КИБЕР АТАКИТЕ – МОДЕРНИЯТ ТЕРОРИЗЪМ В КОНТЕКСТА НА ТУРИЗМА

доц. д-р Златина Караджова
Университет „Проф. д-р Асен Златаров“, Бургас

KIBER ATTAKES – THE MODERN TERRORISM IN THE TOURISM CONTEXT

Zlatina Karadzhova

Резюме: *Съвременната икономика на знанието не само зависи, но и се развива все по-перспективно в нови направления, свързани с интензивното използване на информационните технологии, софтуерни системи за управление, както и на ефективни процеси, базирани на дигиталните инфраструктури. Кибер атаките са директна заплаха за сигурността на гражданите и функциониране на държавата, икономиката, обществото, науката и образованието. Те могат да бъдат извършени от разстояние, с прости и ефективни механизми и минимални ресурси, да причинят значителни поражения с нанасяне на материални и дори човешки загуби. Кибер атаките нямат национални, културни или юридически граници.*
Целта на доклада е да заостри вниманието към атаките в интернет пространството, като алтернативна форма на тероризма и тяхното отражение върху туризма.
Ключови думи: *кибер атаки, тероризъм, електронен бизнес, туризъм.*

Abstarct: *The modern knowledge economy not only depends, but also develops more and more prospectively in new directions related to the intensive use of information technologies, software management systems as well as efficient processes based on digital infrastructures. Cyber attacks are a direct threat to the security of citizens and the functioning of the state, economy, society, science and education. They can be done at a distance, with simple and effective mechanisms and minimal resources, causing considerable damage with material and even human losses. Cyber attacks do not have national, cultural or legal borders.*
The aim of the report is to raise awareness of online attacks as an alternative form of terrorism and their impact on tourism.
Key words: *cyber attacks, terrorism, e-business, tourism.*

УВОД

Информацията е най-ценният актив в 21-ви век. Нейното опазване отдавна се е превърнало в ключов приоритет за всички компании, организации и институции по света, като тази тенденция навлиза все по-усилено и у нас. Доклад на „Gartner“ **[8]**очи, че през 2017 г. за информационна сигурност в световен мащаб са похарчени над 90 млрд. долара, което е ръст от 7,6% в сравнение с 2016 г. Според друг доклад на „Cybersecurity Ventures“ [9] за опазване на информацията през 2017 г. са похарчени 120 млрд. долара.

Развитието на информационните и комуникационни технологии (ИКТ) и дигитализацията като глобален феномен промениха характера на съвременните общества от „технологични“ в „информационни“ в качествено нова, информационна ера. Държавата, бизнесът и гражданите разчитат на лесен достъп и надеждно функциониране на комуникационните и информационните системи и технологии и Интернет средата, или на новото пространство, в което вече живеем и се развиваме – кибер пространството. Кибер пространството е електронният или „виртуален“ свят от взаимосвързани комуникационни и информационни системи, в чиито мрежи глобалната общност от над 3 милиарда граждани, или повече от 45% от населението на земята обменя информация, идеи, услуги, бизнес и приятелство, без територии и граници.

ПРИЛОЖЕНИЕ НА ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ В ТУРИЗМА

Модерните общества развиват и използват все по-целенасочено възможностите на кибер пространството и ИКТ за развитие във всички сфери – икономика, социален живот, култура, наука и образование, политически живот. Под ефективност на иновационните технологии трябва да се разбира интензивността на дейностите по разработка и внедряване на нови или усъвършенствани продукти и технологии в организацията. Самият процес на внедряване на иновационни подходи в стратегическото й управление се явява способ за реално достигане и реализиране на целите на предприятието, обезпечаващи неговото конкурентно преимущество. [7] Дигиталните инфраструктури се превръщат в гръбнак, или критичен фактор за управлението и нормалното функциониране на всички ресурси и системи с национално значение, на модерна и иновативна икономика, прозрачно управление, на модерно и демократично гражданско общество.

Туризмът е един модерен икономически отрасъл. Той е най-бързо развиващата се икономика и зависи изключително много от развитието на модерните технологии. Широко разпространено е мнението, че интернет и технологичните иновации революционизират туристическата индустрия повече от всеки друг фактор през последните десетилетия – не само по линия информираност, но и от гледна точка на достъп до продукти, услуги и дестинации, начин на потребление и др., като това се отразява на цялостния процес на туристическото потребление – от взимането на решение за почивка до последващите продажби. [1]

Туристическата индустрия като социално-икономическа сфера, подлежи на влияние от външната среда, затова и използването на принципите на стратегическо управление се явява необходимост. [5] Къде са подводните камъни, какъв е риска, какви са заплахите от постоянното развитие на електронните бизнес комуникации и как би следвало да се предпазим? Ще се опитам да дам отговор на тези въпроси, но нека първо видим какви са формите на електронен бизнес в туризма.

