**Аналитичен подход за изследване на новите предизвикателства пред сигурността в дигиталното общество**

доц. Златогор МИНЧЕВ

Институт по информационни и комуникационни технологии,

Българска академия на науките

инж. Георги ДУКОВ,

Институт по информационни и комуникационни технологии,

Българска академия на науките

***Резюме:*** Динамиката на новото дигитално общество създава редица нови предизвикателства пред съвременната сигурност. Днес те се развиват в сложната кибер-физическа смесена реалност, включваща информационното пространство и обективната реалност. В статията е представен методологичен подход за моделно изследване на тези нови заплахи. Използвано е системно моделиране и анализ, базиран на анкети, интервюта и експертни знания. Последващата вероятностна валидация, се използва за симулационна оценка в динамика на идентифицираните заплахи. Резултатите са допълнително верифицирани с активното участие на човешкия фактор. Предложеният подход създава добра основа за анализ на бъдещите предизвикателства пред сигурността в дигиталното общество.

***Ключови думи:*** кибер-физическо пространство, заплахи и предизвикателства, моделно изследване и анализ, валидация и верификация.

**Въведение**

Съвременното общество създава все по-тясна връзка между технологиите и хората. Това, от своя страна, става източник на редица социални промени в поведението и реакциите на днешните и бъдещите хора. Технологиите все повече влияят върху формирането на дигиталното общество, което създава своеобразен еволюционен парадокс. Новата кибер-физическа реалност е основополагаща за социалните промени, базирани на технологиите от Интернет пространството [1]. Ускорената социална динамика, допълнително стимулирана от съвременните феномени на: цветните революции, тероризма, миграцията и хибридните войни е много по-различна от тази на 20-и век. В ерата на уеб технологиите и услугите, социалните мрежи и мобилните смарт устройства, понятия като „социален инженеринг“, „лично пространство“ и „компрометираност по дизайн“, пораждат редица въпроси пред бъдещето на човеко-машинната интеракция в новата смесена реалност на съществуване [2]. При това, развитието на идеята за автономност, от гледна точка на технологията, поставя нови предизвикателства пред бъдещето на „изкуствения интелект“. Очакваното развитие за комуникациите на ниво „машина-машина“ в ерата на „Интернет на обектите“, открива и реални възможности за недалечното бъдеще, свързани с „машинно-човешко“ общуване [3]. Едно по-различно равнище в този аспект ще отреди по-активна роля на машите и самоеволюиращият им интелект [4], който неформално да повлияе на хората по нов, неизследван досега начин.

Всичко това поставя неизменната необходимост за създаване на изследователска рамка, представена в следващата точка, за адекватно посрещане на тези нови предизвикателства в днешното дигитално общество.

**Изследователска рамка**

Предвид сложния, многостранен и не напълно определен характер на съвременната кибер-физическа реалност и възникващите в нея предизвикателства пред сигурността, породени от „човеко-машинната“ интеракция, за целите на настоящата работа бе модифицирана и допълнена изследователска рамка, основана на идеите от [5] - [7].

C:\Users\Zlatogor\Desktop\NBU\nbu_2016\figures\grey\Figure 1.tif

**Фиг.1. Общ вид на използваната изследователска рамка**

Както е видно от Фиг. 1, рамката е организирана в четири етапа с активното участие на човешкия фактор: (i) *Дефиниране на проблемното пространство*, (ii) *Системно моделиране и анализ*, (iii) *Вероятностна валидация* и (iv) *Интерактивна верификация*.

В следващата точка рамката ще бъде представена в детайли, в съчетание с аналитични резултати, демонстриращи ефекта от нейното практическо използване в изследването на настоящи и бъдещи заплахи в новата дигитална реалност.

**Практическа реализация**

Представените на Фиг.1 четири етапа от изследователската рамка за изследването на кибер-физическата реалност ще бъдат детайлно разгледани и илюстрирани по-долу.

