СИГУРНОСТ В ДИГИТАЛНОТО ОБЩЕСТВО. ТЕХНОЛОГИЧНИ ПЕРСПЕКТИВИ И ПРЕДИЗВИКАТЕЛСТВА

доц. д-р Златогор Минчев

Институт по информационни и комуникационни технологии/Институт по математика и информатика - БАН

Резюме: Съвременното дигитално общество поставя редица предизвикателства за модерната сигурност. Развитието на уеб технологиите, смарт устройствата и системите от нашето ежедневие предоставят множество нови услуги и, същевременно, пораждат редица явни и скрити заплахи за потребителите. Изследването на този процес е сложна и комплексна задача, за решаването на която нашата и световната изследователска общност полага множество усилия. В доклада ще бъде на правен кратък преглед на основните съвременни тенденции на изследванията в сферата на киберсигурността, като се поставят акценти върху заплахите в социалните мрежи и смарт домовете на бъдещето, използващи Web 2.0 и Web 3.0 технологии. В този контекст ще се представят и някои предизвикателствата от въвеждането на добавена и виртуална реалност, роботизирани системи и усъвършенстван изкуствен интелект в дигиталното общество.

Ключови думи: дигитално общество, нови технологии, киберсигурност, кибер заплахи

1. Въведение

Развитието на новите технологии придоби съществена значимост с появата на глобалната Интернет свързаност още в началото на 90-те години на XX век. Това, от своя страна разкри множество нови възможности за потребителите на Web 1.0 технологията. Днес, в XXI век, навлизаме все по-активно в новото дигитално общество, в което итеракцията между потребителите и машините, опосредствана от Интернет средата, открива много нови възможности, но и същевременно – поставя много нови предизвикателства и заплахи за сигурността на потребителите.

Тази интеракция е именно двигателят на новите поколения съвременни уеб технологии: Web 2.0 и Web 3.0, където основните акценти са свързани с активното отношение на средата към потребителите, обмяната и споделянето на мултимедийна информация в социалните мрежи и мобилността на смарт устройствата.

Какво ни предстои в следващите десетилетия около Web 4.0 и Web 5.0 са само догадки, които днес свързваме с по-пълното навлизане във виртуалното пространство, добавената реалност, развития изкуствен интелект, позволяващ по-пълноценно общуване между човека и машините, роботиката и дори телепатичната комуникация.

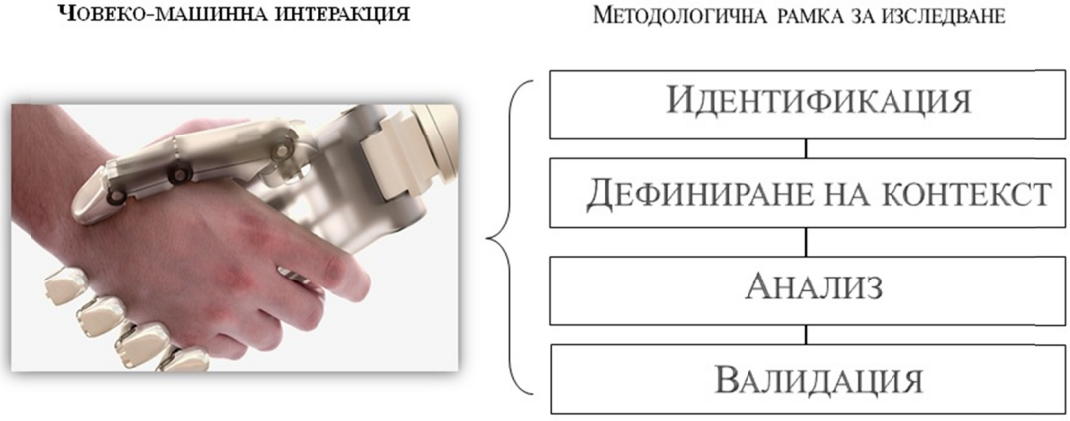
Всички тези тенденции звучат доста фантастично, но някои от тях практически вече са реалност за съвременния човек, живеещ в модерен, високотехнологичен дом, и дори град, общуващ с приятелите си чрез Facebook и Twitter.