ФОРМИ НА ЕЛЕКТРОНЕН БИЗНЕС В ТУРИЗМА

Процесите на е-бизнеса в туризма се фокусират главно върху клиентите под формата на електронен маркетинг и продажби. Най-популярни на този етап са онлайн резервациите и покупките на самолетни билети, нощувки и туристически пакети. Все по-широко се използват и онлайн покупките на тези продукти. Изграждането на цялостна представа за съвременен мениджмънт се постига със задълбочено вникване в същността на процесите в е-бизнеса – постигане на икономическа и технологична ефективност [4] Практиката показва, че автоматизацията на вътрешните бизнес процеси в туристическия отрасъл е по-слабо застъпена отколкото в производ-

ствените сектори. Тя се изразява в използването преди всичко на отделни счетоводни програмни продукти, а не на интегрирани системи за фирмено управление от типа на ERP (Enterprise Resource Planning) системите. Причината за това е преди всичко финансова, тъй като последните са доста скъпи и намират приложение главно в големи фирми и компании.

Най-разпространените форми на е-бизнес в туризма са следните:

1. Електронна (Интернет) търговия – Покупко-продажба на стоки и услуги посредством компютърна мрежа (най-често Интернет).

2. Електронен (Интернет) маркетинг – Интернет средства за анализ и изследване на пазара – продукти, цени, клиенти и конкуренти.

3. Системи за управление на взаимоотношенията с клиентите (Customer Relationship Management – CRM) – Събира информация за клиентите в централизирана база от данни и създава по – тесни взаимоотношения с тях с цел задържането им за дълго време.

4. Системи за планиране на фирмените ресурси (Enterprise Resource Planning – ERP) – Интегрирана система за управление на всички бизнес операции, материални, трудови и финансови ресурси на предприятието въз основа на единна база от данни.

5. Електронни разплащания и електронно фактуриране (electronic invoicing – е e-invoicing) – Създаване и изпращане на електронни фактури и други платежни документи и превеждане на суми по електронен път.

6. Системи за управление на веригата за доставки (Supply chain management – SCM) – Управление на цялостната верига, по която суровините се превръщат в стоки и стигат до крайните потребители.

7. Интелигентни бизнес решения (Business Intelligence – BI) – Процес и технология за извличане и предоставяне на знания за анализ и прогнозиране на бизнеса.

Специални технически стандарти улесняват обмена на данни между компаниите. Софтуерните решения на Електронният бизнес позволява интеграция на вътрешно - фирмени и междуфирмени бизнес процеси. Той може да се раздели на три категории:

1. Вътрешни бизнес системи:

1.1 Управление на взаимоотношения с клиенти.
1.2 Планиране на ресурсите на предприятието.
1.3 Системи за управление на документи.
1.4 Управление на човешките ресурси.

2. Фирмена комуникация и сработване:

2.1 VoIP (Пренос на глас и данни по интернет).
2.2 Системи за управление на съдържанието.
2.3 Електронна поща.
2.4 Гласови съобщения.
2.5 Уеб базирани конференции в реално време.
2.6 Цифрови работни потоци (Управление на бизнес процесите).

3. Електронна търговия – Business – to - business електронна търговия (B2B) или Business – to - customer електронна търговия (B2C):

3.1 Интернет магазини.
3.2 Управление на веригите за предлагане.
3.3 Онлайн-маркетинг (маркетинг в реално време).

Онлайн пазаруването е процесът, при който потребителите купуват продукти и услуги през интернет. Онлайн магазин, е-магазин, е-верига, интернет магазин, уебмагазин, онлайн верига или виртуална верига поражда физическа аналогия от покупки на продукти и услуги от продавачи на дребно и в търговски центрове – mall. Метафората с онлайн каталога също се използва по аналогия с каталозите за поръчка по пощата. Всички видове вериги имат уеб страници за продажба на дребно, включващи тези които имат и тези които нямат книжни каталози и рекламни материали.

