Добри практики в управлението на риска при споделяне на лични данни и защита на информацията в социалните мрежи

Гл. ас. д-р Мирослав Дечев
Институт по роботика – БАН

Good practices in managing the risk of sharing personal data and protecting information in social networks

Ch. Assist. Dr. Miroslav Dechev
Institute of Robotics - BAS

***Abstract**: The research raises an extremely important question related to users' concerns about their privacy on social networks. Consumers' lack of knowledge about data access policies puts the development of the digital world to the test going forward, and researchers will continue to address consumer attitudes. The purpose of this article is to focus not only on data theft and access to third parties, but also on the habits of people to verify and protect their information. There is a huge need for specialized and thematic information security training at an early age, which turns out to be key sometimes for the physical survival of our children and all of us. This is shown by the data from a study carried out in the scientific material regarding the attitudes of users using social networks.*

***CCS concepts**: Human computer interaction (HCI); Security and privacy; Information systems applications*

***Additional Keywords and Phrases**: Information systems, Information security, Information protection, Risk Management.*

Резюме: Изследването повдига изключително важен въпрос, свързан с притесненията на потребителите относно поверителността им в социалните мрежи. Липсата на познания на потребителите относно политиките за достъп до данни поставя развитието на цифровия свят на изпитание занапред и изследователите ще продължат да се занимават с нагласите на потребителите. Целта на тази статия е да се фокусира не само върху кражбата на данни и достъпа до трети страни, но и върху навиците на хората да проверяват и защитават информацията си. Има огромна нужда от специализирано и тематично обучение по информационна сигурност в ранна възраст, което понякога се оказва ключово за физическото оцеляване на нашите деца и всички нас. Това показват да-

нните от проучване, проведено в научния материал относно нагласите на потребителите, използващи социалните мрежи.

CCS концепции: Взаимодействие между човек и компютър (HCI); Сигурност и поверителност; Приложения на информационни системи

Допълнителни ключови думи и изрази: Информационни системи, Информационна сигурност, Защита на информацията, Управление на риска.

Въведение.

Развитието на технологичните атаки и неоторизирания достъп до информационни активи, изискват модернизация на технологиите за защита на информацията в големите масиви от данни. Рискът за информацията в онлайн пространството нараства експоненциално с увеличаване броя на потребителите, хилядите приложения, непрекъснатата свързаност към Мрежата. Голяма част от информационните системи са уязвими, поради грешки в софтуера и трудност при разбиране от потребителите. Изпращачите на вируси разчитат на това, че ползвателите на Интернет пространството нямат познания как тези действия уязвяват информацията. А когато потребителите не разбират какво точно правят, на хакерите е още по-лесно да ги заблудят. Особено трудно е на администраторите по сигурност да се борят с постоянните и новооткриващи се уязвимости. Информационната сигурността става все по-трудна за изграждане и реализация. Технологичните възможности за атаки и за защити са в постоянно съревнование и немалко пъти хората, които извършват атаките имат преднина.

I. Управление на информационната сигурност

Осигуряването на сигурността на информацията започва още с проектирането и изграждането на бъдещата информационна система. Това става с конфигурирането на оборудването и програмно обезпечаване.

Сигурността е свойство на една система да противостои на външни или вътрешни дестабилизиращи фактори, които могат да доведат до нейното нежелателно състояние или поведение. Това важи и за сигурността на информационните системи [1].

Гарантирането на информационната сигурност изисква определен набор от инструменти за контрол, свързани с политиките, процесите, организационните структури, софтуерни и хардуерни функции.

1.1. Заплахи пред информационната сигурност в социалните мрежи и Интернет

Киберзаплаха представя „всеки идентифициран опит, насочен към достъп, извличане, подправяне, или нарушаване целостта, поверителността, сигурността или достъпа на данни, приложение или федерална система без законново право за това”[2].

Компютърните и мрежовите атаки се разделят най-общо на 7 категории: кражби на парола, извличане на информация без оторизиран достъп, използване на слабости и черни врати, възползване от дефекти, грешки в протоколи, мрежови атаки, откази на обслужване на потребителите.

Съвременни изследвания сочат, че киберзаплахите много бързо навлизат в ново появяващите се територии от дигиталното пространство – социални медии, мобилни устройства и облачни услуги [3].

1.2. Стратегии за сигурност в Интернет

Различни са стратегиите за сигурността в Интернет. Те се оформят и създават при изграждането на модела за информационна сигурност.

Управлението на рисковете, тяхното ефективно и своевременно адресиране следва да бъде неразделна част от всички дейности по управление на информационната сигурност и трябва да се прилага едновременно с внедряването и текущата експлоатация на СУИС [4].