Появата на нови технологии, освен удобства, генерира и редица изисквания: като култура на ползване, изисквания за сигурност (прието днес да се определя като „киберсигурност“), политики и правила за контрол на новото дигитално общество.

В тази връзка ще бъде представена, накратко, и практическа методологична рамка за изследване на кибер заплахите в дигиталното общество, която е приложена успешно върху актуалните, към момента, проблеми около социалните мрежи, смарт устройствата и домовете на бъдещето.

2. Методологична рамка за изследване на кибер заплахи в дигиталното общество

Изследването на кибер заплахите в дигиталното общество е практически свързано с изследване на човеко-машинната интеракция. Общата идея на методологична рамка за изследване на този проблем е представена на Фиг.1:



Фиг.1. Обща идея на методологична рамка за изследване на киберзаплахите, произтичащи от човеко-машинната интеракция в дигиталното общество.

Както става ясно от Фиг.1, предложената методологична рамка съдържа четири основни етапа: *идентификация*, *дефиниране на контекст*, *анализ* и *валидация*, които ще детайлизираме по-долу.

Идентификацията на киберзаплахите, произтичащи от човеко-машинната интеракция, може да се извърши на експертна основа чрез техники, като „мозъчна буря“, „дискусии“, „обсъждания“, „анкети“ и филтриране на получените резултати, посредством „Делфи метод“[1].

Едно практическо прилагане на *идентификацията* е показано на Фиг.2:

Технология/Направление	Гражданско общество	Банкиране и финанси	Държавно управление	Критична инфраструктура	Нови технологии	Образование
Web 1.0						
Web 2.0 / Web 3.0						
Web 4.0						
Web 5.0						

Фиг.2. Експертно оценяване на влиянието на уеб технологиите върху различни социални направления: *гражданско общество*, *банкиране и финанси*, *държавно управление*, *критична инфраструктура*, *нови технологии*, *образование*.

Резултатите, показани на Фиг.2, използват цветова скала от зелено към червено, през жълто, показваща засилване на дадено направление в посока към червения цвят и съответно – отслабване, в посока към зеления цвят. Използването на син цвят, отразява наличието на неопределеност. Възможният брой градации е пет, в т.ч. и времевият хоризонт, който също е пет години, подобно на сходно изследването на ЕК по проблема за 2012 година[2].

Ще отбележим, че настоящото обхваща 150 участници и бе организирано през 2013 година от Съвместния център за обучение, симулации и анализ към Института за информационни и комуникационни технологии при БАН с помощта на три непрвителствени организации (Съюз на офицерите от резерва „Атлантик“[3], Асоциация на

[1] Minchev, Z. & Shalamanov,V. Scenario Generation and Assessment Framework Solution in Support of the Comprehensive Approach, In Proceedings of SAS-081 Symposium on “Analytical Support to Defence Transformation”, RTO-MP-SAS-081, Sofia, Boyana, April 26 – 28, 22-1 – 22-16, 2010, Available at: http://gcmarshall.bg/KP/new/MP-SAS-081-22-MINCHEV-SHALAMANOV.pdf

