

Възможности и опасности от внедряването на решения в Интернет на обектите

Любен Боянов*

Резюме: Настоящата статия представя в синтезиран вид резултатите от университетски изследователски проект на тема „Създаване на платформи за изучаване на подходите за приложения в Интернет на обектите“. В нея са изследвани и анализирани сферите на приложения на Интернет на обектите (ИНО) и основните фактори и участници в него. Описан е процесът на създаване на платформа за изследване на ИНО. Дадени са възможностите за прилагане на процеси от образованието с ИНО – т.нар. „умно“ образование. Представени са средата и методологията, които позволяват на студенти и преподаватели да работят върху функциониращи платформи на ИНО и свързаните с това умения и техники. Направена е оценка на развитие състоянието на ИНО през последните години, опасностите и тенденциите за бъдещето.

Ключови думи: Интернет на обектите, образование, умни предмети, икономическо развитие, киберзаплахи.

JEL: F63, I20, I25, L63, L86, O30.

Увод

Развитието и разпространението на Интернет в глобален мащаб и мини-

атюризацията на цифровите технологии, доведоха до появата на Интернет на Обектите (ИНО) – IoT (Internet of Things, което в буквален превод е Интернет на нещата). Терминът е предложен през 1999 г., но стана изключително популярен едва през последните 5–7 години. След компютърната, Интернет и тази на мобилните телефони, ИНО представлява най-новата промишлена революция (Business Insider, 2016).

До съвсем скоро областите на приложение на цифровите устройства и Интернет бяха (и още са) на работното място и в къщи, като напоследък модерни дигитални помощници на хората станали преносими устройства като таблети и умни телефони. Услугите им включват технологии за отдалечен достъп, комуникация, извличане на информация и извършване на редица електронни услуги в нашето ежедневие (проверка за местоположение, банкиране, плащане на данъци и т.н.). С проникването на ИНО в нашето ежедневие, използването на приложенията на дигиталната технология и взаимната свързаност на обекти от нашето обкръжение се увеличило многократно. Офисът става „умен“, градът става „умен“, а домът и уредите в него, които са „умни“ са вече реалност, а не от епизоди на фантастичен филм. Това води до промяна на света около нас, където средата, в която продължава нашият живот, става много по-различна от тази, в която

* Любен Боянов е доктор, доцент в катедра „Информационни технологии и комуникации“ на УНСС, lboyanov@unwe.bg

сме живяли до сега. Умният телевизор ни позволява да разглеждаме уеб сайтове на него, да пускаме музика или видеоклипове, да гледаме предавания по желание и с телевизора да ползваме домашната мрежа и свързаните към нея устройства. Умните бойлери могат да се пуснат да затоплят водата малко преди да се върнем в къщи, а въздухът може да се затопли или охлади от умните климатици. Умният хладилник може да ни информира за липсващи продукти, докато сме в магазина или даже да поръча такива по Интернет. В този ред на мисли всичко и във всяка сфера на човешката дейност около нас става „умно“.

Възможностите за свързването на всички предмети се очаква да донесе огромни икономически ползи и да преобрази промишлените структури, където да се залечат границите между продукти и услуги, а също така и границите между различните сектори European Commission (2016, с. 7). Всичко това води до необходимостта от изучаването на възможностите, които предлага ИНО и прилагането му в сферата на образованието.

Методология на изследването

Анализираната тематика е нова и актуална, тъй като в науката изследванията на ИНО са в начален стадий и все още има сравнително малко резултати и установени постановки в тази област, като това важи с особена сила за нашата страна. Обхватът, ефектът и въздействията на ИНО все още са обект на прогнози, като преобладаващите данни са предимно оценъчни. До преди година се считаше, че броят на свързани устройства през 2020 г. може да достигне 50 милиарда, а някои източници говореха и за трилиони. Последните и по-сериозни изследвания сочат, че броят свързани устройства след три години ще достигне числото 30 милиарда IEEE Spectrum (2016). Други доказателства, потвърждаващи актуалност-