*Дефиниране на проблемното пространство*

Предвид прогнозния характер на този етап, бяха използвани данни от образователната сфера, индустрията и експертната общност. Изследването бе реализирано чрез анкетно проучване сред 350 студенти (21 +/-3 години) от страна на Съвместния център за обучение, симулации и анализ (СЦОСА) към Института по информационни и комуникационни технологии (ИИКТ) – БАН, съвместно с Университета за национално и световно стопанство и Пловдивския университет „Паисий Хилендарски“. Допълнително бяха включени тенденции от анализа, приложен в подготовката на Национална стратегия за киберсигурност на Р България [8]. Мненията на водещи индустриални партньори, събрани от 21 световни лидери в сферата на информационните и комуникационни технологии, предоставени ни от Асоциацията на комуникационните и информационни специалисти в България [9], също бяха използвани при формирането на настоящото проблемно пространство.

Обобщените резултати, в графичен вид, с времеви хоризонт до 2020 година са представени на Фиг.2.

**C:\Users\Zlatogor\Desktop\NBU\nbu_2016\figures\grey\Figure 2.tif  
Фиг.2. Обобщение на тенденциите в развитието на дигиталното общество, уеб услугите, киберпредизвикателствата и възможни вектори за атаки до 2020 г.**

Както става ясно от Фиг.2, основните тенденции до 2020 година, определени в изследването, дават приоритетно развитие на „Среда и качество на живот“ – 40% и „Бизнес и производство“ – 28%. Тенденцията се запазва и в очакваната еволюция на уеб услугите и въвеждането на 4G/5G високоскоростен мобилен достъп, позволяващ увеличаване на „Разширени мултимедийни забавления“ – 35%, използващи смарт устройства за „Подобряване качеството на живот“ – 30%. При това, най-съществените кибер предизвикателства за човешкия фактор се предвиждат в „Лично пространство и технологично пристрастяване“ – 35% и „Информационно претоварване“ – 30%. Възможните вектори за атаки са съсредоточени в „Лично пространство и социален инженеринг“ – 40%, „Зловреден софтуер и насочени атаки“ – 25%.

Като цяло, ще отбележим, че близките пет години не се очаква рязка тенденция за дефиниране водеща роля на машините и изкуствения интелект пред тази на човешкия фактор.

*Системно моделиране и анализ*

Изследването на сложните взаимовръзки в кибер-физическата реалност на дигиталната ера и произтичащите от тях заплахи и предизвикателства, предвижда необходимостта от по-задълбочено разглеждане на проблема. Получените резултати от предишната точка, най-общо очертават проблемното пространство за работа, но не отчитат системното влияние между отделните области на интерес. С цел преодоляване на това несъвършенство, тук ще бъде представен системен модел, предоставящ възможност за по-задълбочен анализ и оценка.

За целите на настоящото системно моделиране и анализ бе използвано проблемното пространство, дефинирано в предишната точка (вж. Фиг.2), в съчетание с обобщените резултати от дискусии с участници от 24 държави (представители на НАТО, Балканите, Черноморско-кавказкия регион и Европа) по време на: “Cyber Forum DESSERT B2S – S2B”, м. май, 2016 и “Third NATO Summer School in Bulgaria: NATO Challenges & Concerns on the Eve of 2016 Summit”, м. юни, 2016.

Практическото използване на тези данни бе осъществено чрез средата I-SCIP-SA, позволяваща лесно и интуитивно моделиране и анализ в различни проблемни области. При това, идеята в процеса на моделиране е основана на машинното представяне на сложни системи чрез подхода „обект-връзка“. Реализация е извършена върху претеглен ориентиран граф, представящ комплексна дискретна система в статичен или динамичен режим [10].