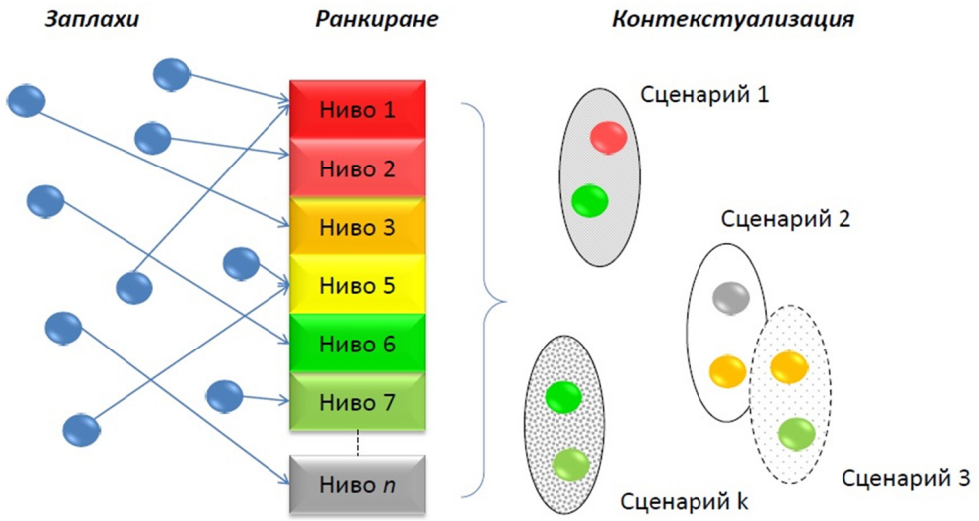
[2] SysSec Deliverable D4.2: Second Report on Threats on the Future Internet and Research Roadmap, September 2012, Available at: http://www.syssec-project.eu/media/page-media/3/syssec-d4.2-future-threats-roadmap-2012.pdf

[3] Съюз на офицерите от резерва „Атлантик“, Уеб страница: http://www.atlantic-bg.org/bg/index.html

комуникационни и информационни специалисти[4] и IFIP Technical Committee on Entertainment Computing[5]), УНСС – София (катедра „Национална и регионална сигурност“[6]) и със съдействието на Европейската мрежа от центрове за върхови постижения в сферата на идентифициране на кибер рисковете и заплахите за Интернета на бъдещето – SySSec[7],

Както става ясно от Фиг.2, тенденциите в Web 1.0/Web 5.0 са свързани с повишаване на кибер рисковете и заплахите за всички изследвани направления, като по отношение на *Банкиране и финанси* и *Нови технологии* за Web 4.0/Web 5.0, участниците не дават ясна оценка за възможното тяхно влияние през следващите пет години, което класифицират като „неопределено“, предвид факта, че тези технологии ще се развият за етап от поне десет години. Това, най-общо, дава основание да преминем към следващия етап от методологичната рамката – *Дефиниране на контекст*, който ще даде по-голяма яснота по отношение на направените оценки в динамика от сценарии.

Дефинирането на контекст е действие, използващо също експертни знания. Схематично то може да се представи по начина, показан на Фиг. 3:



Фиг.3. Дефиниране на контекст за анализ на идентифицирани кибер заплахи.

[4] Асоциация на комуникационни и информационни специалисти, Уеб страница: http://acis-bg.org/about.aspx

[5] International Federation for Information Processing, Technical Committee on Entertainment Computing, http://www.org.id.tue.nl/ifip-tc14/

[6] УНСС-София, катедра „Национална и регионална сигурност“, Уеб страница: http://www.e-dnrs.org/

[7] EU Network of Excellence in Managing Threats & Vulnerabilities for the Future Internet, http://www.syssec-project.eu/

Както става ясно от Фиг.3 идентифицираните заплахи се ранкират по важност и след това се разглеждат като управляващи въздействия по отношение на експертно избрани сценарийни комбинации. Реализацията на този етап също е базирана на експертно участие и прилагане на „метода на сценариите“. Един добър и актуален пример в областта е отново предложен от консорциума SySSec[8], като тук могат да се отбележат и усилията на групата по европейския проект FOCUS[9], създала нова, добре обоснована, пътна карта за изследвания в сферата на сигурността.
Предложените сценарии е добре да бъдат детайлно анализирани за да постигане на по-добра аргументация на получените резултати.