та на тематиката, са поставянето на ИНО в стратегическите планове и влагането на огромни финансови средства за неговото развитие от страна на технологични и индустриални гиганти като Бош, Дженерал електрик, Гугъл, Интел, Самсунг, Фуджицу, IBM, Майкрософт, Хюлет Пакард и много други ComputerworldUK (2017). **Освен значимите инвестиции от страна на частни фирми, влиятелни политически организации и структури като Европейската Комисия също отчитат важноста и насочват внимание към развитието и разрастването на ИНО** European Commission (2016). Такова единомислие и ентузиазъм от страна на частния и правителствения сектор относно развитието на определена технологична сфера е много рядко наблюдавано явление. То е факт, защото **освен икономическо и технологично, ИНО има също така, образователно и социално значение**. Възможностите да се следят обектите по електронен път (т.е. бързо и евтино) и да се оптимизират процесите около тях, като в същото време се предлагат удобства на крайния потребител – без значение дали това е фирма, организация, правителство или частно лице, пораждаят всеобщия интерес към този феномен. Възможностите за вземане на информирани решения за работата на устройства и процеси, води до големи икономически ползи и подобряване качеството на живота.

Обект на изследване в настоящата статия е Интернет на Обектите. Неговото изучаване и възможните му приложения са от огромно значение както за индустриалното, така и за образователното общество. Развитието на подходи за по-обстойно запознаване с ИНО е от голяма важност за всички, в това число бъдещи мениджъри, икономисти и администратори. Въпреки терминът „Интернет“ в ИНО, когато се разглежда свързването на обекти от нашето ежедневие, а не само компютри и устройства за мрежова връзка, е

необходимо да се знае, че тази нова свързаност не представлява втори Интернет. В познатата понастоящем глобална мрежа могат да се правят търсене на информация, да се осъществява комуникация между фирми, между крайни потребители и т.н. В ИНО свързването на всеки предмет към Интернет или друга мрежа, като тази на мобилните телефони, води до автоматизиране, контрол или управление на съответния обект с цел улесняване живота на хората. Предмет на изследване са средата и подходите, които позволяват на изследователи и студенти да работят върху платформи на ИНО и да създават и развиват свързаните с това умения и техники. ИНО е в своята начална фаза на развитие. Той се развива фрагментирано, без общ подход, на базата на създаване на различни приложения в различни сфери на живота, използвайки различни технологии и създавайки различни възможности.

Изследване на възможностите

Възникването на ИНО е неразривно свързано, освен с постиженията в минитюризацията на дигиталните устройства и глобалното развитие на Интернет, и с появата и развитието на радиоидентификатори от типа RFID (Radio-Frequency Identification) и NFC (Near-Field Communication). Те позволяват идентификация на всеки обект в минитюрни размери и на ниска цена, в редица случаи и без необходимост от източник на енергия. Друга важна, свързваща парадигма на ИНО са сензорните мрежи. С тяхна помощ са възможни ефикасният обмен на данни между различните обекти и идентифициране на тяхното състояние и разположение. За да може да се говори за изцяло изграден ИНО на някакъв етап, ще е необходимо съществуващите устройства и предмети (или обекти, които човекът има нужда да следи и управлява) да бъдат свързани. От една страна – помежду си, а от друга – с

човек или система за слеждане и управление, която да предприема някакво действие при необходимост. Свързването с Интернет или мобилна мрежа може да се разглежда като пожелателно, но на практика в съвременната дигитална епоха потребителите не могат да си позволят липса на достъп до произволен процес или устройство, което е част от тяхната среда и което за тях се нуждае от наблюдение или управление.

Изследванията на ИНО се свързват и с различните подходи за неговата класификация. От една страна това може да се направи спрямо клъстерите, които стоят в основата на ИНО – RFID и NFC, микропроцесорни и микроконтролерни системи, мидълуеър, комуникации и Интернет, безжични сензорни мрежи, облачни системи и аспекти на сигурността на всеки един от тези клъстери. Друг подход за класифициране е според обекта на приложение – умни градове, умна околна среда, умни водни ресурси, интелигентни измерватели, защита и спешност, търговия, логистика, индустрия, умно земеделие и животновъдство, умни домове (една от най-бързо развиващите се сфери на приложение на ИНО) и умно здравеопазване.

