СОФИЙСКИ ФОРУМ ЗА СИГУРНОСТ
SOFIA SECURITY FORUM

ЦЕНТЪР ЗА РАЗВИТИЕ НА ЧОВЕШКИТЕ РЕСУРСИ

Erasmus+

ПРОУЧВАНЕ ЗА СИГУРНОСТТА НА МЛАДИТЕ В ИНТЕРЕТ

Мартин Чорбаджийски

Клаудия Чочулова,

Софийски форум за сигурност

Септември, 2015

ПРОУЧВАНЕ ЗА СИГУРНОСТТА НА МЛАДИТЕ В ИНТЕРНЕТ

Настоящото проучване има за цел да обърне внимание на три ключови аспекта: какви са най-често срещаните рискове и заплахи за сигурността на младите в интернет, защо младите хора са особено застрашени в интернет и какви са практиките в някои европейски държави за повишаване на сигурността на младите хора във виртуалното пространство. Изследването е извършено от екип на Софийски форум за сигурност в рамките на проекта *„Сигурностт@ на младите в интернет, предизвикателствата на киберсигурността“*, който се осъществява по Програма Еразъм+ , финансирана от ЕК и със съдействието на Центъра за развитие на човешките ресурси. Докладът се позовава не само на опита на отделни европейски държави, но и на различните инициативи, осъществявани на ниво ЕС. Направен и кратък обзор на практиките е и политиките в Република България, като се правят съответните изводи. В рамките на целия проект ще се изготвят препоръки за повишаване сигурността на младите в интернет.

СЪДЪРЖАНИЕ

РИСКОВЕ И ЗАПЛАХИ ЗА МЛАДИТЕ ХОРА В ИНТРЕНЕТ

Държавната комисия по сигурността на информацията използва следните определения за риск и заплаха, които ще приемем и ние за настоящото изследване. Заплахата е опасност, възможност за поява на нещо неприятно, лошо. Закана да се причини някому нещо неприятно, зло. При риска няма определено предварително време за настъпването му. Дори да бъде установен достатъчно рано, той си остава принципно невъзможен за неутрализиране[1] . Редица проучвания и проекти в областта на киберсигурността и сигурността обръщат внимание на следните рискове и заплахи за младите хора в интернет като най-сериозни и/или най-често срещани:

- *Порнография, сексуални престъпления и насилие*

Все повече млади хора биват излагани на този риск. Интернет все по-често се използва от потенциални и реални извършители на сексуални престъпления за подготовка на сексуални злоупотреби с деца, по-специално чрез сприятеляване с цел сексуална злоупотреба и детска порнография. Младите хора могат да станат жертва на т.нар. сексуални хищници, които в днешно време се насочват към социалните мрежи и примамват младежи, демонстрирайки привиден интерес към техните хобита, любими изпълнители, предавания и пр.[2] Така например педофили лесно могат да се доберат до лична информация- адрес, имена, профили, след което изпращат изображения и видео, които имат сексуално съдържание.

Порнографията и особено детската порнография е друг съществен риск, който може да има дълготрайно въздействие върху психиката на детето или тийнейджъра. Освен прякото негативно въздействие върху психиката и развитието на младите хора, сайтове с порнографско съдържание често крият зловреден софтуер, който атакува компютрите при разглеждане на тези сайтове.

---

[1] „Рискове за интересите на Република България в областта на защитата на класифицираната информация, Държавна комисия по сигурността на информацията, с.3”, http://www.dksi.bg/NR/rdonlyres/5DB28C7E-7B2B-4DBE-894D-759B7329D913/0/Riskove_za_za6itata_na_KI.pdf (Прегледан на 08.09.2015г.)

[2] Kam, K., 4 Dangers of the Internet, page 3 - http://www.webmd.com/parenting/features/4-dangers-internet (Прегледан на 08.09.2015г.)

Онлайн насилието също е вече широко разпространено и също може да има дълготрайни неприятни последици за младите хора, особено поради опасността от повтаряне на видяното насилие.

- *Кибертормоз*

Кибертормозът е съвкупно понятие за действия, които могат да навредят на даден индивид в интернет и включват заплахи, злоупотреби, следене или друго агресивно поведение, което е продължително във времето. Кибертормозът може да включва обидни реплики, публикуване на снимки в интернет без разрешението на притежателя им, споделяне на видеоклипове, които могат по някакъв начин да накърнят достойнството и доброто име. Противодействието срещу тази заплаха е особено трудно, тъй като извършителят остава неизвестен, а често използва идентичността на своя жертва и извършва кибертормоз от нейно име (Kam, K., 4 Dangers of the Internet). Кибертормозът може да има дълбоки последици върху психическото състояние на детето или тийнейджъра.

- *Радикализация чрез интернет*

Разпространението на радикални идеи или призиви към радикални действия, насочени срещу отделни хора или групи е все по-често явление. Свидетели сме на разпространение на радикални идеологии, насочени срещу малцинствени или религиозни социални групи. Интернет позволява и бързата организация на неограничен брой хора за извършване на радикални противозаконни действия.