Основната цел е намаляването до минимум уязвимостта от хакери. Една от стратегиите за сигурност, позволяваща това, е предоставянето на минимални привилегии, където възможностите за действие на хакери са намалени до минимум, а работата на вътрешните компоненти невъзпрепятствана. При тази страте-

гия обезпечаването на сигурността касае най-привилигированите компоненти на системата.

Пример за стратегия на минималните привилеги е групирането на акаунтите в операционни системи като UNIX или Windows NT. При такива операционни системи се създават различни потребителски групи и правата се предоставят за групите като цяло [5].

С други думи казано, привилегии са създадени само за определени групи потребители. В стратегиите за сигурност се използва и така наречената запушване, при която се стеснява връзката между локалната мрежа и интернет.

Това стеснение се нарича точка на запушване и всъщност стеснява канала, по който хакерът може да атакува, като се ограничават точките за достъп до мрежата [5].

В моделите за сигурност се използва и стратегията от типа най-слаба връзка. При нея се идентифицира и поставя под специално внимание компонент опасен за сигурността. Сред останалите стратегии за сигурност са универсалното участие, когато в системата участват всички вътрешни компоненти, разнородна защита, при която се изгражда силна преграда като се използват защитни стени.

Защитната стена е една част от глобалната политика за сигурност, която създава отбранителна зона, за да защити информационните ресурси на ведомството. Всички потенциални точки за мрежова атака трябва да бъдат защитени със съответните нива на мрежова защита [6].

Говорейки за гарантирането на информационната сигурност на преден план изпъкват социалните мрежи, най-малкото защото в тях сме взаимносвързани не само при влизане в профилите си, а изцяло в онлайн потреблението ни. Социалните мрежи по своята същност са богати на много лична информация. Дигиталният ни живот, обаче може да се окаже прекъснат и дори изтрит само с няколко операции от опитни хакери.

Фалшивите профили, наречени *социоботове* (социални роботи), представляват софтуерни агенти, които изглеждат като обикновен профил във Facebook и се представят за човешки същества [7].

1.3. Криптографски приложения

Един от използваните методи и процеси в защитната архитектура на моделите за сигурност е *Криптографията*.

Криптографията е наука за шифриране и дешифриране на данни. Обикновено данните съществуват в своя суров вид и могат да бъдат четени от всеки. Такива данни не са защитени, тъй като хакерите могат да пробият защитата и да ги прочетат. Ако маскирате данните по някакъв начин, който ги прави да изглеждат безсмислени, вие сте ги криптирали успешно [5].

Така наречения шифрован текст оства неразбираем за хората, които не знаят по какъв начин данните са криптирани. Т.е. декриптирането, превръщането на данните в първоначалния им изглед е механизъм познат само на избрани потребители и би бил труден да бъде проследен от хакери. Конвенционалната криптография използва понятието криптиране със симетричен ключ (symmetric key encryption). При такова криптиране се използва само един ключ както за криптиране, така и за декриптиране на данните. Пример за конвенционална криптография е „Цезаровото писмо", което използва метода „отместване с три".

Наименованието „Цезарово писмо" произлиза от използваният от Гай Юлий Цезар шифър, при който всяка буква е заместена с буквата, която стои с три позиции след нея в азбуката. След последната буква в азбуката се счита, че стои отново първата т.е. азбуката е разположена в кръг [6].

Криптирането е един от начините за осигуряването на цялостност при предаването на данните.

Смисълът на една шифрова (криптографска) система е преобразуването на някакъв таен текст, така че неговото съдържание да бъде разбираемо само за посветени в тайната хора и неразбираемо за всички останали.[6].

Основната цел на криптирания текст е защитата му, невъзможността да бъде разчетен от трето лице, освен от този, който го изпраща и този, който го получава.

Най-важната разлика е в начинът на съхраняване на ключовете. При апаратното криптиране ключовете се пазят в специално устройство и до тях няма програмен достъп [6].

Под понятието „програмно криптиране" ще разбираме такова криптиране, при което криптиращата последователност се получава, чрез програмни средства, изпълнявани на универсален компютър, а ключовете на криптографската система се пазят върху стандартните му запомнящи устройства [6].

Апаратното криптиране има няколко характеристики, сред които се нареждат сигурно съхранение на ключа, слаба адаптивност, висока цена и променливи параметри на апаратурата.

Криптографският алгоритъм е система от краен брой указания и правила, задаващи реда на изпълнение на елементарни действия над явния и криптирания текст и над ключа с цел ефективно криптографско преобразуване [6].

Последователността от битове, думи или байтове, които потребителят е избрал при използване на криптографската система определя криптографския ключ.