Общата класификация на обектите в създадения системен модел са графично интерпретирани в „3D Диаграма на чувствителността“, използваща оценки за: „Влиянието“ (правата връзка – *x*), „Зависимостта“ (обратната връзка – *y*) и „Чувствителността“ (резултантната на правата и обратната връзка – *z*) на обектите в четири сектора: „активен“ – червен, „пасивен“ – син, „критичен“ – жълт, „буферен“ – зелен. Допълнително, съобразно стойностите на *z*, обектите са класифицирани като „активни“ (бели, *z* > = 0) и „пасивни“ (сиви, *z* < 0) в рамките на всеки от разглежданите сектори.

Резултатите от системното моделиране и класификация за прогнозно изследване на ефектите от кибер-физическото взаимодействие в новото дигитално пространство са представени графично на Фиг. 3.

C:\Users\Zlatogor\Desktop\NBU\nbu_2016\figures\grey\Figure 3a.tif

C:\Users\Zlatogor\Desktop\NBU\nbu_2016\figures\grey\Figure 3b.tif

**Фиг. 3. Системен модел (а) и резултантна 3D класификация (б) за прогнозно изследване на ефектите от кибер-физическото взаимодействие в новото дигитално пространство чрез средата I-SCIP-SA, v. 2.0.**

Представения на Фиг.3а модел е изграден на базата на два класа обекти от кибер-физическата реалност: *Физически*, представящи социалния фактор в новата дигитална ера: „Управление“, „Публичен сектор“, „Предприятия“, „Индивиди“ и съответните дейности, свързани с тях: „Всекидневни активности“, „Забавления“, „Бизнес“, „Криминални активности“; *Кибер* частта е ориентирана около очакваното технологично развитие до 2020 година, свързано с: „Уеб услуги“, „Смесена реалност“, „Изкуствен интелект“, „Хипермедия“, „Комуникационни услуги“, „Инструменти за сътрудничество“ и произтичащите от тяхното взаимодействие с физическата част на модела, хибридни по характер заплахи: „Дехуманизация“, „Информационно претоварване“, „Е-регулации“, „Мултикултурни сблъсъци“ и „Дигитални неясноти“.

По отношение на класифицирането на тези обекти, с цел определяне на тяхната значимост в модела, бе извършен последващ системен анализ за дефиниране и оценка на връзките между обектите.

Резултатът е представен графично в „3D Диаграмата на чувствителността“ (вж. Фиг.3б), като са определени следните класове обекти: активни: „Уеб услуги – 12“, „Дигитални неясноти – 16“, „Хипермедия – 2“, „Публичен сектор – 7“, „Управление – 8“; критични: „Бизнес – 4“, „Забавления – 11“, „Е-регулации – 3“, „Информационно претоварване – 15“, „Предприятия – 6“, „Мултикултурни сблъсъци – 13“, „Криминални активности – 14“; пасивни: „Всекидневни активности – 10“, „Дехуманизация – 19“, „Комуникационни услуги – 17“; буферни: „Смесена реалност – 1“, „Инструменти за сътрудничество – 18“, „Индивиди – 9“, „Изкуствен интелект – 5“.

Наличието на множество обекти от модела в критичната зона показва ясно, че заплахите и предизвикателствата в кибер-физическото пространство имат сложна природа. Всичко това способства за развитието на средата, при отчитане водещата роля на бизнеса и публичния сектор. Критичните моменти в модела са определени за Е-регулациите, мултикултурните сблъсъци, информационното претоварване и криминалните активности.

Развитието на изкуствения интелект не е определено явно за заплаха. То е отразено индиректно в дехуманизацията, вследствие на интелигентната електронизация на всекидневните активности и нарастващата популярност от развиващите се мобилни технологии и комуникационни услуги. При това, активна остава ролята на нарастващите дигитални неясноти в новото общество. Тези резултати се потвърждават и от други изследвания с по-широк времеви хоризонт [11], [12].

Поради статичния характер на предложения модел, в следващата точка е извършено и изследване на възможностите за неговата, динамична вероятностна валидация.