Появата на т. нар. Ислямска държава и засилването на други терористични групировки даде тласък на този вид заплаха и доведе до стартирането на интернет кампании за привличането на бойци и симпатизанти. Това става чрез различни мултимедийни материали или обещания за заплащане и просперитет. Използвайки интернет терористите се насочват най-често към деца и юноши от проблемни семейства, т.нар социални аутсайдери, маргинализирани младежи или имигранти и бежанци. Тази заплаха включва и десният радикализъм- дискриминация на мюсюлмани и други малцинства, което се превръща във все по-голям проблем.

Наред с радикалния ислямизъм наблюдаваме и ръст на неговото отрицания - антиислямския радикализъм, набиращ сила в много европейски държави.

- *Фишинг*

Това е широко използван похват от компютърни престъпници за получаване на важна информация. Те просто създават съобщение или интернет сайт, които "претендират", че са добронамерени, като приканват да се въведе важна лична информация. При фишинга измамници разпращат електронна поща, която претендира, че идва от почтена компания, и се опитва да убеди получателя да даде важна лична или финансова информация. Електронното съобщение обикновено моли да се изпрати в отговор или да се въведете на уебсайт, към който има връзка. Тези данни, например потребителски имена, пароли и номера на кредитни карти, после се използват от измамниците, за да се получат пари или услуги от името на пострадалия.[3]

- *Кражба на информация и използване на зловреден софтуер*

Кражбата на информация е сериозна заплаха, тъй като може да доведе до кражба на идентичността в интернет, в който случай крадецът се представя за своята жертва и по този начин безнаказано извършва престъпления /в реалното и във виртуалното пространство/. Ако не се вземат своевременни мерки (като например докладване за откраднат профил до компетентните органи или администратори на съответния уебсайт), престъпленията могат да се припишат на жертвата. Младежите често не обръщат внимание на последиците от споделянето на лична информация в киберпространството и пренебрегват декларациите за поверителност при използването на онлайн услуги. В съчетание с неприлагането на настройките за поверителност, споделената от тях лична информация е лесна плячка за различни видове зловреден софтуер, като тя може да бъде директно откраднатa или да бъде изтеглена без знанието на нейния собствени/автор за това. Тази информация може да се използва за проникване в устройствата за достъп до интернет (компютър, лаптоп, телефон и др.) и така злонамерени лица да се доберат до още по-голямо количество информация като лични снимки, пароли за уебсайтове, кодове на кредитни и дебитни карти (особено ако детето/тийнейджъра и родителя използват едно и също устройство).

[3] „Фишинг", http://www.cybercrime.bg/bg/internet (Прегледан на 24.09.2015г.)

- *Кражба на самоличност*

Извършва се, когато някой използва личните Ви данни като име и фамилия, ЕГН, осигуровки, номера на кредитни/дебитни карти или друга идентифицираща Ви информация без Вашето знание и съгласие, за да извърши измама или други престъпления. [4] В много случаи кражбата на самоличност се установява изключително късно, когато са направени непоправими щети на личността или имуществото.

- *Игри, съдържащи насилие*

Сред младите все по-популярни стават видео игрите, които съдържат насилие. Същевременно те крият риска от приемането на виртуалната реалност за действителна и пренасянето на виртуалния свят в реалния. Това може да доведе както до проблеми в общуването и социална изолация, така и до опити за пресъздаване на виртуалните изживявания. Специалисти все повече отчитат, че игрите, съдържащи насилие, играят важна роля в радикализирането на младежите и приобщаването им към различни терористични и криминални групировки.

- *Онлайн финансови измами и други финансови рискове*

Все по-голям е броят на пазаруване и разплащане за различни услуги чрез интернет. Въпреки че големите компании обръщат сериозно внимание върху сигурността, не са изключени ситуации, при които хората попадат на неистински търговци. Рискът се крие в извършването на самата транзакция и постигането на различен от очаквания резултат-заплатеният продукт или не се получава, получава се в занижено качество или количество или лицето се оказва обвързан с нежелан абонамент, за който плаща повече. Примерите в това отношение могат да бъдат многобройни.

Сред другите финансови рискове следва да се отбележи незаконният хазарт, което може да се отрази негативно на семейния бюджет, може и да се пренесе в реалния живот като превърне младия човек в редовен посетител на казина или да доведе до неговата задлъжнялост в резултат на онлайн играта. Собствениците на хазартни сайтове физически се намират в офшорни зони; в резултат на това операторите могат да променят, преместват или напълно да отстраняват сайтовете си в рамките на няколко минути. Тази възможност позволява недобросъвестните оператори да вземат номера на

[4] „При кражба на лични данни“ - http://www.cybercrime.bg/bg/internet/f04ff8/ (Прегледан на 24.09.2015г.)

кредитни карти, както и пари, депозирани в сметките на играчите, след което да закрият дейността си.[5]

- *Хакерство сред младите*

Все по-популярна сред младите хора се превръща „професията“ хакер. Деца и юноши намират забавление и удоволствие, но най-вече усещане за предизвикателство при проникването в сайтове, кражбата на кодове, данни и пр. По този начин те се превръщат в част от проблема и излагат на риск свои връстници. В повечето случай това е невинна игра и не се получава сериозно увреждане на личността или собствеността, но има случаи на сериозни негативни последици.