Електронна доставка, покупка или продажба на стоки и услуги чрез интернет както и други информационни и мрежови системи като обмяна на електронни данни и фирмено планиране на ресурсите. В обичайния случай, електронната доставка позволява квалифицирани или регистрирани потребители да търсят купувачи или продавачи на стоки и услуги. В зависимост от подхода продавачите или купувачите могат да конкретизират разходите или да отправят цени. Транзакциите могат да бъдат инициирани и завършени. Онлайн покупките могат да бъдат придружени с ценови отстъпки и специални предложения. Софтуерът за електронна доставка прави възможни автоматизираните покупки и продажби. Участващите компании очакват да имат възможност за по-ефективен контрол върху инвентара, ограничавайки разноските за търговски представители и подобрявайки на производствените цикли. Електронната доставка се очаква да бъде интегрирана с тенденция към компютъризираното управление на вериги на предлагане.[14]

Друг иновационен процес е бизнес стратегия за подбор и управление на взаимоотношенията с клиентите (Customer Relatioinship Management – CRM). Предназначението на CRM системата е да събира цялата информация за клиентите и нейната централизирана обработка, а резултатите от анализа на тези данни се използват в маркетинга. Така, анализирайки поведението на клиентите по възрастови групи, специално положение и др., туристическата фирма може да предложи индивидуални продукти и услуги на всеки турист, съобразявайки се с неговите предпочитания. Нещо повече, CRM извлича знания за клиентското поведение (customer intelligence), чрез които се диференцират нуждите на всеки клиент и се повишава качеството на услугите, които той получава.

При Web базираните call-центрове връзката с клиентите се осъществява чрез e-mail, чат, телефонна и видео връзка в реално време. Особено ефективна е самонастройващата се система Web Collaboration, която позволява автоматично синхронизиране на браузърите на клиентите и туристическите агенти. Чрез нея агентите помагат на клиентите да разгледат туристическия уебсайт и да намерят необходимата им информация. Освен това те дават съвет, отговарят на въпроси и подпомагат вземането на решение от страна на клиента. На практика се получава една многопластова директна връзка с клиента в реално време, което осигурява високо качество на услугите, подобрява ефективността на бизнеса и се печелят лоялни клиенти.

Системите за планиране на фирмените ресурси (Enterprise Resource Planning – ERP) са ефективно софтуерно решение, което интегрира и покрива всички по-важни бизнес дейности, като планиране на произвежданите продукти и услуги, управление на запасите, проследяване на поръчките, управление на персонала, финанси, управление на проекти и др. Най-подходящи условия за тяхното използване съществуват в хотелиерството, като осигуряват бекофиса. Например системата „Fidelio", чрез която рецепционистът може директно да направи резервация по време и след телефонното обаждане на клиента. ERP системите могат да играят важна роля и при взаимодействието между туроператорите и хотелите, като в последните те се използват в по-голяма степен.

Електронното фактуриране (electronic invoicing – e – invoicing) представлява замяна на традиционните фактури с електронно генерирани и изпратени такива при осъществяването на компютърно опосредствани транзакции между продавачите и купувачите. Практически е-фактурирането се осъществява паралелно с електронните разплащания. Чрез него се намаляват разходите и на двете страни, участващи в транзакцията. Поради това, че процесът по създаването на електронните фактури е стандартизиран, електронните формуляри се обработват много по-бързо и се избягва станалото традиционно забавяне на класическите хартиени фактури. В днешно време почти всички фирми в туристическия сектор изпращат и поръчките си по електронен път. Особено голям акцент се очертава отново при туристическите агенции и туроператорите – 80% от тях практикуват онлайн доставките. Това е предопределено от природата на тяхната дейност, която е ориентирана към класическите посреднически функции между доставчиците на туристическите продукти и услуги и клиентите. Основно те се използват за намиране на нови доставчици в интернет пространството, за приканване на доставчиците да оферират пазарните цени, за изпращане на поръчки и др. Като цяло това рационализира и повишава прозрачността на пазара на туристическите продукти и услуги.