*Вероятностна валидация*

Представените резултати от системния анализ дават добра основа за системно разглеждане на предизвикателствата и заплахите в кибер-физическата реалност. Получената класификация обаче е статична. Интерес представлява нейното развитие, предвид прогнозния ѝ характер. Тук ще отбележим и други сходни достижения, като: циклите на Кондратиев и Теория на перспективите на Канеман-Тверски за описване на социалната и икономическа динамика [13]. Използването на трендове за прогнозиране на бъдещето е доста амбициозна задача, решението на която може да бъде осъществено, най-общо, по два начина: (i) чрез разработване на аналитичен модел от система уравнения или (ii) посредством вероятностни разпределения.

Практическото използване на първия метод е предложено в [14], като е постигната много добра точност, но при сравнително гладки трендове, което не винаги е възможно. В настоящата работа ще бъде приложен вторият – вероятностният. Основна причина за това е липсата на трендове за изследване. Друг проблем е сложността при създаването на модели за тяхното генериране, по отношение на стабилност и чувствителност, при наличие на голям брой параметри, необходими за постигане на близък до реалността модел.

Вероятностният подход, реализиран на базата на бета разпределение, системно моделиране и средата Matlab R2011b е предложен в [7], като ще отбележим, че дава добра основа за изследване и позволява лесното симулиране на различни типове атаки, по отношение на връзките между обектите в системата. Това е сериозно предимство, предвид възможността за комбиниране на анкетни, експертни, симулационни и сензорни данни, с прякото участие на човешкия фактор [5]. Същевременно така се преодоляват проблемите с различните скорости на изменение на трендовете и техните размерности.

Графични резултати от прилагането на методологията за вероятностна валидация на тенденциите в развитието на избрани заплахи от системния модел (вж. Фиг. 3) са показани на Фиг.4.

**C:\Users\Zlatogor\Desktop\NBU\nbu_2016\figures\grey\Figure 4-I.tif**

**C:\Users\Zlatogor\Desktop\NBU\nbu_2016\figures\grey\Figure 4-II.tif**

**C:\Users\Zlatogor\Desktop\NBU\nbu_2016\figures\grey\Figure 4-III.tif**

**Фиг.4. Вероятностна валидация на тенденциите в развитието на избрани заплахи от Фиг. 3 („Дигитални неясноти“ – I, „Информационно претоварване“ – II, „Дехуманизация“ – III) в средата Matlab R2011b**

Предствените на Фиг. 4 резутати са отнесени към трите класа заплахи, идентифицирани в ситемния модел от Фиг. 3: активни: „Дигитални неясноти“ – 16, критични: „Информационно претоварване“ – 15 и пасивни: „Дехуманизация“ – 19.

Изследването на тяхната еволюционна динамика чрез предложената валидация, показва някои интересни резултати по отношение промяната в априорната спрямо апостериорната вероятност. За „Дигитални неясноти“ (панел I, Фиг. 4б) значима роля се очаква да имат: „Криминални активности“ – 2, „Изкуствен интелект“ – 4, „Смесена реалност“ – 3, „Инструменти за сътрудничество“ – 5. „Информационно претоварване“ (панел II, Фиг. 4б) ще бъде повлияно най-силно от „Хипермедия“ – 4 и „Комуникационни услуги“ – 5. „Дехуманизация“ (панел III, Фиг. 4б) ще зависи най-вече от: „Изкуствен интелект“ – 3, „Комуникационни услуги“ – 6, „Забавления“ – 2, „Уеб услуги“ – 4 и „Хипермедия“ – 5.

Получените резултати са за атаки в диапазона 30-45% от общия брой използвани, симулирани заявки към всяка от изследваните връзки и M > 0.5.

Резултатите от идентифицираните потенциални заплахи в кибер-физическата реалност, получени като комплексна комбинация на системния анализ и вероятностната валидация имат основно прогнозен характер за изследвания контекст. Предвид техния бъдещ хоризонт за развитие (до 2020 година), в следващия параграф ще разгледаме и възможност за верифицирането им с цел постигане на по-добро разбиране.