- *Плагиатство*

Плагиатството е представянето на нечии мисли, идеи за свои собствени. Съществува целенасочено плагиатство, но в някои от случаите то е следствие от липсата на знания за правилата по използването и цитирането на чуждия труд. Последствията от плагиатството могат да бъдат изключване от образователни институции, съд или глоба. За да се предотвратят неблагоприятните последствия, младите хора трябва да бъдат запознати с правилата за използване на чуждия труд при техни разработки. Наблюденията показват, че това е изключително силно разпространено явление сред студентите, като повечето от тях не осъзнават или нямат информация, че неправомерното използване на чужд интелектуален продукт е престъпление.

- *Рискове при запознанства в интернет*

Рискът тук произтича от неспазването на определени правила, като например да не се споделя незабавно личната информация, уверение, че насрещната страна е такава, за каквото се представя (идентичността на другата страна, много престъпници скриват реалната си възраст, пол и намерения, възползвайки се от доверието на младите хора), срещата да се проведе на публично място, където има много хора и др.

- *Пренебрегване на правилата за онлайн комуникация*

Младите хора често не взимат необходимите мерки, за да гарантира своята сигурност при онлайн комуникация. Рискът е свързан с липсата на предпазливост, а донякъде и липса на култура за защита при онлайн комуникация. Това може да доведе до

[5] Незаконен хазарт - http://www.cybercrime.bg/bg/internet/3ad1da/

злоупотреба с лична информация, кражба на снимки, видео, нежелани контакти, попадане на неподходящо съдържание и др.

Изброените по-горе рискове са само една малка част от рисковете и заплахите в интернет. Интернет може да създаде рискове или чрез него традиционните рискове да се задълбочат. Ние считаме, че е необходимо да се засили общественото внимание към тези опасности. Те са многобройни и разнопосочни и същевременно се развиват бързо, еволюират и възникват все по-изобретателни методи, чрез които се застрашава сигурността на младите в интернет. Нека да не забравяме, че интернет създава изключителни възможности за получаване и обмен на информация, за извършване на различни дейности, които ни обогатяват или правят живота ни по-лесен, но в същото време той крие и рискове, които ние трябва да познаваме за да се защитим. Това се отнася най-вече до младите хора.

ЗАЩО МЛАДИТЕ СА УЯЗВИМИ

Опасностите, които интернет пространството крие могат да засегнат всички. Защо тогава младите са особено уязвими към тях?

Никога преди младите хора не са имали достъп до толкова много информация и до толкова различен набор от дейности на едно място. Може да кажем дори, че те „живеят“ в интернет. Независимо дали говорим за деца или тийнейджъри интернет е важна част от техния живот, а като такава много от представите им за света и живота могат да се оформят именно там. В интернет те общуват, споделят информация, запознават се с нови хора, градят социален имидж. От друга страна това, което се случва в интернет се отразява на живота им и преживяванията онлайн могат да имат ефект върху житейското им развитие. Младите хора са по-склонни към нови контакти, към нови запознанства, по-доверчиви са, а често не са запознати с рисковете, които интернет крие или с това как да гарантират своята безопасност онлайн.

Влошената семейна среда е един от факторите за уязвимостта на младите в интернет. Ако те не се разбират добре със своите родители, не споделят с тях своите преживявания и се стремят да ги държат напълно настрана от своя „живот“ онлайн,

това повишава вероятността младите хора да бъдат изложени на рискове. В такива случаи самите те са по-склонни към рисково поведение, тъй като чувстват родителите далеч от себе си и отказват да чуят съветите им.

Социалната изолация е друг фактор, който допринася към уязвимостта на младите. Ако те не чувстват, че „принадлежат“ в училище, сред своите приятели и семейство, ако редовно са обект на нападки от свои връстници и търпят лошо отношение, те търсят утеха в интернет, където могат да общуват с напълно непознати хора, които не знаят нищо за тях. Тук отново стават по-склонни към рисково поведение и е по-вероятно да пренебрегнат правилата за сигурност. [6] [7]

Нека да вземем за пример тийнейджърите. Те са индивиди, които започват да изграждат свой личен живот и дълготрайни социални контакти, но имат стремеж да водят този живот независимо от своите родители. Всъщност това е процес, при който те търсят своето място в обществото и своята идентичност. В много случаи се сблъскват с обществени нагласи, които не им импонират. Получават се конфликти между установените принципи в обществото, от една страна, и желанието, амбициите на младежите, от друга. Голяма част от хората, които се радикализират го правят именно на тази основа – те се чувстват неразбрани, не намират място в обществото, не споделят неговите норми и смятат, че то ги потиска. Лица с престъпни намерения, използващи интернет, се възползват от това и атакуват именно тази част от съзнанието на младите хора, като се представят за приятели, разбиращи и симпатизиращи на намеренията и целите им, насърчаващи ги да не слушат родителите си. Постепенно, стъпка по стъпка, те печелят доверие, което улеснява извършването на избраното от тях престъпление.

