Проучване и сравнителен анализ при компютърни експертизи на системи в екосистемата на Индустриалния Интернет на Нещата (IIoT)

Невена Петрова

***Резюме**: Цел на статията е проучване и сравнителен анализ на системи в екосистемата на Индустриалния Интернет на Нещата, съпоставяйки основните им характеристики, техните предимства и недостатъци, с други, по-стари и добре изучени системи. Това служи за отправна точка в последващите идеи за заимстване на вече известни методи за компютърна експертиза на дигитално съдържание за изследване на компрометирани данни в IIoT системи.*

***Ключови думи:** Интернет на Нещата, Индустрия 4.0, Компютърна експертиза*

Research and comparative analysis of digital forensics investigation in Industrial Internet of Things ecosystem

Nevena Petrova

***Abstract**: This article aims to observe and summarize the similarities, differences, advantages and disadvantages of Industrial Internet of Things systems, comparing them to well knows technologies. This serves as a starting point in the subsequent ideas for borrowing already known methods for computer expertise of digital content for the study of compromised data in IIoT.*

***Key words:** IoT, IIoT, SCADA, Industry 4.0, Digital Forensics*

1. ВЪВЕДЕНИЕ

Индустрия 4.0 представлява текущата тенденция в развитието на автоматизацията и обмена на данни при технологиите за производство. Това включва кибер-физични системи, свързващи механични и електронни части посредством софтуерни компоненти. Комуникацията им се осъществява върху една инфраструктура или свързани такива чрез облачни услуги. Терминът бива въведен в немските производствени фабрики и в последствие е широко приет в цял свят. Наименованието идва от идеята за четвърта индустриална революция, базирана на съвместното имплементиране на механика, електричество и информационни технологии в индустриалните системи. Такава революция е възможна след като Интернет на Нещата и Интернет на Услугите биват интегрирани в производството [5].

Индустрия 4.0 въвежда термина „умен завод“. В рамките на този завод кибер-физичните системи контролират физичните процеси, създавайки виртуално копие на физическия свят и вземат независимо и децентрализирано решения. Благодарение на IIoT кибер-физичните системи осъществяват комуникация помежду си и към човек в реално време. [7]

Нарастването на броя на „умните“ устройства и тяхното непрекъснато усъвършенстване внася развитието на нови технологии, свързани най-вече с изискването за непрекъсната комуникация между устройствата. Така се повишава и уязвимостта на системата и нуждата да се подсигуряват различни видове комуникационни методи. [1]

Това важи с най-голяма сила за Индустриалните Интернет на нещата, където допълнителни уязвимости са: нужда от бързодействие, обработката на голямо количество данни, работа в реално време и координиране с множество

устройства, част от които остарели откъм използвана технология.

Защитните механизми се преориентират да изпълняват функциите си еднакво добре, независимо от вида на устройството, което защитават. Често при Интернет на Нещата се прибягва до централизирано управление, където именно се поставят и въпросните методи за защита. По-комплексно е разследването, при което вече има кибер-физична атака. В този случай не може да се пренебрегне информация получена, от което и да е звено на системата. Актуалността на тази тема идва от сложността на анализите, които са необходими да се извършат, както и недостатъчната информация по темата.

Когато става дума за дигитално разследване и компютърна експертиза, с цел намиране на зловредно действие спрямо някоя машина, разследващите експерти заимстват разнообразни техники, използвани при вече познатите ни технологични решения. Те целят да проследят вътрешни и външни атаки, като наблягат на разследване според спецификите на комуникационните механизми и слабите звена в архитектурата на Интернет на Нещата.