В подхода, който беше възприет в проекта за изграждане на платформа за изследване възможностите и приложенията на ИНО се обърна внимание на най-популярните и използвани в световен мащаб малки управляващи контролни микропроцесорни системи, някои от които с възможностите, които разполага съвременен лаптоп или настолен компютър. Проучените и анализирани възможности на такива системи доведоха до избор на среда и съответно – създаване на платформа, с помощта на която могат да се правят различни проекти и да се провежда изследване спрямо избрани целеви групи (напр. наблюдение на околна среда, логистика, умни домове и т.н.). Платформата за изследване на ИНО включва хардуерни модули, комуникационни модули и софтуерни среди за програмиране, които служат за основа и

предоставят възможности за надграждане и използване на платформата в разнообразни приложения.

През последните години се появиха, и са в процес на утвърждаване и развитие, различни облачни услуги, с помощта на които е възможно разработчиците и потребителите да събират и изпращат данни в облак, да зареждат и анализират събраната информация и да използват различни сценарии за по-нататъшното развитие и усъвършенстване на приложенията. Сред най-известните такива услуги са AWS (Amazon Web Services) IoT (2015 г.), Microsoft Azure (от 2015 г.), IBM Watson Internet of Things (IoT) и др. Тези услуги работят така, че да поддържат различни устройства и протоколи, притежават вградени механизми за сигурност и възможности за връзка с мобилните мрежи. Освен че събират, облачните услуги също така съхраняват и анализират данните (които могат да бъдат в много големи размери), като последните може да се прехвърлят и обменят в необходимата за клиента посока (от и към облака).

Образование и ИНО

В областта на образованието има все по-масово въвеждане на технологиите, като наборът от различни ресурси и инструменти (Интернет, видео, звук и т.н.) се ползва успешно в съвременните класни стаи. Освен компетенциите на преподавателите, интелигентното ползване на данни от обучаемите (ученици и студенти) ще доведе до персонализация на обучението, където ще бъдат отчитани и съобразени индивидуалните нужди на обучаващите се. В този процес, ИНО безусловно ще промени начина на преподаване, а с това – и възприемането на лекции и упражнения.

Може да се направи следното структуриране от гл.т. на прилагане на ИНО в областта на образованието спрямо целева група, към която е насочено влиянието на ИНО.

1. Хора – насоката е образователният процес да не протича непременно в класни стаи/аудитории. Същият може да е онлайн, като учащите могат да бъдат на всяко място извън учебното заведение. Споделянето на информация чрез стрийминг или видео в реално време се допълва от характеристики за ИНО възможности да се предава или симулира състоянието на произволен обект, който е предмет на учебния процес. Обучението ще може да включва и различни данни от реално време от реални места, което ще води до значително по-качествени практически умения.

2. Процеси – една от много важните съставки на образователния процес е оценяването. С възможностите на новата възможности от ИНО може да се добавят обратни връзки от представянето на обучаемите. Резултатите на ученици или студенти от решаването на даден проблем или задача могат да бъдат сравнявани с резултатите на други, при това в реално време. Става възможно използването на виртуални среди за обучение, споделяне или използване на средства за обучение, събиране на информация за навиците на обучаемите и др.

3. Данни – при ИНО всички свързани обекти (неща, устройства) позволяват предоставянето на разнообразна и все полезна и интересна информация. Данните престават да бъдат просто числа в някакво представяне, а анализирана информация от машини и облачни услуги, които са удобни за по-нататъшно използване и бързо вземане на решения. Учащите се могат да получат достъп до проекти, свързани с изследване на животни в естествената им среда в реално време чрез уеб камери и сензори, прикрепени към телата на животните, да следят в реално време изменението на климата или състоянието на океаните, процеси в земеделието или животновъдството и т.н.

4. Обекти – това са физическите елементи, които чрез сензори или RFID/NFC се

свързват към Интернет и съответно – хората. С помощта на сензорите може да се следи температурата на някаква конструкция при различно натоварване в реално време, или пък интензивността на трафика в критично място/кръстовище. Самите обучаеми може да събират данни от обекти на места, където до момента това не е правено. Сензорите и RFID/NFC могат да играят много важна роля в безопасността на обучаващите се. Интегрирането им с наблюдателни камери може да гарантира зони за безопасност, която да се ползва от ученици и студенти, а в същото време да се наблюдава от родители и учители. Връзката между реални обекти и обучението води до много по-добро разбиране на функциите и ролята на тези обекти в контекста на образователния процес.