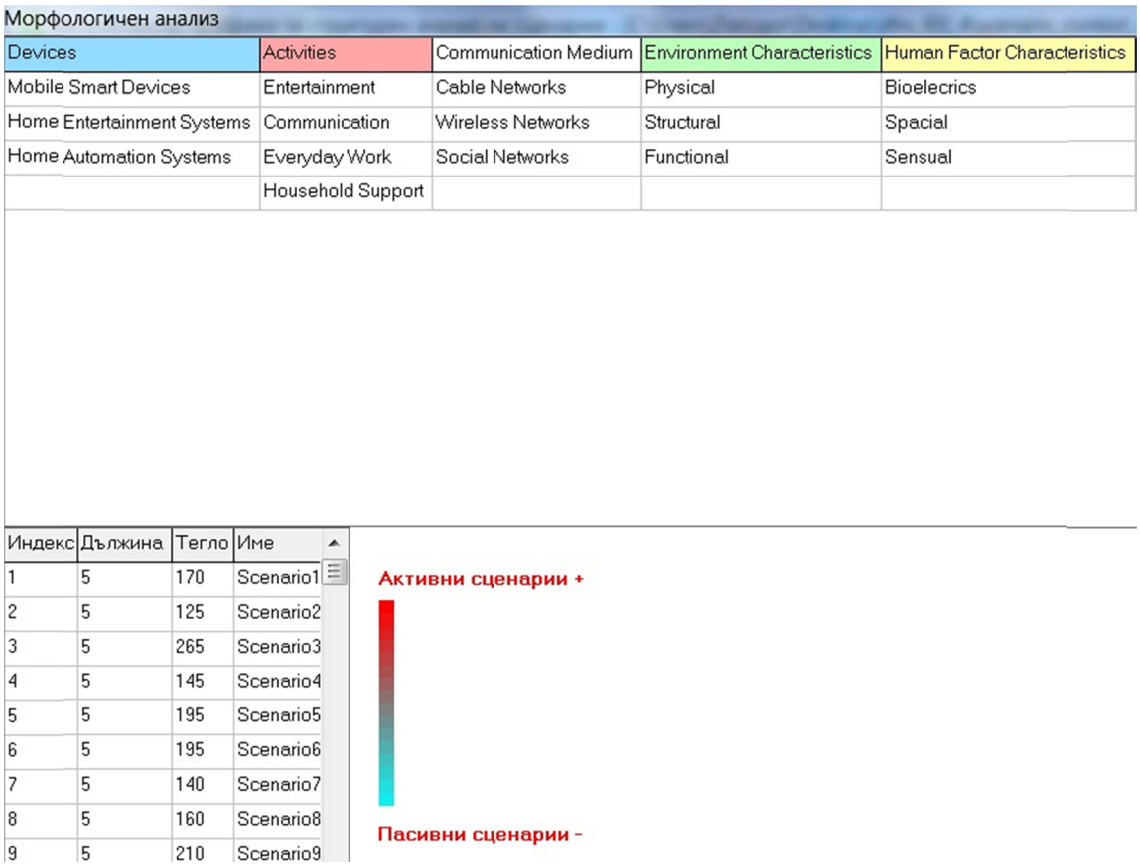
Анализът, използван при прилагане на метода на сценариите включва в себе си структурен (морфологичен) анализ, а по-детайлните изследвания по отношение на динамиката и значението на отделни кибер рискове и заплахи, може да се извърши посредством системен анализ.

Предвид сложността на процеса се използва авторска разработка под формата на програмата I-SCIP-MA/SA[1], чрез която се постига лесна, интерактивна работа и бързо представяне на получените резултати.

Практическото прилагане на структурен анализ за генериране на сценарии по изследване на кибер заплахите и рисковете в домовете на бъдещето, е показано на Фиг.4:

[8] SysSec Deliverable D4.1: First Report on Threats on the Future Internet and Research Roadmap, September 2011, Available at: http://www.syssec-project.eu/media/page-media/3/syssec-d4.1-future-threats-roadmap.pdf

[9] FOCUS Project Web Site, http://www.focusproject.eu/



Фиг.4. Екранна снимка от програмата I-SCIP-MA, показвща експертно дефинирани сценарийни комбинации за изследване на домовете на бъдещето[10].