Най-голям ефект от тази дейност се достига посредством внедряване на системи за управление на веригата за доставки (Supply chain management – SCM). Мобилният бизнес е една нова и многообещаваща тенденция, която съчетава в едно цяло електронния бизнес, Интернет и безжичните технологии. Мобилността създава уникални предимства за туристическия бизнес свързани със свободата на движение с възможността за заявка на туристически продукти и услуги по време на пътуване. Мобилните компютърни устройства от тип PDA (персонален цифров помощник), smart phones (умни телефони) и др. имат способността да комуникират без кабели и да обменят данни по между си посредством всякакъв вид мрежи. В допълнение и с развитието на международния транспорт, вече новите и по-далечни дестинации стават достъпни по ефективен начин от финансова и времева гледна точка, което способства за развитието на международния туризъм на база повишаване трансперантността и мобилността на туристическия продукт. [2]

Успешната реализация на мобилните решения зависи до голяма степен от използването на средства за синхронизация с базата от данни и достъп до фирмените сървъри чрез безжична връзка. Друга важна характеристика на мобилната инфраструктура е защитата на предаваните данни и надеждната идентификация на потребителите.

От описаното по-горе разбрахме, че туризма е изключително обвързан с модерните технологии, но дали данните, с които оперираме са надеждно защитени и какви са заплахите за информацията и как би следвало да я опазим?

Гражданите и обществото разчитат на достоверна и надеждна информация в интернет пространството, но също така имат нужда от доверие и защита на персоналните данни, на дигиталното „аз“, както и на адекватна защита на човешките права и свободи в кибер пространството.

КИБЕР АТАКИТЕ В КОНТЕКСТА НА ТУРИЗМА

Кибер пространството предоставя практически неограничени възможности за развитие на общество и бизнеса, но нарастващата и необратима дигитална зависимост на основните функции и дейности на обществото ера, поражда нови значими рискове и заплахи. Умишлени или неумишлени действия могат да доведат до компрометиране на системи за управление и устройства, касаещи критичната инфраструктура или приложните системи, да възпрепятстват нормалното им функционира-

не или чрез нерегламентирано проникване да манипулират или извличат данни и информация. Начините за откриване или блокиране на тези възможности не са традиционни и изискват нова култура на взаимодействие между участниците в кибер пространството.

Съвременната икономика на знанието не само зависи, но и се развива все по-перспективно в нови направления свързани с интензивното използване на информационните технологии, софтуерни системи за управление, както и на ефективни процеси, базирани на дигиталните инфраструктури. Веригите за доставки (или веригите за създаване на стойност) работят чрез информационните си системи и през Интернет. Така към бизнес рисковете се добавят нови, кибер рискове с ключово значение, игнорирането на които може да доведе до катастрофални резултати.

Кибер атаките са директна заплаха за сигурността на гражданите и функциониране на държавата, икономиката, обществото, науката и образованието. Те могат да бъдат извършени от разстояние, с прости и ефективни механизми и минимални ресурси, да причинят значителни поражения с нанасяне на материални и дори човешки загуби. Кибер атаките нямат национални, културни или юридически граници. Рисковете и заплахите в кибер пространството са трудни за дефиниране поради сложността за определяне на източника на въздействие, целите и мотивите, бързото ескалиране на заплахата и трудно предвидимите перспективи за развитие, сложността и интензивността на съвременните комуникационни и информационни процеси, динамиката на логическите и физическите връзки и неопределеността на процесите. Сред най-сериозните деструктивни въздействия са тези от хибриден характер – комбинация от кибер атака и физическа атака, кибер атака целяща критичен кинетичен процес, кибер атака по време на природно бедствие или неизправност в критични системи. Еднакво засегнати от случайни кибер инциденти или целенасочени кибер атаки са публичният и частният сектор, както и цялото общество в Република България. [12]

Кибер атаките с най-голям потенциал за нанасяне на значителни щети са срещу различни критични инфраструктури (КИ) и уязвимости на техните системи за управление и комуникация. Нарушение в работата на общата и споделена критична комуникационна и информационна инфраструктура (ККИИ)оказва изключително въздействие върху обществото с непредвидими и потенциално катастрофални последици. Свързаността и зависимостта в кибер пространството позволяват пробивът в сигурността или дефект на една комуникационна и информационна система от даден сектор да доведе до каскаден ефект и отказ в други, отново със сериозни възможни последици и вреда на жизненоважни услуги.

