмислено оказват голямо влияние върху всички области на съвременния живот, като променят начина, по който хората общуват, изразяват себе си, споделят, но и социалния и обществен живот. Най-силни и видими промени се наблюдават при младите поколения (Aleksandrova et al, 2019). Именно затова влиянието в тях е особено важно. Една от негативните им черти е възможността за злоупотреба с лични данни (Nacheva, 2013).

Социалните мрежи и медии използват тъмни шаблони, с които нарушават поверителността. Най-често тъмните шаблони са под формата на допълнителна идентификация за сигурност, събиране на незадължителни идентификационни атрибути и задължително мрежово идентифициране (Fritsch, 2017).

Обикновено услугите, които изискват създаване на потребителски акаунти, поддържат ниско ниво на сигурност, за да снижат разходите и да привлекат повече потребители. При възникване на нови бизнес възможности за ползване данните на потребителите, платформите за услуги обогатяват своите бази, като прилагат нови тактики за събиране на повече данни. Те свързват профилите на потребителите с реална самоличност. Често използван е тъмният шаблон Допълнителна идентификация за сигурност (Fogging identification with security). Той се прилага и от Google и от Facebook. Целта му е да придобие допълнителни атрибути за идентификация, замаскирани под формата на повишаване на сигурността на потребителския профил. Потребителят е подведен от обещания за повишаване на сигурността, а услугата попълва информация за допълнително добавени атрибути за идентичност. Това намалява анонимността и псевдо анонимността на потребителите и увеличава възможностите за проследяване, профилиране и наблюдение. Подобно искане от услугите се отправя, когато потребителите са под времеви натиск, при въвеждане или подновяване на пароли, или на друг елемент на профилите или пък при създаване на поръчка. Много популярна мярка за подновяване на паролата е заявка за проверка чрез SMS. Понякога в съответствие със законовите мерки, заявките за допълнителни данни могат да бъдат заобиколени, но те отново се появяват при следващото взаимодействие с услугата. Друг пример е изискване на потвърждение или съгласие за профилиране, базирано на бисквитки с цел повишаване на безопасността. Фейсбук дори отива по-нататък, като прилага и групов натиск, показвайки броят на приятелите, които вече са споделили телефонния си номер. Подобни тъмни шаблони са Принудителна регистрация (Forced registration) и Сенчести потребителски профили (Shadow user profiles).

Друг шаблон е Сладко съблазняване (Sweet seduction). Той съотвества на шаблона на Цукеринг (Privacy Zuckering) и Сенчести потребителски профили (Shadow user profiles). При

събирането на повече от нужните данни за реализирането на услугите, потребителите често са съблазнени от обещанието за несподеляне на данните или от възможността да деактивират използването и споделянето на наскоро въведена информация. Обаче не се споменава, че въведената информация се използва за допълване на потребителския профил и за по целенасочен бизнес, например промяна на социалната графика. По този начин се прехвърля отговорността за управляване на данните върху потребителя. При това за данни, които са напълно излишни от гледна точка на сигурността. Основната контрамярка при такъв тъмен шаблон е отказ за предоставяне на данни или въвеждане на фалшиви. Често Facebook изпраща съобщение за грешка „Error! Reference source not found.“, което цели да принуди потребителят да въведе още данни, за да използва услугите на платформата. А при споделяне на телефонните си номера потребителите са подлъгани от Facebook с модел за отказ от използване.

Един от инструментите за защита на самоличността е чрез използване на технологии за анонимизиране. Има браузъри, като TOR, които позволяват скриване на IP адреса и друга идентифицираща мрежата информация. Потребителските сесии изглежда, че идват от различни изходни възли, които са компютри разположени в различни страни. По този начин се скрива и местоположението – Geo-IP. Обаче част от потребителите на подобни браузъри срещат затруднения в обслужването. При опит да използват услуга, те получават различни съобщения за грешки от „невъзможност за свързване“, или други произволни съобщения, директни лъжи за отказ от услуга и дори директно признаване на отказ от обслужване на анонимни потребители. Сигурността отново е обявена, като оправдание за наложените санкции. Платформите за услуги използват тъмен шаблон Можете да бягате, но не може да се скриете (You can run but you can’t hide). Същността му се състои в отказ от услуга, при скриване на мрежовата идентификация. Най-вече се използва в сайтове за търговия, правителствени сайтове и блогове. Обаче използването на този шаблон е означава, че е отказана услуга на потребителите. За да я получат, те трябва да разкрият IP адреса си, местоположението си, областта си и други данни. В този случай те нямат опция за отказ от разкриване на данните си, освен ако не използват конкретната услуга. Обаче в случая с правителствените услуги, те нямат друга алтернатива. Този шаблон се използва, когато се упражнява власт във връзката.