Друга причина се състои в емоционалната уязвимост. Много деца и юноши се чувстват несигурни, особено когато са поставени в условията да заемат по-ниско социално положение сред своите връстници. Те често изпитват проблеми у дома, което поражда у тях нуждата да търсят тръпка, ново усещане, риск, какъвто може да е случаят при срещата с непознат от интернет. Около 30% от децата в ЕС имат контакти, с които са се запознали онлайн, а 23% от тях се запознават с пет или повече души. Девет процента от

[6] „What can make young people vulnerable online”- http://parentinfo.org/article/what-can-make-young-people-vulnerable-online (Прегледан на 25.09.2015г.)
[7] „Vulnerable young people, social media and e-safety” - http://www.saferinternet.org.uk/content/childnet/safterinternetcentre/downloads/Research_Highlights/UKCCIS_RH_19_MPP.pdf (Прегледан на 25.9.2015г.)

тези деца са се срещали на живо със свои онлайн познати[8] (Smahel, D. Helsper, E. J., Barbovschi, M. & Dedkova, L., 2012). От друга страна същият риск се отнася и за т.нар. „лидери" на социалните групи или „популярните", за които статистиката показва, че рискуват запознанства на живо поради голямата си увереност.[9] Към списъка с причини следва да добавим и начина, по който в интернет се използва интересът на младите към игри, гатанки, предизвикателства и задачи. В много сайтове с игри често може да се открие зловреден софтуер, а една от тактиките на престъпниците включва привличане на вниманието чрез сложни задачи и загадки. В заключение по този аспект следва да отбележим, че причините за уязвимостта се крият както в самия живот, който младите водят, така и в степента им на запознатост със заплахите, които киберпространството крие.

ЕВРОПЕЙСКАТА ПРАКТИКА

Посочването на рисковете и причините за уязвимостта на младите в интернет логично води към следващия въпрос, а именно какви са добрите практики в справянето с тези проблеми. В Европа Държавите членки на ЕС са възприели различни подходи и прилагат многобройни решения, ето и някои от тях:

В Латвия впечатление прави проектът Net-Safe[10], който препоръчва обучението на младите хора по безопасност в интернет да се съчетае с атрактивни за тях дейности. В сайта на проекта посетителите могат да свирят на пиано, да решават забавни и същевременно образователни тестове. Сред една от интересните и иновативни идеи е създаването на форум, в който младите могат взаимно да се образоват по въпросите на интернет безопасността, да споделят полезни идеи и информация, а също така и неприятни преживявания, от които техни връстници да се учат.[11]

[8] Smahel, D. Helsper, E. J., Barbovschi, M. & Dedkova, L., 2012 , „Meeting Online Strangers among European Children" - http://www.cyberpsychology.eu/team/storage/Smahel-2012-Bergen.pdf
[9] Ibid
[10] „Net Safe Project" - http://www.canee.net/latvia/net_safe_project
[11] http://www.ebaltics.com/00704598

Доклад за рисковете и безопасността на младите в интернет във Франция показва, че ролята на родителите в страната е голяма и те са първият източник, към който младите хора се обръщат за помощ и съвети в интернет.[12] Словакия представлява интересен пример, тъй като един от основните рискове се крие в социалните мрежи, риск илюстриран от факта, че 81% от словашките тийнейджъри използват Фейсбук всеки ден. В социалните мрежи младите хора споделят твърде много лична информация и за тази цел е създаден интернет порталът Bezpečný /Безопасен/[13], фокусиран и върху елиминирането на заплахи за онлайн сигурността. Сайтът е посветен на деца и родители и съдържа различни практически съвети относно начина за справяне и избягване на проблеми в интернет. В съответствие с авторите на този уебсайт, публикуването на истинско име или фамилия, домашен / училищен адрес и публикуването на снимки може да доведе до физически нападения и тормоз. Обръща се внимание на „статусите" в социалните мрежи, описващи чувствата и дейностите на младите потребители като например приготвяне на багаж за почивка, чакане на летище, пристигане на определеното за почивка място. В резултат на това, са описани много случаи на домашни обири след споделянето на такава информация онлайн. Словашкият опит посочва още, че родителите трябва да са основният източник на информация, а незаинтересоваността им към проблема на онлайн безопасността сама по себе си представлява риск за техните деца.

От тази гледна точка почти всички проучвания и проекти в ЕС на тема безопасност и сигурност в интернет препоръчват родители и деца взаимно да разговарят по тази тема, а родителите да упражняват контрол в различна степен върху заниманията на децата онлайн. Препоръчват се също така съвместни обучения между родители и деца, които от ранна възраст да повишат своята култура на сигурност и така да се установи връзка на доверие между родител и дете по отношение на сърфирането в интернет. Редица проучвания, съфинансирани от институциите на ЕС, сочат, че според родителите някои от най-добрите практики в повишаване на интернет безопасността са обученията на децата и юношите в училище, по-достъпна и разбираема информация, която да запознае самите родители с рисковете, обучения и курсове за самите родители, които да бъдат организирани от правителствата, местните власти или НПО-та.

[12] Catherine Blaya and Seraphin Alava, Risks and safety for children on the internet: the FR report, page 56 http://eprints.lse.ac.uk/46442/1/FranceReportEnglish.pdf (Прегледан на 04.09.2015г.)
[13] Bezpečný Internet. (2015). Sociálne siete. Nebezpečenstvá sociálnych sietí. http://www.bezpecnyinternet.sk/ (Прегледан на 05.09.2015г.)