1.4. Опасности при работа в социалните мрежи и Интернет

В социалните мрежи се създава огромно количество от данни за човешкото поведение и интереси, притегателно за злонамерени атаки, а защитите, предоставени в тях се оказват лесно-пробиваеми. Кликвайки върху определени линкове, посетителите неволно допускат вирус в компютрите и телефоните си.

Един от най-известните вируси в социалните мрежи е „Кубфейс", който поразява потребителите на „Фейсбук" по целия свят. Той се разпространява като съобщение, което гласи: „Току-що видях този клип с твое участие" [8].

Тази хоризонтална и органична система за комуникация предлага напълно нов начин за съобщение, разпространение и споделяне на информация. Особено мощна е, когато се съчетае с други технологии за децентрализиране, като например облачно съхранение, анализ на големи масиви от данни, криптография, машинно учене, отворени данни и блокчейн – технологии, чиято способност за взаимодействие означава, че са свързани пряко с платформите за публикация в социалните мрежи [9].

Социалните мрежи могат да бъдат разгледани като огромен свръхорганизъм. Безспорно най-голямата социална мрежа днес Facebook, която продължава да увеличава потребителите си. С публикуването на статусите започва изграждането и на дигиталната личност, оформя се и ясна информация за връзките между потребителите. Получават се голям брой точки на пресичане и от друга страна възможностти за по-лесното и бързото ни „*откриване*". През 2010 г. Марк Зукърбърг говори за термина Open Graph. Тук целта е обединяване на всички социални графи в социалната мрежа Facebook.

Това се осъществява чрез Facebook API, който свързва вашия профил, вашите връзки, съдържание на Facebook страници, а също така и външни сайтове и блогове. Една от формите е и бутонът Facebook Like [10].

Натискайки бутона Like един потребител ясно изразява предпочитание или харесване, което, обаче, не остава скрито, а напротив – появява се на неговата профилна страница в социалната мрежа. Така той разпространява и записва харесаната публикация в социалния си граф.

В информационното общество технологиите позволяват нежелано нахлуване в личното пространство на хората, тъй като огромни компютърни бази данни съхраняват голяма част от личната информация за живота на всеки един индивид [11].

Все повече хората се чувстват застрашени и незащитени в потока от информация за тях, използвана от различни институции или пък от недроброжелатели.

Уязвимите компютърни мощности ни гарантират социална несигурност и лавинообразен ръст в престъпността, за който сме напълно неподготвени. Общият брой на снимките във „Фейсбук" надхвърля четвърт трилион, което превръща компанията в най-голямото хранилище на биометрични данни на планетата [8].

Тази голяма база от данни с биометрична информация е абсолютно възможно да бъде инструмент освен за следене, а и за манипулиране на потребителите от частни ръце, а не само с цел предотвратяване на пръстъпност.

II. Човешкият фактор в основата на ефективността при информационната сигурност в социалните мрежи

С експоненциално развиващата се технологична епоха киберпрестъпността става неизменна част от дигиталния ни живот. Все повече хакери откриват пробойни в операционните системи и както по-горе стана ясно необходим е един смс, изпратен от хакер, за да бъдат източени данните ни в телефона. Сведените до минимум рискове при използването на социалните мрежи няма да спрат атаките, но биха ги ограничили.

2.1. Проучване нагласите на потребителите, използващи приложения чрез Фейсбук и рисковете, свързани със сигурността на личните им данни

Основната цел на проучването е да се получи информация на базата на личния опит на потребителите относно комуникационното поведение при работа със социалната медия Фейсбук. Изследвана е необходимостта от социалните мрежи в личния живот на ползвателите, предпочитанията при публикуването на лични данни в социалните медии, влиянието на заплахите в комуникационния процес между потребителите и избора на комуникационни стратегии, като поверителност, интегритет и защита на личната информация в платформата и различните приложения в нея. За целите на проуването са анкетирани общо 100 респонденти на различна възраст, с различни професии и образование. Изследването е проведено по комбинирана методика **онлайн/лична анкета (90/10)**. Анкетната карта е разпространена в два варианта: на хартиен носител /*попълнена след предварителна уговорка с участници*/ и чрез онлайн платформата за създаване и разпространение на анкети **Google Forms** /*попълнена чрез разпращане на линк по* ***e-mail*** *и чрез* ***Messenger*** *в социалната мрежа Facebook*/.