При доказани престъпления, дори не само компютърни, почти винаги има дигитални доказателства – телефон, лаптоп и други устройства, които доказват конкретни действия на участниците в престъплението. Когато става дума за Индустрия 4.0 (или IIoT), трябва да се имат предвид спецификата на изграждане на една такава система. Дори алгоритъмът за анализ на компютърните доказателствени материали да е познат от дълги години и да съществуват много софтуерни продукти, които автоматизират анализите на данните, за спецификата на Индустрия 4.0, всичко това може да се окаже безполезно. Трябва да се вземе предвид, че една Индустриална Интернет на Нещата система по своето същество може да се приеме за един вид SCADA (Supervisory Control, Administration and Data Acquisition, преведено означава система на контрол и извличане на данни). Този вид системи се базира на софтуер за следене и контрол, който обикновено има визуализиращ модел на процесите и позволява комуникация със сензорите, механичните устройства (клапи, помпи, колела и др.) и контролерите. Понякога устройствата са „умни“ и самостоятелно реагиращи, а друг път са свързани с контролер, който е инициатор на действие. В първия случай устройствата са защитени от кибер атаки, защото решението за конкретно действие не идва от друга система през комуникационен канал, но все още са подвластни на физични такива. При втория случай освен споменатото се добавя и връзката между контролера и клиентската система, която се нуждае от протоколи за комуникация, които от своя страна определят различни мерки на подсигуряване – криптиране, кодиране, методи на автентикация и други. Често за комуникация в по-широки граници се налага и превеждане на протоколите в често използваните стандарти за комуникация като TCP/IP. [13]

2. СРАВНИТЕЛЕН АНАЛИЗ НА ТРАДИЦИОННИТЕ КОМПЮТЪРНИ СИСТЕМИ: IOT И IIOT. СПЕЦИФИКА НА IIOT.

Поради скорошното обособяване на IIoT като отделна технология за Индустрия 4.0 започва да се говори през 2015. До момента няма достатъчно точна методика за нейните компютърни експертизи. Ето защо е добре да се започне от познати методи, които се прилагат за подобните вече SCADA или IoT технологии.

2.1. Основни характеристики на SCADA. С какво IIoT е по-добра технология?

- Събиране на данни

SCADA системите са се наложили толкова в индустрията заради голямото количество данни, което са започнали да складират, подпомагайки бизнес решенията. Сензори, контролери и други модули работещи в реално време изиграват основна роля в събирането на тези данни.

- Предаване на данни

За комуникация и предаване на информация между клиент и устройства SCADA системата създава мрежова свързаност. Тази свързаност изисква и конкретни решения за сигурност, в зависимост от вида и особеностите си.

- Представяне на данните

Тъй като има голямо количество информация, складирана от SCADA, важно е да се отдели и обработи важната такава. Интерфейс „човек-машина“(HMI) прави визуализацията и презентирането на нужните данни.

- Контролиране и следене

SCADA системите използват ключове, за да оперират с различните устройства, така ги включват или изключват. SCADA системата работи автоматизирано, без намеса на човек, но при нужда има възможност човекът лесно да се включи.

PLC (programmable logic controller) е технология, която акомпанира SCADA през последните десетилетия, но поради технологичния напредък, е вече остаряла. PLC получава данни от сензорите и я препраща на базата с предварително зададени параметри. Има възможност да се запишат и следят данните в реално време, както и автоматично да спират или стартират процеси в производството, да се генерират аларми, ако се намерят проблеми с функционалността.

IIoT подобрява това, като внася възможности за автономно вземане на решения и обучаване на машините. Изгражда се цялостна екосистема, която се саморегулира, самообучава и променя, не само според предварително зададени параметри, а

според статистики и анализи. Тази технология се появява като разширение на SCADA. Често двете дори оперират заедно, като SCADA информацията служи за основа на по-горното ниво от IIoT инфраструктурата. В литературата двете системи не само не се изключват една друга, а често се гледа на IIoT като специфична SCADA система. [13]

2.2. Диференциране на индустриалните (IIoT) от неиндустриални (IoT) технологии.

Важна разлика между системи тип Интернет на Нещата и Индустриален Интернет на Нещата е, че производствените технологии са създадени с цел по-продължителен живот и работа в индустриални условия – топлина, влага и др. Поради продължителността на живот от порядъка на десетилетия и по-високата цена на замяна, в индустриалните системи се получава смесица от старо и ново оборудване и технологични решения. Освен това много от тези системи трябва да подсигурят оперативно време 24×7.[4]

IIoT се отнася за подкатегория на по-обширното понятие IoT. IoT включва в себе си и неща като „умни“ аксесоари, печки, хладилници и всякакви подобни уреди за бита. Докато IIoT се фокусира изцяло върху индустриални технологични решения и устройства, използвани в производството, земеделието и разпределение на обществени ресурси и блага.