В Обединеното кралство се обръща сериозно внимание на мнението на младите хора по отношение на сигурността в интернет, което има принос към политиките, които се развиват в тази област и специфичните проблеми, които могат да възникнат. Акцентира се върху ролята, която училищата и университетите имат в запознаването на деца и юноши с въпросите за сигурността в интернет и е създаден специален сайт с практични съвети за организации различни от училища и университети, които работят с млади хора (вж. http://www.onlinecompass.org.uk/).

В Германия филтрирането на определено онлайн съдържание е нещо, зад което застават мнозинството родители. Много немски мобилни оператори са създали софтуер, посветен на родителския контрол и същевременно са подписали различни кодекси, свързани със защитата при сърфиране от мобилни устройства. [14]

Голямо е значението, което се отдава на различните инструменти за докладване, чрез които може да се реагира на неподходящо за деца съдържание. Такива инструменти трябва да бъдат максимално опростени, за да могат да се използват както от родители, така и от деца. Подчертава се и уникалната позиция, в която IT компаниите и интернет доставчиците се намират за развиване на интернет сигурността и помощта която могат да окажат на своите клиенти. Някои IT компании разполагат със специален софтуер за родители, който да ги запознае с опасностите в интернет или да им помогне при наблюдение на онлайн дейността на децата им.

Обект на фокус са и процедури, чрез които съществуващите закони по отношение на киберпрестъпленията се прилагат, като ЕС се фокусира върху сътрудничество на ниво държави членки и на глобално равнище, тъй като киберпрестъпленията често пресичат границите. В държави като Франция, Холандия, Великобритания и Швеция например вредите, нанесени на деца посредством онлайн контакти, са обект на наказателно преследване.

Европейският съюз взема мерки за подобряване на сигурността в интернет като насърчава саморегулацията и съвместната регулация на интернет пространството и неговата безопасност чрез публично-частно партньорство с IT компании, интернет

[14] Global Resource and Information Directory. (September, 3, 2014). Germany. Country Profile, para. 6- http://www.fosigrid.org/europe/germany (Прегледан на 02.09.2015г.)

доставчици и социални мрежи, които доброволно се ангажират с тази задача.[15] Тежестта на превантивните мерки срещу кибертормоза нараства все повече, тъй като голяма част от него се извършва от деца или тийнейджъри и затова е важно в училищата да се работи по този проблем и да се насърчава отделянето на повече време за децата днес, за да не се превърнат в престъпници утре.

Политиките на правителствено ниво трябва да дадат основната насока за развитието на сигурността на младите в интернет. Някои държави членки възприемат цялостни национални стратегии за сигурността на децата в интернет (Великобритания) , други залагат на институцията на омбудсмана за защита правата на децата (Унгария и Полша) или са създадени специални органи, които се занимават с предпазването на младите в интернет и сътрудничат тясно с органите на реда, медиите, мобилните оператори и интернет доставчиците.

В много европейски училища програмата за обучение по онлайн сигурност е съобразена с възрастта на учениците. Във Великобритания много деца се канят на форуми, посветени на онлайн рисковете и политиките за противодействие, за да дадат своето мнение, т.е. на тях се гледа като на активна заинтересована страна. Младите хора, успешно преминали обучения за безопасност в интернет се привличат за работа със свои връстници, които все още не са запознати с тези въпроси.

В ЕС голяма роля играят неправителствените организации, които често участват във формирането на правителствените политики и спомагат за засилването на международното сътрудничество по интернет безопасността.

Много полезен е опитът на мрежата InHope[16], обединение на различни неправителствени организации, които държат отворени горещи телефонни линии, чиято крайна цел е премахването на сексуалния тормоз над деца в интернет и сайтове с такова съдържание. Мрежата действа както на ниво ЕС, така и в глобален мащаб. Друга подобен източник е т.нар. мрежа Insafe[17], организатор на Деня за безопасен интернет, който се провежда всеки февруари и се състои в различни дейности, промотиращи безопасността на младите хора в интернет. В мрежата Insafe си сътрудничат НПО-та, образователни институции, органи на реда, бизнес организации и родители.

[15] Safer Social Networking Principles for the EU, February 10, 2009- https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf (Прегледан на 10.09.2015г.)
[16] http://inhope.org/gns/home.aspx (Прегледан на 10.09.2015г.)
[17] http://www.saferinternet.org/ (Прегледан на 10.09.2015г.)

Европейският парламент е наясно с опасностите, които онлайн средата крие за децата и на интернет страницата InHope се акцентира върху подчертания от европейските депутати факт, че над 80% от жертвите в киберпространството са деца по-малки от 10 години. Ето защо ЕП положи усилия за приемане на резолюция относно безопасността на децата в киберпространството в началото на тази година. Сред конкретните стъпки, препоръчани в съответствие с инициативата на Европейския парламент[18] е снабдяването на Европол и националните правоприлагащи органи с необходимите средства, човешки ресурси, разследващи правомощия и технически възможности за сериозно и ефективно съдебно преследване, разследване и изправяне пред съд на извършителите на киберпрестъпления, разработване на нови високотехнологични способности, които да помогнат при анализирането на огромни количества изображения, свързани например с малтретирането на деца, включително материали, скрити в т.нар. „тъмна мрежа“(Dark web), призоваване страните от ЕС, които все още не са транспонирали Директивата от 2011 г. относно борбата със сексуалното малтретиране и сексуалната експлоатация на деца и детската порнография в националните си закони да го направят.