2.2. Въпроси, включени в Анкетната карта

Въпросите са 10 от затворен тип с възможност от 2 до 6 отговора. Формулирани са по следния начин: *Въпрос 1*: Ползвате ли социалната мрежа Фейсбук?, с възможни отговори „*Да*" и „*Не*"; *Въпрос 2*: По колко време дневно прекарвате във Фейсбук? Възможностите за отговор тук са 4: *От 0 до 1 час*, *от 1 до 2 часа*, *от*

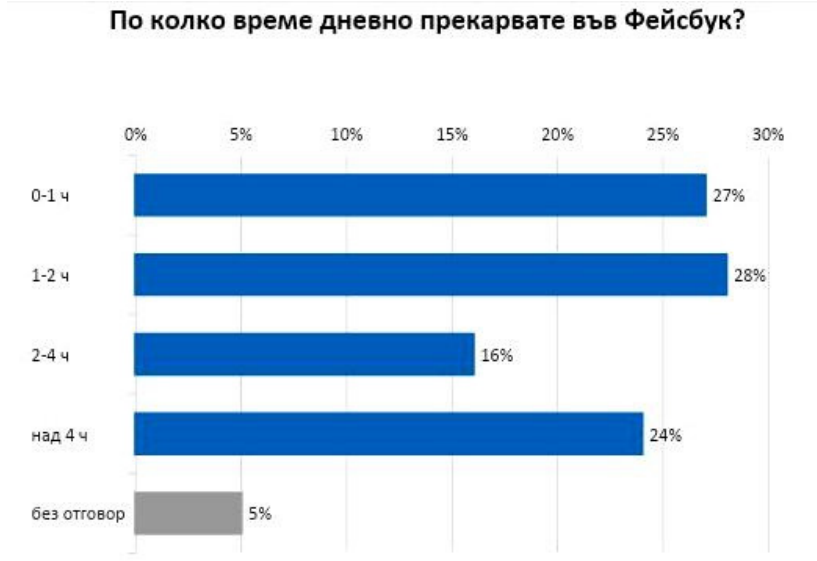
2 до 4 часа и *над 4 часа*; *Въпрос 3*: Страхувате ли се от кражба на лични данни при споделяне на информация в социалната мрежа Фейсбук?, тук са два отговора: „*Да*" и „*Не*"; *Въпрос 4*: Влизате ли в приложения или уеб сайтове, като използвате профила си във Фейсбук? /например игри, онлайн магазини, новинарски сайтове и др./, където отговорите са два: „*Да*" и „*Не*"; *Въпрос 5*: Знаете ли, че дори премахнати приложенията от профила Ви във Фейсбук, все още могат да имат достъп до Ваша споделена информация в социалната мрежа?, с два възможни отговора: „*Да*"и „*Не*"; *Въпрос 6*: Запознати ли сте с основните принципи на поверителност при използване на приложения чрез Фейсбук?, с три възможни отговора: „*Да*", „*Не*" и „*Не съм наясно*"; *Въпрос 7*: Ограничавате ли достъпа до снимки и лични данни във Фейсбук чрез различни инструменти и настройки?, с три отговора: „*Да*", „*Не*" и „*Не съм запознат с тази политика на социалната мрежа*"; *Въпрос 8*: Смятате ли, че ваши споделени снимки и лични данни във Фейсбук се използват от трети страни без Вашето съгласие?, като възможните отговори са 3:„*Да*", „*Не*", и „*Това не ме притеснява*"; *Въпрос 9*: Възраст - *до 18 години*, *18-25 години*, *25-40 години*, *40-50 години*, *50-65 години* и *над 65*; *Въпрос 10*: Образование: „*основно*", „*средно*", „*висше*".

2.3. Резултати и анализ на данните, получени от Анкетната карта

На базата на резултатите от изследването е направен количествен и качествен анализ, описващ поведението на отделните социални групи при работа със социалната мрежа Фейсбук. Тя присъства трайно в живота на съвременното ни общество и това се потвърждава от отговорите на първия въпрос: **Ползвате ли социалната мрежа Фейсбук?**, на който 93% от респондентите отговарят с „Да". Най-голям процент на използващите Facebook са хората с висше образование - 95,3% и на възраст от 18 до 50 години – близо 100%. Докато във възрастовата група от 50 до 65 години, 11,8% споделят, че нямат профил. С покачването на възрастта, тенденцията за присъствие в социалната мрежа е низходяща, като най-малко използвана е тя от възрастните хора над 65 г., като по-малко от половината, почти 43% от тях споделят, че използват Facebook. От съществено значение е следващия въпрос, тъй като с него ще се

определи активността в социалните мрежи, а именно: **По-колко часа дневно прекарвате във Фейсбук?**