Изследване на опасностите

Заедно с бързото развитие и разрастването на Интернет на обектите, съществуват множество проблеми и опасности, които трябва да се познават и за които е важно да се положат усилия за тяхното преодоляване. В глобален аспект може да отличим следните категории проблеми, когато се разглеждат различните решения на приложения на ИНО:

- Стандартизация на Интернет на обектите – въпреки че съществуват инициативи за стандартизация, все още няма цялостна, интегрирана и единна система за стандартизация в тази област – даже в отделните сектори все още не е постигнато разбиране за това как и кои стандарти да се ползват, нещата се правят ad hoc;
- Протоколи за пренос на данни – съществуващите утвърдени протоколи за пренос на данни в Интернет (например протокола TCP/режовият протокол за управление обмена на информация TCP - Transmission Control Protocol) не са подходящи за ИНО, за-

щото са твърде неефективни при преноса на данни от сензори, както и от RFID/NFC.

От времето на неговия зародиш до момента, се счита, че най-големите опасности пред ИНО са сигурността и поверителността на данните. Според едно изследване, което анализира над 750 публикации в областта на „Интернет на обектите“ Yап, В 2015, pp. 1285–1300, най-често разглежданият проблем при ИНО е сигурността. В тази област, най-ярко се открояват теми за автентикация и конфиденциалност.

- Автентикация – много често това е трудна задача за ИНО поради факта, че е необходима подходяща инфраструктура (ресурси като памет, процесор), която невинаги е достъпна. Заедно с това „обектите“ са значително ограничени в сравнение с традиционните комуникационни и компютърните устройства, поради което за тях е трудно да изпълняват функциите по автентикация. Последните са добре усвоени от работещите дигитални устройства в съвременния Интернет – сървъри, рутери и персонални станции.
- Конфиденциалност – когато обектите са от домайна на личното/неприкосновеното пространство на всеки човек (или организация), тогава съществува огромна опасност от достъпът и събирането на частни/лични данни. Контролът върху разпространението и неоторизираното използване, на тези данни с наличните в момента технологии на ИНО е изключително трудна задача.

Поради леснотата на изграждане и влизане в употреба, повечето комуникации в ИНО са безжични, което ги прави лесни за подслушване и манипулиране. Голяма част от цифровите компоненти в ИНО, поради факта, че се добавят в миниатюрен вид към даден обект, се характеризират със слаби енергийни и изчислителни възможности (характерно за пасивните RFID системи). Това от своя страна не позволява изграждането на сложни и съ-

ответно – по-сигурни решения, каквито се прилагат при други дигитални системи. Едно изследване сочи, че 70% от устройствата в ИНО са уязвими към кибератаки – HP (2014). Последните са вече ежедневие в нашия живот, но понастоящем те напускат сферата на персонални компютри, сървъри и Интернет и започват да използват ИНО – The Royal Institute of International Affairs (2017), а там ще-тните и обхвата са несравнимо по-големи от тези, които са в съвременния Интернет.

Поради непрекъснатото развитие на ИНО е трудно да се покаже какви заплахи ще се появят след месец, година или пет години, но е логично да се предположи, че предстоящите заплахи ще са повече и по-опасни от съществуващите днес. Въпреки тази несигурност, ние се нуждаем от непрекъснато внимание в тази област и от постоянно повишаване на средствата за сигурност в ИНО. Идентифицирането на заплахите в ИНО е и ще продължава да бъде важна област на настоящи и бъдещи изследвания – Воуапов (2017), Nabib (2015).

Приложни приноси и насоки за развитие

От извършените изследователски и научно-приложни дейности на проекта *Създаване на платформи за изучаване на подходите за приложения в Интернет на обектите* могат да бъдат обособени следните по-важни приноси с научно-приложен характер:

- Проучени са сферите на приложения и състоянието на ИНО;
- Проучени са добрите практики, възможностите, опасностите и заплахите, които съществуват в областта на ИНО;
- Направен е анализ на възможностите за приложение на ИНО в областта на образованието;
- Създадена е платформа за работа, на която студенти и изследователи могат да създават модели и изследват поведението на различни приложения на ИНО;