Въпреки GDPR тъмните шаблони продължават да се прилагат. Често те са замаскирани с преследване на по-високи цели като сигурност. Обаче не се проследява начинът на използване на събраните данни от компаниите под това оправдание. Стои и въпросът за етичността на използваните мерки за събиране на данни от подтикващи техники, разгръщане на натиск върху различни социални групи и дори откровена измама.

Еволюцията на игрите като социална дейност е засегнала света на технологиите и е променила глобалния пазар. Игрите непрекъснато разширяват аудиторията си, като игралните корпорации използват социални канали за популяризиране на своите продукти и привличане на нови клиенти (Bankov, 2019). В **областта на игрите** тъмните шаблони имат негативни последици за индивида в три направления изразходване на време, финанси и влияние на социалния статус (Zagal et al., 2013).

Тъмните шаблоните, които предизвикват изразходване на време отнемат повече време от предвиденото от играчите. Такива са шаблоните Изтощение (Grinding) и Игра в определен час (Playing by Appointment). Шаблонът Изтощение е свързан с изпълнение на повтарящи се и досадни задачи (Nakamura, 2009). Той изисква от играча да инвестира много време, за да напредне в играта, без да може да прояви умението си. Целта му е да удължи продължителността на играта. Разчита на състезателния дух на играчите. Играч достигнал по-високо ниво няма проблем да победи играч от по-ниско ниво, защото играчът е получил привилегии за инвестираното време. Шаблонът води до отрицателно изживяване както в играчите, които са принудени да инвестират много време в играта, така и в играчите, които имат умения, но не и време, за да достигнат определено ниво.

Тъмният шаблон Игра в определен час изисква игра по време, което е определено от играта и не винаги е удобно за играчите. По този начин играчите настройват задълженията си в реалния свят според графика на играта.

Представители на тъмните шаблони за игри, които предизвикват финансови загуби са Плащане за пропускане (Pay to Skip), Предварително доставено съдържание (Pre-Delivered Content) и Плащане за конкурентност (Monetized Rivalries). Целта им е да насърчават играчите да харчат повече пари, отколкото са планирали. Тъмният шаблон Плащане за пропускане не насърчава играча да плати, за да продължи да играе, а позволява на играча да плати, за да преодолее предизвикателството заложено в играта. Например да мине на следващо ниво. Понякога дори преодоляването на определено ниво не е възможно без заплащане. При шаблона Предварително доставено съдържание играчът е платил, за пълно копие на играта, но докато не плати допълнителна такса, няма достъп до всички възможности в нея. Шаблонът Плащане за конкурентност насърчава играчите да плащат, за да постигнат статус в играта, например високо място в класацията. Много често чрез плащане играчите могат и да получат предимство пред уменията на останалите играчи. Например забавяне на темпото на играта или консумативи, които улесняват играта. Победата от играта се тиражира в социалните мрежи или други канали и това подтиква играчите да плащат.

Тъмните шаблони, които влияят върху социалния статус предизвикват играчите да играят, но не заради удоволствието от играта, а за да запазят социалния си статус. Примери за такива шаблони са Схема за социална пирамида (Social Pyramid Schemes) и Превъплъщения (Impersonation).

Пирамидите са незаконна схема. Дори и да не предизвиква финансови облаги, набирането на повече участници, които да носят предимство в играта е вид пирамида. В някои игри липсата на приятели не позволява да се изпълнят определени дейности в играта. Проблемът се корени в социалното задължение, което изпитват приятелите да се присъединят към играта. Шаблонът Превъплъщения се използва от играта, за да подтикне играчите да поканят свои приятели в играта, която имитира действия на приятели и показва ползата от приятелите в играта. Друг вариант на този шаблон е Спам от приятели, при който играта изпраща от името на играча писма или съобщения до приятелите му. Това може да има негативни последици за играча и в реалния живот.

Conclusion

В заключение можем да обобщим, че всички шаблони за проектиране на интерфейс почиват върху едни и същи модели на взаимодействие. Самата идея, интерфейсът да е удобен и лесен за употреба, предполага познаване на психологията и начина на работа на потребителя. Обаче етичният интерфейс изисква тези познания да се използват в полза на потребителя, а не в негов ущърб. При всички видове тъмни шаблони, потребителят е подлъган по някакъв начин да извърши определено действие, което противоречи на интересите му. Използваните психологически тактики и стратегии са едни и същи при всички разновидности на тъмните шаблони. Познаването им помага на потребителя да разпознае шаблоните в интерфейса. Предприетите законодателните инициативи успяват донякъде да защитят потребителя, но проблемът идва с трудното поставяне на граница на влиянието, което има положително въздействие върху обществото като цяло и защитата на индивидуалните интереси и свободи на отделния потребител. Именно от тези несъвършенства на законите продължават да се възползват тъмните шаблони.