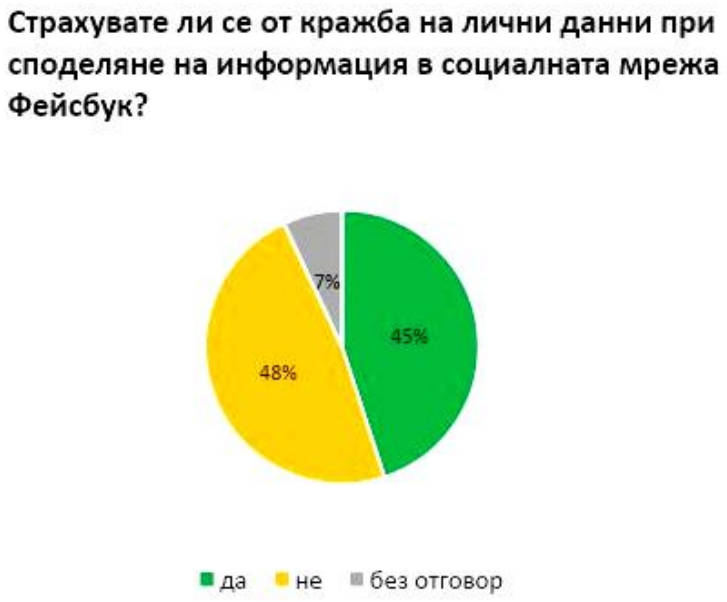
Отчетените данни проследяват честотата на „влизане" в социалната мрежа тъй като именно тя би могла да бъде показател за активността в мрежата и използването ѝ понякога като основно средство за комуникация, забавление, новини и обмен на информация между потребителите ѝ.



Фиг.1. Резултати от Въпрос 2 в Анкетната карта

Резултатите показват, че социалната мрежа се е наложила като основен комуникационен канал за младите хора на възраст от 18 до 25 години, които прекарват до 2 часа дневно в нея или това са близо 70% от анкетираните във възрастовата група. Над 4 часа на ден прекарват активните хора на възраст от 25 до 40 г., показват още данните или 36,4% от участниците в тази възраст. Голям процент, посочват часови диапазон на използване на Facebook от 1 до 2 часа дневно (28%). Изводът може да бъде само един, че за голяма част от обществото Facebook играе все по-голяма роля за комуникацията. Най-малко се възползват от социалната мрежа възрастните хора над 65 години, което говори или за малък интерес, или

за невъзможност и непознаване възможностите на мрежата. 42,9% от потребителите на Facebook над 65 години прекарват в платформата не повече от час дневно. От важно значение е анализа на дадените отговори на 3-тия въпрос: **Страхувате ли се от кражба на лични данни при споделяне на информация в социалната мрежа Фейсбук?** С него потребителите дават ясна представа затова, дали са запознати с един от най-големите рискове в Интернет - кражбата на лични данни.

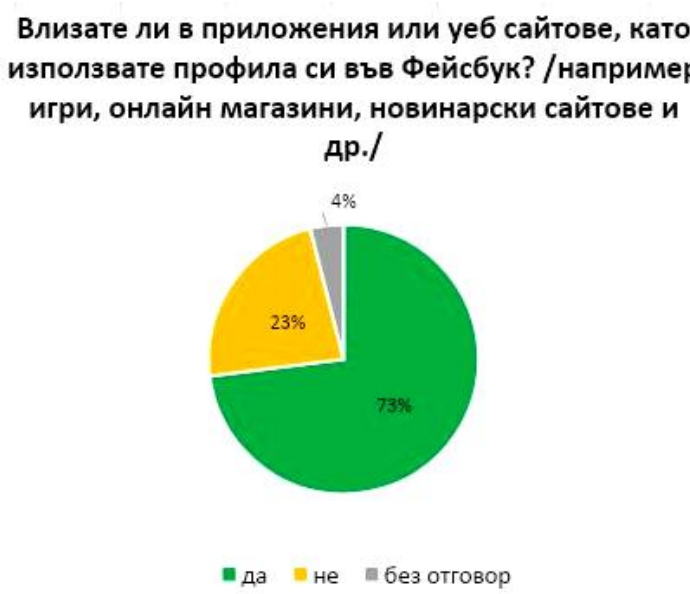


Фиг.2. Резултати от Въпрос 3 в Анкетната карта

Близките стойности на отговорите „Да" и „Не", категорично показват, че голяма част, почти половината от запитаните (48%) не се страхуват от кражба на лични данни при споделяне на информация във Facebook. Този отговор отвежда изследователите към размисъл, защо хората не подозират за опасностите в интернет пространството, дали от липса на информираност или просто вярват, че опасност за данните им не съществува. Голям процент, от младите хора от 18 до 25 години (55,6%), от активните хора – 40-50-годишни (59,1%), както и хората на възраст от 50 до 65 го-