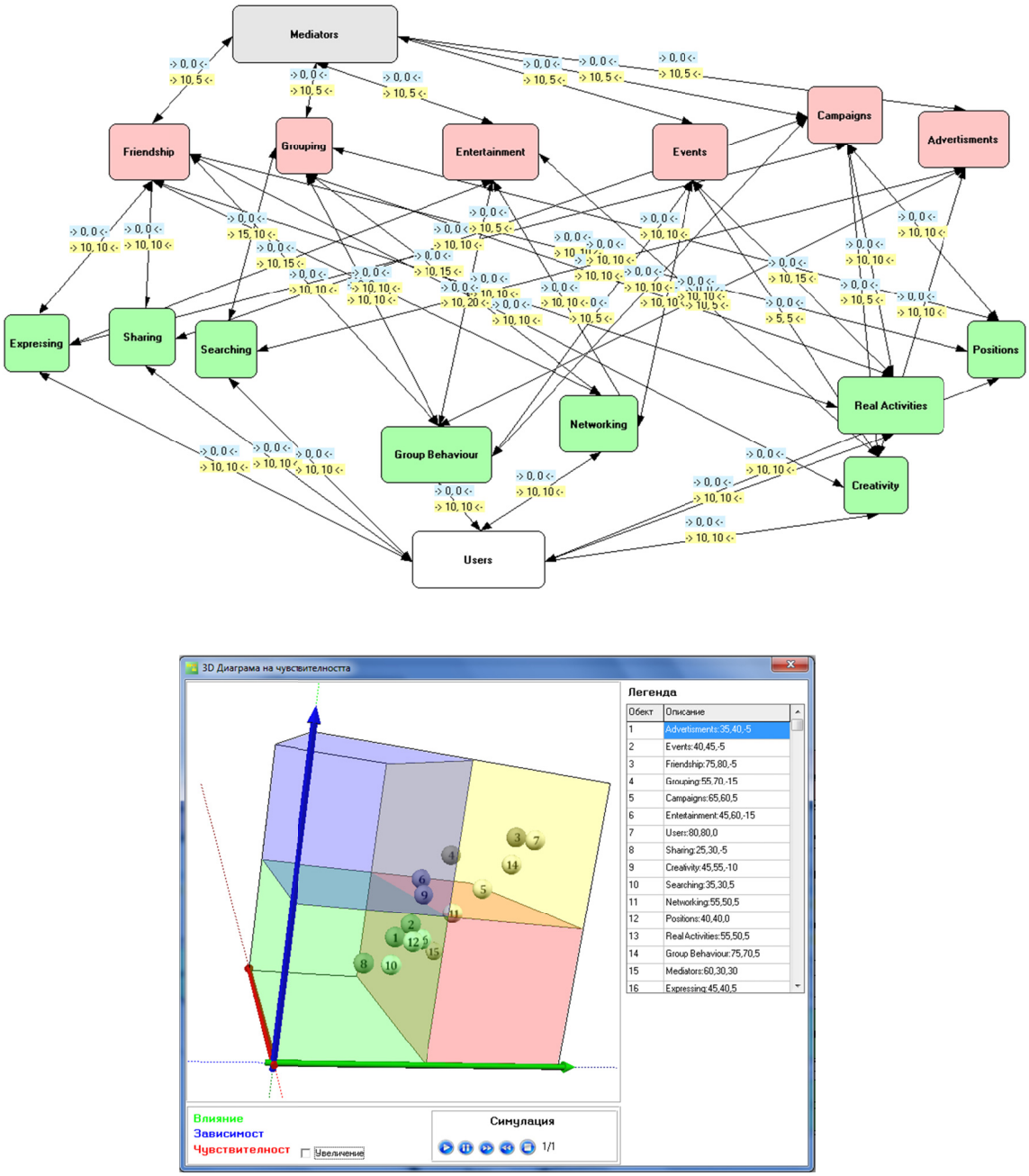
Реалното използване на системния анализ се извършва след преминаване през структурния (морфологичен) анализ, организиран около различни измерения (представени на Фиг.4, като оцветени и именувани колони) и взаимно изключващи се алтернативи за тези измерения, формиращи матрицата на кросконсистентност, която реално съдържа всички възможни сценарии. Една възможна илюстрация на процеса е свързана с анализа на сценарийна комбинация, използваща социалните мрежи, като среда за комуникация.