Европейската стратегия за интернет сигурност препоръчва засилване на интернет сигурността на ниво местна власт и създаване на местни е-правителства, като се прилага принципът на продължителното обучение на служителите, тъй като поради бързите технологични промени, методите за измама се подобряват[19]

БЪЛГАРИЯ И ВЪПРОСЪТ ЗА СИГУРНОСТТА НА МЛАДИТЕ В ИНТЕРНЕТ

В България все още не съществува стратегия, насочена към преодоляване на рисковете за сигурността на младите хора в интернет. Компетенциите в тази сфера са разпределени между различни държавни органи, но това е още една предпоставка да се размива отговорността.

[18] „European Parliament calls for crackdown on online child sexual abuse” - http://www.inhope.org/tns/news-and-events/news/15-03-12/European_Parliament_calls_for_crackdown_on_online_child_sexual_abuse.aspx (Прегледан на 12.09.2015г.)

[19] European Internet Security Strategy, page 14 - http://cor.europa.eu/en/documentation/studies/Documents/european-internet-security-strategy-2013.pdf (Прегледан на 04.09.2015г.)

Органите, които основно се занимават с въпросите на безопасността на децата в интернет е Държавната агенция за закрила на детето, Министерството на транспорта, информационните технологии и съобщенията, а също така и ГДБОП- МВР. Нека не забравяме, че основата в борбата с престъпленията, включително и тези, свързани с интернет, е превенцията. Добра практика в това отношение е сайтът cybercrime.bg, който освен всичко друго съдържа и полезни съвети към родители за безопасната работа на децата им в интернет. Тези съвети включват използването на интернет семейно, т.е. комуникация между дете и родител относно посетените сайтове, опасностите, които крият сайтовете за запознанства и др.[20] Дейност по въпроса за сигурността на младите в интернет извършва и неправителствения сектор, като сайта safe.teacher.bg, Фондация „Партньори- България“, а в страната също се провежда международният Ден за безопасен интернет[21]. Трябва да се отбележи дейността на Националният център за безопасен интернет, който обединява държавния сектор, бизнеса и неправителствени организации в опит да превърне интернет в едно по-безопасно място и да се предотвратяват киберпрестъпления. Друг пример от кампанията на Микрософт България „НетАларма“, в рамките на която ученици от гимназиите в цялата страна съставиха първия „Манифест за безопасен интернет“. Кампанията е осъществена със сътрудничеството на членовете на Детския съвет към Държавната агенция за закрила на детето и младежката асоциация “Български детски и младежки парламент” . Чрез своя Манифест, учениците не само споделят какво е важно за тях в Интернет, но и дават идеи за това какви етични и професионални норми е необходимо да се спазват от страна на потребителите[22].

По данни на Националния статистически институт около 83% от българските граждани на възраст между 16 и 24 години редовно използват интернет. Ако прибавим към тази цифра децата под 16 години, тогава цифрата може да скочи до 90%, както стана ясно на провелата се кръгла маса по въпросите на защитата на децата в интернет пространството, организирана от Министерството на транспорта, информационните технологии и съобщенията. От друга страна проучване, извършено за Европейската комисия от мрежата European Schoolnet и Университетът в Лиеж показва, че българските осмокласници са сред най-неуверените в ЕС по отношение на своята

[20] „Съвети към родителите” - http://www.cybercrime.bg/bg/exploitation/aee587/ (Прегледан на 24.09.2015г.)
[21] http://www.saferinternetday.org/web/bulgaria/home (Прегледан на 24.09.2015г.)
[22] Ученици от цялата страна съставиха първия „Манифест за безопасен интернет” - https://www.microsoft.com/bulgaria/press/news_15122010.mspx (Прегледан на 25.09.2015г.)

онлайн безопасност. Процентът на увереността обаче бележи растеж в 11 клас, като стига средното за ЕС ниво.[23] Основните рискове за младите хора в България са опасността от скъсване с реалността и пристрастяване към видеоигрите, манипулация следствие на онлайн запознанства, експлоатация на детски труд. Като мерки за противодействие на тези рискове се организират най-вече срещи с ученици, обучителни курсове за родители и различни рекламни кампании, целящи повишаване културата на сигурност в интернет.

Банковият сектор в България също е ангажиран със сигурността в интернет и в частност по отношение на електронното банкиране. На сайтовете на банките могат да се открият детайлни правила за сигурността при извършване на финансови операции онлайн, което е от особено значение за младите хора, които се запознават с онлайн услугите на банките. Сред най-важните препоръки са работа единствено с личен компютър, редовно обновяване на софтуера, проверка на страницата за интернет банкиране, която трябва да започва с https (което означава, че сайта притежава специален сертификат за сигурност (SSL certificate или новият TLS certificate), гарантиращ, че връзката със страницата е кодирана, тази препоръка важи и за работа с всякакви други сайтове), въвеждане на допълнителни потребителски идентификатори под формата на кодове, чрез които извършената транзакция да се потвърждава с безплатен SMS, съхранение на такива кодове и друга чувствителна информация на физически носител, а не на компютъра или друго устройство с достъп до интернет.