дини (52,9%) заявяват, че нямат притеснения при споделянето на данни във Facebook. А над 53% от запитаните, които не се страхуват от кражба, са с висше образование. Това категорично показва, че потребителите се чувстват сигурни в мрежата и са убедени, че данните им са добре защитени. Наблюдава се едно противоречие на фона на статистиките от цял свят, че обект на кражба на лични данни са именно социлните мрежи. Жените остават, обаче, по-предпазливи при публикуване на информация в социалната мрежа, показват още резултатите. Над 50% от нежния пол се страхуват за личните си данни, споделени във Facebook. Развитието на социалните мрежи даде възможност на потребителите да използват профилите си за регистрация в различни приложения, които изискват единствно синхронизация на данните. Т.е. веднъж регистрирани във Facebook, чрез профила си можем да се „логнем" в желаното приложение без да е необходима допълнителна автентификация.

От гледна точка на използването на профилите във Facebook за регистрация в различни приложение или уеб сайтове, игри, онлайн магазини, новинарски сайтове и ред други, 73% от участниците споделят, че влизат в приложения чрез профила си. На въпроса: **Влизате ли в приложения или уеб сайтове, като използвате профила си във Фейсбук? /например игри, онлайн магазини, новинарски сайтове и др./**, 23% не се възползват. От резултатите става ясно, обаче, че силната застъпеност на използването на даден профил в социалната мрежа за регистрация в други платформи открива пред потребителите още повече рискове, свързани с информационната сигурност, защото на практика, обмена на техните данни се увеличава многократно заедно с притежателите на данните им. Следва да се отбележи, че чувствителни данни като e-mail, име, парола или снимки, местоположение, свободно могат да попаднат в трети страни след едно безобидно на практика „логване" в приложение или игра, тъй като за да ползват услугите му собствениците на профили споделят доброволно своите данни. Именно тази по-лесна нова възможност поставя нови задачи и предизвикателства към защитата на тези системи и защитата на информацията в тях.



Фиг.3. Резултати от Въпрос 4 в Анкетната карта

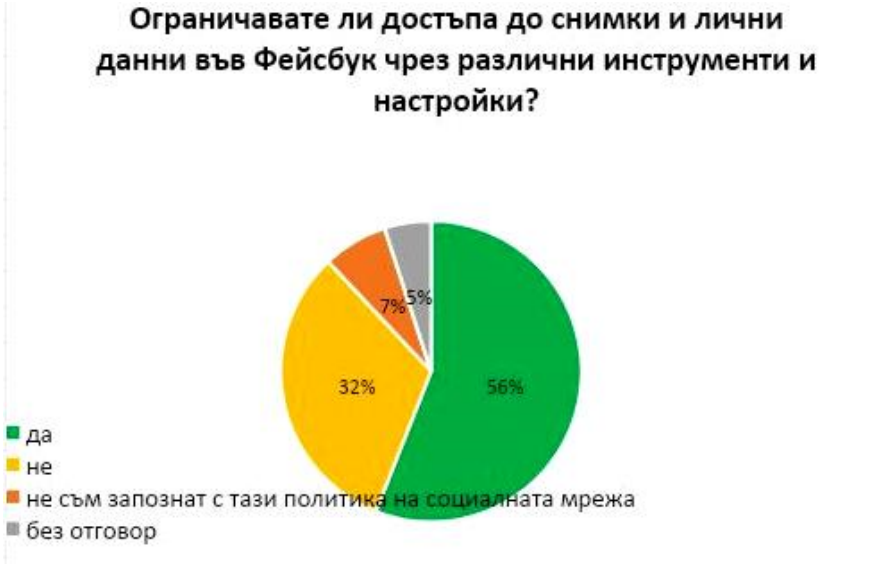
Най-висок е процентът на младите хора от 18 до 25 години, които смело използват профилите си в социалната мрежа за регистрация в други приложения, почти 90% от анкетираните. Важно е да се отбележи, че тук процентът е висок във всички възрастови групи, като намалява постепенно при по-възрастните хора и тези над 65 г. (30%). След като такъв висок процент заявяват, че използват социалната мрежа за вид автентификация в различни приложение и уеб сайтове, следва да се анализират данните дали потребителите разбират огромния риск за споделената информация. На впрос 5-ти: **Знаете ли, че дори премахнати приложенията от профила Ви във Фейсбук, все още могат да имат достъп до Ваша споделена информация в социалната мрежа?**, над половината от участниците (57%), дават положителен отговор. Тенденция, обаче, е непредпазливостта и незнанието отстрана на потребителите относно опасността дадени приложения да разполагат с лична информация.