*Интерактивна верификация*

Реализацията на този последен етап от предложената методологична рамка (вж. Фиг. 1) се осъществява, на базата на компютърно подпомагани учения за изследване на нови заплахи и предизвикателства в киберпространството [15], [16].

Основната идея, използвана при този подход, реализиращ интерактивна симулация, е да се създадат въображаеми ситуации, при които, съобразно сценариен скрипт от планирани и непланирани събития, да се изследват отговорите и избрани психофизиологични корелати на играещите, с цел оценяване адекватността на техните знания, емоции и поведение в изкуствено създадената среда.

Предвид комплексния характер на изследваните кибер-физически заплахи ще бъдат използвани резултатите от проведено международно учение CYREX 2016, организирано от: Съвместния център за обучение, симулации и анализ в Пловдивския университет „Паисий Хилендарски“, в рамките на обучителния курс „Основи на сигурността в киберпространството“. Подкрепа, с наблюдатели и участници на събитието, бе предоставена от: IFIP, Асоциацията на комуникационни и информационни специалисти и представители на бизнеса от Р България и Р Македония [17].

Обучаемите бяха организирани в затворена Facebook група (от 30 студенти, на възраст 20 +/– 2 години, в т. ч. и 8 наблюдатели), свързана с полигон на смесена кибер-физическа реалност, позволяваща на участниците да използват различни смарт устройства (таблет, фаблет, смартфон, айпод, ултрабук и лаптоп), десктоп компютри, включени във вътрешна LAN мрежа, посредством Wi-Fi рутер (за лесно организиране на вътрешна мрежа и записване на лог за събитията по време на учението), имейл сървър и SMS нотификация. Учението бе проведено чрез пет отбора (мотиватори: „Дигитален живот“: неправителствена организация, наблюдаваща и търсеща регулация в дигиталното общество; хактивисти: „Омега“, неформална организация от хакери; международна разследваща киберпрестъпления агенция: „Хидра“; стартираща шпионска компания „Хоуп“ и мултинационална компания, разследвана за финансиране на криминални дейности: „Корпорация Зет“.

В CYREX 2016 бяха изследвани сценарийни комбинации за реализиране на индустриален шпионаж чрез инсайдери в смесена реалност, с използване на: QR кодове, криптиране, мултимедийни съобщения, базирани на аватари, клауд и чат услуги, както и въздействие чрез: зловреден софтуер, разпределен отказ от услуги – DDoS по IP и социален инженеринг за мотивиран хактивизъм. Идейната архитектура и моменти от учението са показани на Фиг. 5.

C:\Users\Zlatogor\Desktop\NBU\nbu_2016\figures\grey\Figure 5.tif

**Фиг.5. Идейна архитектура (а) и моменти от учението CYREX 2016 (б)**

Като резултат от CYREX 2016, бе установена практически значимата роля на хипермедията в съвременната смесена кибер-физическа реалност, при използване на множество интелигентни устройства за комуникация чрез различни комуникационни услуги. Същевременно, нуждата от Е-регулация на новата дигитална среда за контролиране на различни криминални активности, остава неизменна и, за момента, е в процес на развитие. Наличието на множество дигитални неясноти позволяват сравнително лесното създаване и внедряването на организационни инсайдери, посредством инструментите на социалния инженеринг, с цел шпионаж. При това, новите технологии отварят редица незащитени области за атаки, свързани с удобни и забавни технологични решения и услуги със свободно разпространение. Последното е пряко свързано и с търсенето на лесни и автоматизирани решения за работа, вследствие на информационното претоварване, което поставя еволюцията на изкуствения интелект в приоритет за бъдещите уеб услуги.

**Заключение**

Предложената изследователска рамка за изследване на новите заплахи и предизвикателства в кибер-физическата смесена реалност на дигиталната ера предлага надеждна изследователска основа за работа. Предвид прогнозния си характер, тя е основана на анкетни, експертни и моделно генерирани данни, което й придава завършеност по отношение на възможностите за валидация и верификация с активното участие на човешкия фактор.