Всички посочени по-горе мерки или добри практики в България са реализирани по-скоро като инициатива на отделни министерства или организации /основно неправителствени/. Прави впечатление липсата на единно виждане и политика в областта на защита на младите хора в интернет, която да обхване както обучението на самите млади хора, така и предоставяне на повече информация на всички лица и институции, отговорни за тяхното израстване. Естествено, трябва да има и ясна визия за ролята и мястото на държавата н този процес, защото интернет се само че дублира, но понякога и замества реалността, в която досега изцяло живеехме.

[23] Survey of Schools, ICT in Education, p.104-105 - https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/KK-31-13-401-EN-N.pdf (Прегледан на 03.05.2015г.)

ИЗВОДИ

Младите действително остават най-уязвимата група в интернет. Те са склонни да възприемат нови неща много по-бързо от останалата част от населението, а същевременно са уверени в способността си да се справят с потенциални рискове. От друга страна интернет предоставя неограничени възможности за комуникация и информация, но паралелно с тази неограниченост съществуват рискове и заплахи, които се развиват много бързо (появяват се нови, старите се усъвършенстват), а техни жертви най-често стават именно децата и юношите. За да се преодолее тази уязвимост е необходим комплексен подход при формиране на политиките.

Семейството и образователните институции са най-близко до младежта и затова следва да имат водеща роля при запознаването им с опасностите в интернет. Това разбира се не би било достатъчно без усилията на държавата, която да даде насоките за гарантиране на киберсигурността и гражданския сектор, който да допринесе за развитието на тези насоки чрез своя иновационен капацитет. Банките, интернет доставчиците и IT компаниите са последната част от уравнението, която не може да се изключи. Чрез специфичната дейност, която извършват техният принос в повишаване на безопасността в интернет е безценен. Трябва да се даде възможност на младите да участват активно в този процес чрез участие в проекти и проучвания, които се фокусират върху киберсигурността и чрез възможността да споделят опит и идеи със свои връстници. В сравнение с повечето държави членки от ЕС България не работи достатъчно активно по сигурността на младите в интернет. Европейските държави залагат на публично – частното партньорство и отдават сериозно значение на комуникацията и взаимодействието между всички заинтересовани, отделят специално внимание на киберсигурността чрез създаването на стратегии, органи, организирането на продължителни обучения и изготвянето на специални препоръки.

Не бива да се забравяме и ролята на училището. Това е мястото, което следва да подготви младите хора за предизвикателствата на живота. Именно тук те трябва да се запознаят с рисковете в интернет. Отделянето на часове, посветени на безопасността в интернет в рамките на програмата по Информатика/Информационни технологии е от съществено значение за повишаване сигурността в интернет.

В България като цяло проблемите, свързани със сигурността в интернет се подценяват. Затова говори и фактът, че в България няма единен орган, който да се занимава с политиките и мерките в областта на киберсигурността. Все още няма и разработена стратегия за киберсигурност, въпреки че няколко поредни правителства си поставят нейното приемане като приоритет.

Отделни министерства и държавни органи са изградили способности за превенция на рисковете във виртуалното пространство, но това е по-скоро в резултат на реализацията на секторните политики, за които те са отговорни, но не и цялостна визия. Както редица европейски държави и България следва да създаде свой национален орган в областта на киберсигурността, който да гледа глобално на тези въпроси, необходимо е осъвременяване на законодателството и предприемане на конкретни практически стъпки в тази насока.

Като особено уязвима група, каквато са младите, държавните институция трябва да имат един по-широк поглед при информирането за рисковете и представянето на мерките, които младите трябва да предприемат за тяхната лична безопасност в интернет. Отделните инициативи на фирми и неправителствени организации са полезни, но сигурността на младите в интернет трябва да се превърне в устойчива държавна политика, а тъй като младежта е бъдещето на всяка една държава това ще е полезно и за цялото общество.

ИЗПОЛЗВАНИ ИЗТОЧНИЦИ

- Банка ДСК - препоръки за сигурност в интернет- https://dskbank.bg/Page/default.aspx?xml_id=/bg-BG/Individuals/dskdirectpersonal/.security/
- Фондация "Партньори-България" - Безопасно използване на интернет- http://partnersbg.org/2013/03/safe-internet/
- „Българските деца на възраст между 9 и 16 години използват интернет през мобилни устройства в ниво над средното за Европейския съюз.“- http://www.focus-news.net/news/2015/06/24/2083295/balgarskite-detsa-na-vazrast-mezhdu-9-i-16-godini-izpolzvat-internet-prez-mobilni-ustroystva-v-nivo-nad-srednoto-za-evropeyskiya-sayuz.html
- „Горнооряховски младежи преминаха обучение за справяне с формите на насилие онлайн и офлайн.“- http://www.helpline.bg/
- Децата не си дават ясна сметка за опасностите, които крие за тях И'нет
- http://computerworld.bg/25281_decata_ne_si_davat_yasna_smetka_za_opasnostite_koito_krie_za_tyah_inet
- „Децата рядко търсят помощ при проблеми онлайн“- http://www.safenet.bg/index.php?id=1391&art_id=16103
- Държавна комисия по сигурността на информацията, Рискове за интересите на Република България в областта на защитата на класифицираната информация.
- http://www.dksi.bg/NR/rdonlyres/5DB28C7E-7B2B-4DBE-894D-759B7329D913/0/Riskove_za_za6itata_na_KI.pdf
- Кръгла маса по въпросите на защитата на децата в интернет пространството, 18 май 2015 г.- https://www.mtitc.government.bg/page.php?category=700&id=8279
- Национален център за безопасен интернет.
- http://www.safenet.bg
- Обединена българска банка- правила за сигурност.