Тук може да се изследват изключително актуални проблеми, като „социалния инженеринг“ например[11]. На Фиг.5. е показан модел на това изследване и

[10] Minchev, Z., Boyanov, L., Georgiev, S. Security of Future Smart Homes, Cyber-physical Threats Identification Perspectives, Proceedings of HOME/2010/CIPS/AG/019 Conference", Part II, ISBN 978-954-92552-7-0, 2013, Aavailable at: http://smarthomesbg.com/files/dfni_t01_4_zm_lb_sg_paper_june_4_2013.pdf

[11] Minchev, Z. Social Networks Security Aspects. A Technological and User Based Perspectives, Proceedings of TELECOM 2012, Available at: http://snfactor.com/snfactor/sites/files/sns_eng_model_telecom_2012_zm_paper_oct_18_19_2012.pdf

резултантната класификация, използваща четири зони: буферна (зелена), активна (червена), пасивна (синя) и критична (жълта).



Фиг. 5. Модел за изследване на социалния инженеринг, посредством системен анализ в средата I-SCIP-SA[10] (горе) и резултантна класификация (долу).

Така получените аналитични резултати е добре да бъдат валидирани.

Валидацията е процес, който се осъществява на базата на мониторинг на динамиката на активностите на потребителите и средата. Възможно решение тук е прилагането на

директен и индиректен психофизиологичен мониторинг и биометрична идентификация от страна на потребителя[12]. Технологиите също могат да са предмет на мониторинг, като се отчитат физически параметри на средата, обем на трафик и др.[13], а също математическо моделно валидиране и използване на компютърно подпомагани учения[1].

На Фиг. 6 са показани моменти от психофизиологичната валидация за оценка на потребителите по отношение на идентифицирани кибер рискове и заплахи.

Фиг. 6. Моменти от психофизиологичната валидация за оценка на потребителите по отношение на идентифицирани кибер рискове и заплахи.

[12] Minchev, Z. Cyber Threats in Social Networks and Users' Response Dynamics, IT4SEC Reports, 105, Available at: http://www.it4sec.org/bg/system/files/IT4Sec_Reports_105_2.pdf

[13] Георгиев, С. Колев, Х. Обрешков, Н. Лалев, Е. Система за сигурност в домовете на бъдещето. „Сборник материали - HOME/2010/CIPS/AG/019", Част втора, ISBN 978-954-92552-7-0, 2013, Достъпна на: http://smarthomesbg.com/files/dfni_t01_4_sg_hk_no_el_paper_june_4_2013.pdf

Тук ще отбележим, че предложената методологична рамка не изчерпва изцяло методите за постигане на добри резултати в отделните етапи, а по-скоро служи като добра и надежна основа за по-нататъшно развитие и усъвършенстване.

3. Дискусия

Гарантирането на сигурността в дигиталното общество е интердисциплинарна задача, за решаването на която, са необходими както технологични, така и социални действия. Развитието на технологиите е свързано с необходимост от изследване на тяхното въздействие върху потребителите, ограничаване на вредните влияния, създаване на потребителска култура и гарантиране на достъп до актуална информация за новите тенденции и произтичащите от тях потенциални кибер рискове и заплахи.

4. Благодарности

Авторът изказва благодарности за финансовата подкрепа на: Фонд „Научни изследвания“, Министерство на образованието, младежта и науката, проекти: „Изследване на информационните заплахи и поведенческа динамика на потребителите в социални мрежи от Интернет пространството“, ДМУ 03/22, www.snfactor.com; „Изследване на възможностите за идентифициране на кибер заплахи и тяхната връзка с поведенческата динамика на потребителите в домовете на бъдещето“, ДФНИ-Т01/4, www.smarthomesbg.com; „Мозъчно-корова регулация на спокойния стоеж при сетивен конфликт“, ТК 02/60, www.cleverstance.com;

ЕК и проект: EU Network of Excellence in Managing Threats and Vulnerabilities for the Future Internet: Europe forthe World – SySSec,No. 257007, www.syssec-project.eu.

Благодарност също и към всички организации и компании, партньори на Съвместния център за обучение, симулации и анализ, подпомагащи работата по изследванията в тази актуална област.