- Създадени са учебни помагала за студентите, които да им помагат в работата им със създадената платформа;
- Реализирани са курсови и дипломни работи в областта на ИНО;
- Предложени са модели за изграждане и изследване на приложения, подходящи за различни научно-приложни дейности;

В рамките на периода на проекта пет студенти от 3-и и 4-и курс участваха активно в неговата работа, а над 20 проявиха сериозен интерес, при което всички те разработиха малки примерни приложения, запознавайки се с платформата и възможните и приложения. Много важно е да се отбележи, че този интерес продължава и ще бъде много полезно и важно ИНО тематиката да продължава да се развива. Възможно е предоставяне за работа на някоя от водещите ИНО облачни платформи, които за жалост са в редица случаи платени, което не помага на образователните институции, ще разшири уменията и възможностите на изследователски екипи и студентите, които работят по тези тематикати.

Заклучение

Интернет на Обектите има потенциала да промени основно начина, по който ние взаимодействаме със средата около нас – в дома, в града, в офиса, в болницата, в транспорта, в селското стопанство и навсякъде другаде. Възможността да следим и управляваме обектите от физическия свят с дигитални средства (мобилни телефони, умни часовници, други електронни уреди) предоставя нов свят за човешката дейност – оптимизирани процеси и системи, които спестяват време на хората и бизнеса и подобряват качеството на живота. Това се вижда и оценява от бизнеса – разрастването на ИНО продължава, при това в бурни темпове и според McKinsey Global Institute (2014), въздействието на ИНО върху глобалната икономика може да достигне

6.2 трилиона долара до 2025 г. Освен бизнеса, с този феномен е важно да се занимават и образователните институции, като се задълбочава обучението в ИО. Необходимо е фирми и институции да подкрепят образователните процеси в създаването на практични и полезни курсове и продукти, които да се използват от преподаватели, студенти и институции за едно по-добро бъдещо образование. За да стане възможно използването и внедряването на Интернет на обектите в неговия потенциал, преподавателите трябва да бъдат подготвени, както относно възможностите, които той предлага, така и за потенциалните рискове, които той крие.

Цитирани източници:

Business insider, Tech Insider, 2016. Here's why some are calling the Internet of Things the next Industrial Revolution [online] Available at: <http://www.businessinsider.com/iot-trends-will-shape-the-way-we-interact-2016-1>, последно посетен на 06 октомври 2017.

European Commission, 2016. Advancing the Internet of Things in Europe, [online] <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110>, последно посетен на 03 ноември 2017.

ComputerworldUK, 2017. The most powerful internet of things companies, [online] <https://www.computerworlduk.com/galleries/data/most-powerful-internet-of-things-companies-3521713/>, последно посетен на 6 ноември 2017.

IEEE Spectrum, 2016. Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated, [online] <https://spectrum.ieee.org/tech-talk/telecom/internet/popular-inter->

[net-of-things-forecast-of-50-billion-devices-by-2020-is-outdated](#), последно посетен на 10 октомври 2017.

Yan, B., Tian-Shyug Lee, Tsung-Pei Lee, Mapping the intellectual structure of Internet of Things (IoT) field (2000-2014): a co-word analysis, *Scientometrics* (2015) vol. 105, pp. 1285–1300, Budapest, Hungary.

The Royal Institute of International Affairs, 2017. The Internet of Things Will Be Even More Vulnerable to Cyber Attacks, [online] <https://www.chathamhouse.org/expert/comment/internet-things-will-be-even-more-vulnerable-cyber-attacks>, последно посетен на 7 ноември 2017.

HP, 2014. HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack, [online] <http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WhAnt1WWa70>, последно посетен на 7 ноември 2017.

Boyanov L. and Z. Minchev, Digital transformation disruptive threats identification, *International Scientific Journal*, year 2, issue 2/2017, ISSN 2543-8582, Scientific Technical Union of Mechanical Engineering Publ., pp. 64-65.

Habib K and W. Leister, Threats identification for the smart Internet of Things in eHealth and adaptive security countermeasures, 2015, Proceedings of the 7th International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, IEEE, ISBN 15:978-1-4799-8784-9, pp. 1-5.

McKinsey Global Institute, 2014. The Internet of Things: Sizing up the opportunity, [online] http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_sizing_up_the_opportunity, последно посетен на 8 ноември 2017.