References

1. Aleksandrova, Y., Parusheva, S. (2019) Social Media Usage Patterns in Higher Education Institutions – An Empirical Study. *iJET*. Vol. 14 (05). pp.108-121.
2. Arkes, H., Ayton, P. (1999) The sunk cost and Concorde effects: Are humans less rational than lower animals? *Psychological bulletin*. Vol. 125. 5. pp. 591-600.
3. Bankov, B. (2019) The Impact of Social Media on Video Game Communities and the Gaming

Industry. *ICTBE 2019*. Varna. is. 1. pp.198-208.
4. Bösch, C., Erb, B., Kargl, F., Kopp, H., Pfattheicher, S. (2016) Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies*. vol. 2016. no .4. pp.237-254.
5. Brignull, H., (2018) *Dark Patterns*. [Online] Available from: https://darkpatterns.org [Accessed 07/11/2021]
6. Conti, G., and Sobiesk, E. (2010) Malicious Interface Design: Exploiting the User. *In Proceedings of the 19th International Conference on World Wide Web* (Raleigh, North Carolina, USA) (WWW '10). Leeds: Association for Computing Machinery. New York. pp. 271–280.
7. Day, G., Stemler, A. (2020) Are Dark Patterns Anticompetitive? *Alabama Law Review*. Vol. 72. pp. 1–45.
8. Fritsch, L. (2017) Privacy dark patterns in identity management. *Open Identity Summit 2017*. pp. 93-104.
9. Gamma, E., Helm, R., Johnson, R., Vlissides, J. (2004) Design Patterns: *Elements of Reusable ObjectOriented Software.* Addison-Wesley Professional Computing Series.
10. Gray, C., Kou, Y., Battles, B., Hoggatt, J., Toombs, A. (2018) The Dark (Patterns) Side of UX Design. *CHI '18*. ACM. NY. USA. 534. pp. 1-14.
11. Hannak, A., Soeller, G., Lazer, D., Mislove, A., Wilson, C (2014) Measuring Price Discrimination and Steering on E-Commerce Web Sites. *IMC '14*. Association for Computing Machinery. New York. USA. pp. 305–318.
12. Hoepman, J., (2014) Privacy Design Strategies. *ICT Systems Security and Privacy Protection*. Springer. Heidelberg. Berlin. pp. 446–459.
13. Johnson, E., Bellman, S., Lohse, G. (2002) Defaults, Framing and Privacy: Why Opting In-Opting Out 1. *Marketing Letters* vol. 13. 1. pp. 5–15.
14. Mathur, A., Acar, G., Friedman, M., Lucherini , E., Mayer, J., Chetty, M., Narayanan, A., (2019) Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proc. *ACM Hum.-Comput. Interact.* volume 3. CSCW. 81. Nov. 2019.
15. Mathur, A., Mayer, J., Kshirsagar, M., (2021) What Makes a Dark Pattern... Dark? *ACM Conference on Human Factors in Computing Systems*. CHI '21. May 8–13. 2021. Yokohama. Japan.
16. Mittone, L., Savadori, L. (2009) The scarcity bias. Applied Psychology. vol. 58, 3. pp. 453–468.
17. Nacheva, R. (2013) Social networks - a tool for providing a flexible learning process. Scientific Conference of Young Researchers. Varna. pp. 152-158.
18. Nakamura, L., (2009) Don't Hate the Player, Hate the Game: The Racialization of Labor in World of Warcraft. *Critical Studies in Media Communication.* vol. 26. 2. pp. 128-144.
19. Schüll, N. (2014) *Addiction by design: Machine gambling in Las Vegas*. Princeton University Press.
20. Sherif, M. (1936) *The psychology of social norms*. Harper & Brothers. New York and London.
21. Soe, T., Nordberg, O., Guribye, F., Slavkovik, M. (2020) Circumvention by Design – Dark Patterns in Cookie Consent for Online News Outlets. *NordiCHI '20*. Association for Computing Machinery. NY. USA.
22. Tversky, A., Kahneman, D. (1974) Judgment under uncertainty: Heuristics and biases. Science vol. 185. 4157. pp. 1124–1131.
23. Tversky, A., Kahneman, D. (1981) The framing of decisions and the psychology of choice. *Science* vol. 211, 4481. pp. 453–458.
24. Waldman, A. (2020) Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology* vol. 31. pp. 105–109.
25. Zagal, J., Björk, S., Lewis, C. (2013) Dark patterns in the design of games. *FDG 2013.*