Източници на организирани кибер атаки може да са държавни, военни и терористични организации, индустриален шпионаж, кибер престъпници. Мотивацията варира от икономически ползи до любопитство или хулиганство, демонстриране на надмощие и др. Значителна част от кибер атаките са престъпления с цел финансови облаги от различно естество. Кибер атаки се извършват и с цел тормоз, измама, разпространение на детска порнография, нарушаване на права на интелектуална собственост. По природа те са „асиметрични“ – с малки усилия и инвестиции могат да бъдат нанесени огромни поражения, при това не винаги предсказуеми. Кибер пространството е привлекателно за престъпниците поради отдалечения достъп, липсата на ефективно правораздаване по отношение на кибер престъпленията. Улесняващи фактори са анонимността, недостатъчните международни регулации, неинформираността и небрежността на собствениците на информационни системи и крайните потребители. Противодействието срещу кибер престъпността се усложнява от разнообразието на атаки, очаквани поражения и мотивация на хората, извършващи атаките. В послед-

ните години действията на кибер престъпниците са далеч по-изтънчени, поради придобитите значителни ресурси и капацитет, усъвършенстване на организационните и „бизнес“ структури, разпределението на роли и взаимодействието между криминални мрежи.

Източник на заплаха от особено голям мащаб са държави с тоталитарни режими и такива с неукрепнала демократична система, с доктрина за водене на информационни, кибер и хибридни войни. Тези държави, както и различни недържавни (или терористични) групировки, развиват специализирани способности за кибер тероризъм и водене на кибер войни чрез прилагане на целия набор от методи, въздействащи върху комуникационните и информационните системи за нарушаване на физическата, персоналната, информационната и комуникационната сигурност. [10]

Интернет се използва като основен канал за манипулирана информация и пропаганда, създаване на психоза, привличане на последователи, терористи и подпомагане на терористични организации. Кибер престъпността е цялостно хомогенизирано явление и всички изграждащи я компоненти са в неразривна взаимовръзка и взаимозависимост. [6]

КИБЕР СИГУРНОСТ НА ИНФОРМАЦИЯТА

Най-уязвимо звено в кибер сигурността продължава да е човекът. Небрежност, незнание или недоброжелателност могат да доведат до изтичане и злоупотреба с чувствителна информация, фирмени и държавни тайни, лични данни. Липсата или непълното реализиране и спазване на фирмени и организационни политики и адекватни мерки за информационна сигурност са основното улеснение за кибер престъпниците.

Кибер сигурността е състояние на кибер пространството определяно от нивото на конфиденциалност, интегритет, достъпност, автентичност и отказоустойчивост на информационните ресурси, системи и услуги. Кибер сигурността се основава на ефективно изграждане и поддръжка на активни и превантивни мерки. [13]

Координираното развитие на способностите на обществото чрез ангажиране на всички заинтересовани лица с цел противопоставяне на преднамерени или непреднамерени заплахи, адекватна реакция, овладяване и възстановяването от тях е ново ниво на зрялост, известно като кибер устойчивост. Високата кибер устойчивост подготвя обществото за „неизвестните неизвестни“ и включва защита и ограничаване на вредните последствия от разрушителни въздействия, максимално запазване и функциониране на жизнено важните дейности и услуги, и своевременно възстановяване. Постигането й изисква сигурност и надеждност на всички компоненти и активи на кибер пространството, или на цялата дигитална екосистема, на която разчитаме: информация, технологии, хора и съоръжения, както и специфични изисквания към дизайна и реализацията на комуникационните канали, системи и услуги, надеждната им свързаност и оперативна съвместимост. [3]

ЗАКЛЮЧЕНИЕ

Българското общество, като част от глобалното интернет семейство, се развива интензивно и уверено в цифровата и информационна ера. Държавата, бизнесът и гражданите разчитат на надеждното функциониране на комуникационните и информационните системи, технологиите и интернет средата, или на новото „пето“ пространство, в което вече живеем и се развиваме – кибер пространството. Дигиталните инфраструктури се превръщат от поддържаща среда в основен и критичен фактор за управлението и нормалното функциониране на всички ресурси и системи с национал-

но значение, на развитието на конкурентна и иновативна икономика, прозрачно управление и на модерно демократично гражданско общество. Същевременно, нарастващата и необратима дигитална зависимост на основните функции и дейности на обществото поражда нови значими рискове и заплахи. Кибер пространството носи нови уязвимости с непознат досега мащаб и потенциална сила на въздействие, които изискват повишаване на общата кибер култура и колективна кибер сигурност на цялото общество, прилагане на активни мерки за предпазване от известните видове заплахи (от небрежност до умишлени действия, използване на технически и човешки слабости), както и подготовка за „неизвестните неизвестни“ и постигане на кибер устойчивост във всички сфери.