	18–25 г.	25–40 г.	40–50 г.	50–65 г.	над 65 г.	средно	висше
Да	33,3	65,9	63,6	58,8	14,3	46,9	65,6
Не	66,7	34,1	36,4	23,5	57,1	43,8	31,3
Без отг.	0	0	0	17,7	28,6	9,3	3,1

Таблица.1. Резултати от Въпрос 5 в Анкетната карта в проценти (%)

Не можем да подминем резултите, при които близо 70% от анкетираните млади хора във възрастова група 18-25 години споделят, че не знаят, че дори премахнати приложенията от профила във Facebook, все още могат да имат достъп до споделена информация в социалната мрежа. Оказва се, че по-запознати с рисковете в тази област са хората в активна възраст от 25 до 50 години, сред които близо 65 на сто са наясно с това, че достъпа до лични данни в социалната мрежа е възможен и след отстраняването на приложенията от профила ни във Facebook. От значение в тази област е и образованието на потребителите. 65,6% от участниците в Анкетата с висше образование посочват, че са запознати с проблема, респектовно на тези със средно образование - 46,9%. Важно е да се отбележи, че почти 30 на сто от хората в напреднала възраст над 65 години изобщо не са запознати с проблематиката, тъй като оставят въпроса в изследването без отговор, а 57,1% от възрастовата група отговарят с „Не". Необходимостта от информираност по проблема нараства и от факта, че 43,8% от анкетираните със средно образование не знаят за достъпа на приложенията до личните им данни дори след като бъдат премахнати посредством определен инструментариум в мрежата. Следващият 6-ти въпрос в Анкетната карта касае ***Поверителността*** при използването на приложения чрез Facebook. Както стана ясно по-горе отговорите тук бяха три, което даде и доста разнороден резултат. На въпроса: **Запознати ли сте с основните принципи на поверителност при използване на приложения чрез Фейсбук?**, 39% от потребителите са наясно с тях, по 28 на сто от участниците споделят, че не са наясно и не ги познават (отговор „Не), и 5% оставят въпроса без отговор. Или сумарно над 60% от хората, използващи приложения във Facebook изобщо не са запознати със защитата и конфиденциалността на информацията, споделена при работа с приложения чрез Facebook.

Facebook разкрива известна информация за това какви ще бъдат данните в приложенията и достъпа до тях, когато потребителите ги инсталират, но потребителите са оставени да разчитат на своите собствени разбирания на политиките за поверителност на Facebook [12].



Фиг.4. Резултати от Въпрос 7 в Анкетната карта

Най-голям процент се оказаха хората на възраст от 40 до 50 години – 50%., следвани от потребителите на възраст от 25 до 40 години (43,2%) и тези във възрастова група 18-25 години (33,3%). Необходимо е да се посочи, че почти 45% от младите хора не познават принципите на поверителност при работа с приложения чрез Фейсбук, като отговарят на въпроса с „Не", следвани от хората на възраст от 25 до 40 години, също с отрицателн отговор почти 32%. Отговор „Не съм наясно" дават 42,9% от хората на възраст над 65 години, следвани от тези между 40 и 50 години (36,4%) и на възраст 25- 40 години – 25%. Като основен извод може да се изведе, че младите потребители и хората в по-активна възраст със средно (28,1%) и висше (28,1%) образование не се влияят от рисковете, свързани с конфиденциалността на информацията, защото не познават политиките за поверителност в Мрежата. Много от хората

нямат информиран избор какво и с кого споделят, при изтегляне на различни приложения в социалната мрежа. Спорни и разнородни спрямо възрастта и образованието се оказаха отговорите на потребителите, свързани с включването на настройките за ограничаване на достъпа до снимки и лични данни, и необходимостта от публикуването им публично. Това пролича в следващия въпрос, 7-ми по ред, свързан с **ограничаването на достъпа до снимки и лични данни във Фейсбук чрез различни инструменти и настройки**.

Най-висок процент сред анкетираните отговорили положително с „Да" на въпроса, е този на хората от 18 до 25 години (77,8%) и тези с висше образование (59,4%). 63,6% от потребителите от 25 до 50 години използват различни инструменти и настройки, за да ограничат достъпа до снимки и лични данни във Facebook.