- https://ebb.ubb.bg/help/security_BG.html
- Помощ за вашата безопасност онлайн – Societe Genrale Експресбанк
- http://www.sgeb.bg/bg/byrzi-vryzki/sigurnost-v-internet.html
- Правила за сигурност и безопасност в Интернет- http://sacp.government.bg/deinosti/deca-info-obshtestvo/pravila-bezopasnost-internet/
- Сигурност на младите в интернет- http://safe.teacher.bg/html/etusivu.htm
- УниКредит Булбанк- препоръки за сигурност при работа с интернет банкиране
- http://www.unicreditbulbank.bg/weblayout/groups/bulbankwebsite/documents/bbproductdocument/bg_online_recommendations.pdf
- „5-те най-големи киберзаплахи за 2014-та“- http://www.security.bg/topnews/5-te-naj-golemi-kiberzaplahi-za-2014-ta
- Bezpečný Internet. (2015). Sociálne siete. Nebezpečenstvá sociálnych sietí.- http://www.bezpecnyinternet.sk/
- Gregussová, M., Drobný, M. (2013). Deti v sieti. Ako chrániť seba a naše deti na internete. - http://www.zodpovedne.sk/index.php/component/jdownloads/finish/1-knihy-a-prirucky/9-kniha-deti-v-sieti-2013-14?Itemid=0
- Anti-bullying- http://www.safenetwork.org.uk/help_and_advice/Pages/AntiBullying.aspx
- Children using internet from age of three, study finds http://www.telegraph.co.uk/technology/internet/10029180/Children-using-internet-from-age-of-three-study-finds.html
- Cyber Safety, An Interactive Guide to Staying Safe on the Internet
- http://www.opencolleges.edu.au/informed/cyber-safety/
- E-safety policy- http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/esafety-policy

- EU Kids Online, Towards a Better Internet for Children- http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20III/Reports/EUKidsOnlinereportfortheCEOCoalition.pdf
- European Internet Security Strategy, European Union, April 2013.
- Global Resource and Information Directory. (September, 3, 2014). Germany. Country Profile- http://www.fosigrid.org/europe/germany
- InHope Annual Report- http://inhope.org/Libraries/Annual_reports/Inhope_Annual_Report_2013.sflb.ashx
- InHope. (March, 12, 2015). European Parliament calls for crackdown on online child sexual abuse- http://www.inhope.org/tns/news-and-events/news/15-03-12/European_Parliament_calls_for_crackdown_on_online_child_sexual_abuse.aspx
- Results of an Expert Survey on Matters of sSafer Internet and Youth Protection in Europe, Youth Protection Roundtable http://uploadi.safe.si/editor/1224568678YPRT_Survey_2007.pdf
- Risks and safety for children on the internet: the FR report- http://eprints.lse.ac.uk/46442/1/FranceReportEnglish.pdf
- Safer Social Networking Principles for the EU, February 10, 2009- https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf
- Smahel, D. Helsper, E. J., Barbovschi, M. & Dedkova, L. (2012) Meeting Online Strangers among European Children. Proceedings of the 15th European Conference on Developmental Psychology. Bologna, Italy, 419-422.
- Survey of Schools, ICT in Education- https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/KK-31-13-401-EN-N.pdf
- The Protection of Children Online http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf
- The Internet and Today's Youth: Protecting our Future- https://blogs.mcafee.com/executive-perspectives/the-internet-and-todays-youth-protecting-our-future/

- Vulnerable young people, social media and e-safety - http://www.saferinternet.org.uk/content/childnet/safterinternetcentre/downloads/Research_Highlights/UKCCIS_RH_19_MPP.pdf
- Wagener, V. (May, 13, 2015). Dangers that lurk on the Internet http://www.dw.com/en/dangers-that-lurk-on-the-internet/a-18448820
- What can make young people vulnerable online? - http://parentinfo.org/article/what-can-make-young-people-vulnerable-online
- „ 4 Dangers of the Internet“-http://www.webmd.com/parenting/features/4-dangers-internet
- https://en.wikipedia.org/wiki/Internet_safety
- https://www.microsoft.com/bulgaria/press/news_15122010.mspx
- http://www.ofcom.org.uk/
- http://www.saferinternetday.org/web/bulgaria/home
- http://www.saferinternetday.org/web/guest;jsessionid=166DDAEEBB283440677EA1AF49C1C604