България, като част от европейски и международни формирования, по силата на сключени такива споразумения е длъжна да отговори адекватно на стремежа за унифициране и синхронизиране на действията, от страна на коалициите. Тези действия засягат предимно функциите на институциите и съпровождащата ги нормативната уредба. Бързо променящата се среда за сигурност и развитието на информационните технологии улесняват битовите потребности, но в същото време и създават изключително големи заплахи за сигурността на информацията. За да защити позицията си на страна – партньор и по отношение на киберпространството, България изпълнява предписанията залегнали в стратегията по киберсигурност на Европейския съюз и създаде „Национална Стратегия за Киберсигурност – Киберустойчива България 2020“. Тя е в действие от 2016 г. и има цели и мерки за развитие в девет ключови области: [4]

- Установяване и развитие на националната система за кибер сигурност и устойчивост;
- Мрежовата и информационна сигурност – фундамент на кибер устойчивостта;
- Защита и устойчивост на дигитално зависимите критични инфраструктури;
- Подобряване на взаимодействието и споделянето на информация между държава, бизнес и общество;
- Развитие и подобряване на регулаторната рамка;
- Засилване на противодействието на кибер престъпността;
- Кибер отбрана и защита на националната сигурност;
- Повишаване на осведомеността, знанията и компетентностите и развитие на стимулираща среда за изследвания и иновации в областта на кибер сигурността;
- Международно взаимодействие – кибер дипломация и оперативно взаимодействие;
- Изпълнението на целите и набелязаните мерки ще бъдат развити в План с пътна карта съобразно набелязаните фази за развитие.

Основните фактори за успешното и ускорено постигане на целите са:

- Обвързаност с приоритетите и целите на Програмата на правителството за стабилно развитие на Република България (2014-2018 г.) и националните секторни стратегии;
- Идентифициране и ангажиране на всички заинтересовани страни и изграждане на модел и механизъм за координация на стратегическо, политическо, оперативно и техническо ниво, както и ефективна платформа за споделяне на информация и колективен отговор;

- Ефективно проектно управление за реализиране на набелязаните мерки и ясна оценка на постигнатите резултати и способности;
- Активно международно взаимодействие – използване опита на водещите партньори в ЕС и НАТО, активно включване в партньорски програми и инициативи, и активизиране на партньорствата в региона за изграждане на общ капацитет и способности.

ЛИТЕРАТУРА

1. Илиева, Елена. 2018. Китайските туристи и технологичните иновации – възможности за преодоляване на пречките пред посещението им в България, Сборник доклади от международна научна конференция „Туризмът и иновациите“ по случай „55 години Колеж по туризъм – Варна“, изд. „Наука и икономика“ към ИУ – Варна, Варна, с. 286.
2. Илиева, Елена. 2018. Характеристика на китайския международен турист. Академично списание „Управление и образование“ към Университет „Проф. д-р Асен Златаров“, Бургас, т. XIV (2), с. 35
3. Николова Д., Божилова М., „Аспекти на киберсигурността“, http://cio.bg/3964_aspekti_na_kibersigurnostta.
4. Петкова – Георгиева, Ст., Анализ на факторите, водещи до повишаване ефективността на дейността на аутсорсингови производства, списание „Известия на Съюз на учените”, стр. 122-130, Варна, 2017.
5. Петкова, Ст., А. Янакиева Балансираната система от показатели (БСП) като съвременен метод на управление в туристическото предприятие, 2012, Академично списание „Управление и образование”, том VIII(1), International Scientific Conference „Management and Education”, Burgas, Bulgaria, стр.135-138, ISSN 13126121.
6. Стефанова, С., Лекционен материал по „Психология на девиантното поведение“, ЮЗУ „Неофит Рилски“, Благоевград, 2006.
7. Янакиева, А., Стратегически подход за оценяване конкурентоспособността на здравно-възстановителните организации, 2017 г., Академично списание „Управление и образование”, том XIII (2), Международна научна конференция „Образование, наука, икономика и технологии” на Университет „Проф. д-р Асен Златаров”, Бургас, стр. 176 - 181, ISSN 13126121.
8. www.gartner.com
9. www.cibersecurity.com/cyber-security-market-report
10. http://ncs.nlcv.bas.bg;
11. www.strategy.bg/StrategicDocuments/, Национална *стратегия за киберсигурност* „Кибер устойчива България 2020”
12. http://www.cybercrime.bg/bg;
13. https://www.consilium.europa.eu/ media/30803/qc7809568bgc.pdf;
14. http://www-it.fmi.uni-sofia.bg/courses/BonI/chapter2.html)