Почти 30 на сто от хората на възраст от 50 до 65 години и около 14 на сто от участниците в проучването над 65-годишна възраст отговарят с **„Не съм запознат с тази политика на социалната мрежа"**. Едва 11% от по-младите анкетирани до 25 години и 36,4% от 25 до 50 години, не ограничават достъпа до публикувани свои снимки и лични данни в социалната мрежа Facebook, показват още резултатите. Като извод тук може да се изведе, че притесненията, относно оторизирания достъп до данните ни в социалната мрежа се засилват, а познаващите рисковете на това, публикаците ни да са публични, са по-младите и активни потребители, както и тези с по-висока степен на образование. Въпреки, че голям процент от ползвателите на социалната мрежа Facebook споделят, че са притеснени да излагат публично свои снимки и лични данни, не малък процент от анкетираните в изследването, или малко под половината (45%) изразяват увереността си, че споделени снимки и лични данни във Фейсбук не се използват от трети страни. Това бе и **8-мия** въпрос в проучването, който по категоричен начин доказа, че доверието в социалната мрежа по отношение на защита на данните и опазването им от трети страни нараства. И все пак не малко от запитаните - 38% са убедени, че достъп до нашите данни имат трети страни. Сред тях са повече на възраст между 40 и 50 години и висше образование. Факт е, че възрастните хора над 40 до 50 години и тези над 65 смятат, че платформите не са безопасни (над 40%). Интерес

представлява мнението на хората в най-младата възраст от 18 до 25 години, които споделят, че според тях достъп от трети страни до данните ни няма (почти 89%) от анкетираните млади хора.

Задълбочен изследователски анализ изисква мнението във възрастовата група от 50 до 65 години, зрели и образовни хора, които заявяват: **„Това не ме притеснява" (23,5% от анкетираните в групата)**. 53,6% от хората със средно образование не смятат, че лични данни и снимки споделени в мрежата се използват от трети страни. **Изводът недвусмислено тук е, че** доверието в социалната мрежа Facebook по отношение на защита на данните и опазването им от трети страни се покачва рязко при по-младите потребители, за сметка на по-улегналите и по-висока степен на образование.

Проучването повдига изключително важен въпрос, свързан с притесненията на потребителите относно поверителността им в социалните мрежи. Липсата на познания на потребителите относно политиките за достъп до данни поставя развитието на цифровия свят на изпитание занапред и изследователите ще продължат да се занимават с нагласите на потребителите. Целта на тази статия е да се фокусира не само върху кражбата на данни и достъпа до трети страни, но и върху навиците на хората да проверяват и защитават информацията си.

Заключение

Изложените по-горе проблеми налагат няколко изследователски въпроса в настоящото научно изследване. На първо място изясняването на рисковете при споделяне и обмен на информация между потребителите, нейната обработка и съхранение. На второ място – защитата на информацията, нейната поверителност, конфиденциалност и цялост в Интернет средата. Наложително е потребителите да спазват основни правила при изграждане на потребителските навици, за да бъде осигурено правилното и ефективно управление на информационната сигурност в социалните мрежи. В условията на ускорено развитие на дигиталния свят, запазването на поверителност при кореспонденция в информационно пространство е все по-трудно. Автоматичните системи за сигурност

са уязвими по подразбиране и винаги могат да се преодолеят от нападател с достатъчно мотивация. Намалените рискове при използването на социалните мрежи няма да спрат атаките, но биха ги ограничили доколкото е възможно. Хората не са достатъчно информирани какви мерки са необходими за защита на информационната сигурност.

Литература:

[1] Cheresharov, S., & Krushkov, H. (2016). NoSQL Approaches in SQL Database, Scientific Conference "Innovative ICT in Business and Education: Future Trends, Applications and Implementation", Pamporovo, Retrieved from: http://fmi-plovdiv.org/GetResource?id=2519.

[2]Boyanov, L., Cybersecurity in "smart houses", http://smarthomesbg.com/files/lb_cybersecurity_of_smart_homes_unwe_3_4_oct_2013.pdf, Кибер-сигурност в „умните къщи"

[3] Li, T., Yang, H., He, J., Ai, Y., A Social Network Analysis Methods based on Ontology, International Symposium on Knowledge Acquisition and Modeling, 2005., 258-261, DOI: 10.1109/KAM.2010.5646196.

[4] Stoyanov, N., Ismailov, O., Tselkov, V., Risk management, testing and evaluation of network and information security. Sofia, 2016

[5] Pritam, VV, NIIT, Firewalls and Internet Security, 2005

[6] Petrov, R., Information protection in computers and networks. Sofia, 2002

[7] Chakarova, I., Social networks on the Internet - Features and risks. Paisii Hilendarski University of Plovdiv - Smolyan Branch, 5th National Conference "Education in the Information Society" 155

[8] Goodman, M., 2016 Future Crimes Anchor Book Press

[9] Luckett, O., Casey, M., The Social Organism. How social networks function as a living organism and change our business, society and future. Sofia, 2017

[10] Toms, J., Georgieva, K., Tools for social networks. Marketing in the age of Web 2.0. Sofia, 2011

[11] Dermendzhieva, G., Online Journalism, Media in the Digital World, Sofia, 2012

[12] Golbeck, J. Mauriello, M L 2016 User Perception of Facebook App Data Access Future Internet 8 9 p 14