Допълнително е възможно нейното последващо усъвършенстване по отношение на:

* обобщен анализ и предсказване на трендовете за очаквани киберзаплахи и предизвикателства в агрегиран вид с цел динамична оценка на прогнозните резултати;
* добавяне на високо интегрирани средства за интелигентен мониторинг и стимулация на емоциите и поведението на потребителите, позволяващ своевременно модифициране на смесената реалност и по-пълно задоволяване на техните потребности.

**Благодарности**

Авторите са признателни за финансовата и експертна подкрепа, оказана им от фирма СТЕМО ЕООД при създаването на модела за киберразузнаване, основан на големи масиви от данни, в рамките на ESGI 113, както и за провеждането на компютърно подпомаганото учение CYREX 2016.

***Използвана литература:***

*1. Floridi, L. The Fourth Revolution (How the Infosphere is Reshaping Human Reality), Oxford University Press, 2016.*

*2. Kim, G. Human-Computer Interaction, CRC Press, 2015.*

*3. Höller, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S., Boyle, D. From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, Elsevier, 2014.*

*4. Bostrom, N. Superintelligence: Paths, Dangers, Strategies, Oxford University Press, 2014.*

*5. Minchev, Z. Human Factor Role for Cyber Threats Resilience, In Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare, Chapter 17, IGI Global, pp. 377 - 402, 2015.*

*6. Minchev, Z. Cyber Threats Identification in the Evolving Digital Reality, In Proceedings of Ninth National Conference “Education and Research in the Information Society”, Plovdiv, Bulgaria, May 26-27, pp. 011-022, 2016.*

*7. Minchev, Z., Dukov, G., et al. Cyber Intelligence Decision Support in the Era of Big Data, In ESGI 113 Problems & Final Reports Book, Chapter 6, FASTUMPRINT, pp. 85-92, 2015.*

*8. Минчев, З. Прогнозни заплахи и предизвикателства в киберпространството, Позиции ЦМСО, No. 31, ЦМСО, ИИКТ-БАН, София, юни, 2015,* [*http://it4sec.org/bg/system/files/views\_031\_0.pdf*](http://it4sec.org/bg/system/files/views_031_0.pdf)

*9. Асоциацията на комуникационните и информационни специалисти,* [*http://acis-bg.org/*](http://acis-bg.org/)

*10. Minchev, Z. Methodological Approach for Modelling, Simulation & Assessment of Complex Discrete Systems, In Proceedings of National Informatics Conference Dedicated to the 80th Anniversary of Prof. Barnev, IMI-BAS, Sofia, November 12-13, 2015, pp. 102-110, 2016.*

*11. Blowers, M. (Editor) Evolution of cyber technologies and operations to 2035, Springer International, Switzerland, 2015.*

*12. Built Environment 2050 (A Report on Our Digital Future), BIM2050 Team, 2014,* [*http://cic.org.uk/download.php?f=be2050-cic-bim2050-2014-1.pdf*](http://cic.org.uk/download.php?f=be2050-cic-bim2050-2014-1.pdf)

*13. Dopfer, K. The Evolutionary Foundations of Economics, Cambridge University Press, 2005.*

*14. 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, NATO RTO ST Organization, 22-1-22-16, 2010.*

*15. Минчев, З. и к-в, Хибридни предизвикателства в киберпространството и ролята на човешкия фактор, Сборник доклади от Международна научна конференция „Югоизточна Европа: новите заплахи за регионалната сигурност“, Поредица „Наука, образование, сигурност“, том 3, София, НБУ, Планета 3, стр. 354-362, 2-3 юни, 2015, публикувана: февруари, 2016.*

*16. Kick, J. Cyber Exercise Playbook, The MITRE Corporation, 2014,* [*https://goo.gl/SOkkw6*](https://goo.gl/SOkkw6)

*17. CYREX 2016 Facebook News Post, February 26, 2016,* [*https://goo.gl/Pa8ArN*](https://goo.gl/Pa8ArN)