В много отношения IIoT превъзхожда IoT и тепърва ще се видят по-бързите темпове на напредък, заради основната разлика, а именно, клиентите. Индустриалните технологии обслужват бизнеса и големите индустрии. Те свързват критично важни машини със сензори, в индустрии от огромно значение за човечеството, като например самолетостроенето и въздушната защита, здравеопазване и изследвания, включително лабораторни, енергетика. Потенциална грешка и спиране на подобна система, води до множество финансови и ресурсни загуби, а понякога и човешки живот бива застрашен. За сравнение, масовата употреба на не-индустриалните IoT включва производство на спортни часовници, домашни електроуреди – перални, печки и други. Употребата на един такъв уред е значително по-маловажна и евентуалното спиране на работа не донася до големи последици. Именно това са основните „двигатели“ за развитието на IIoT с по-големи темпове от IoT.

2.3. Потенциал на IIoT

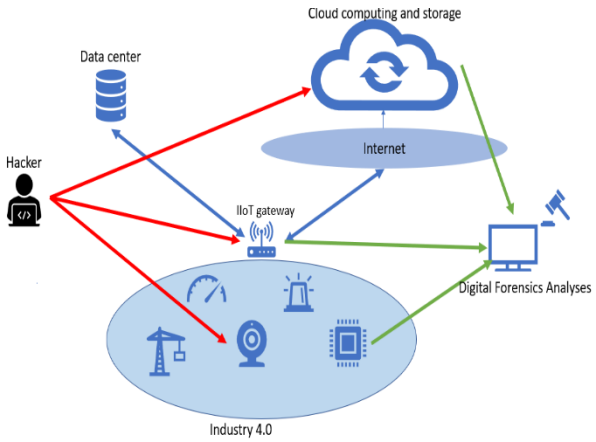
През последните години иновации в хардуера, свързаността и анализирането на големи количества данни, както и машинното (само)обучение (machine learning) създават множество възможности за индустриите. Хардуерните иновации водят до по-евтини и чувствителни сензори, батерия с по-дълъг живот и други. Подобренията в свързаността означават по-евтино и бързо изпращане на данни към облачната система или електрическите и механични части. Всичко друго допринася за задълбочен анализ и възможността системата да се саморегулира много по-успешно, следователно по-добра автоматизация. Намаляване на човешката интеракция с електрическите и механични части, освен всички познати плюсове за бързодействие и надеждност, подобрява и условията на труд за работниците и намалява риска за живота и здравето. Подобрявайки автоматизацията, като я развива до едно нови ниво, вече е възможна и автоматизирана поддръжка. Става лесно задаването на предварителен алгоритъм, който да бъде следван през определено време, за да се прави планирана профилактика и да се отстранявам проблеми, преди те да нарушат реалната работа на системата.

2.4. Бариери пред IIoT

Двете най-големи бариери при IIoT са сигурността и взаимосвързаността при работа.

Когато свържем физическите системи в заводите онлайн, ние внасяме много новости, които подпомагат ежедневната работа. Но в същото време подлагаме системите на нови възможности за компрометиране. Кибератаките са изключително опасни, когато могат да поемат контрол върху управлението на системите или да повредят част от хардуера. Последиците могат да бъдат огромни финансови загуби, сериозни проблеми за здравето на хората, работещи там, а в най-лошия случай дори летален край. Ето защо на сигурността трябва да се гледа с особено внимание и да се отчете, че това е голямо предизвикателство пред IIoT, което трябва непрекъснато да бъде компенсирано чрез различни защитни механизми.

За да се съберат данните от сензорите и да бъдат полезни, всички части на системата трябва да бъдат свързани и да работят заедно. За да се избегнат проблеми в тази насока, се създават стандарти за работа и свързаност, комуникационни и работни протоколи, процедури и процеси, които да ръководят непрекъснато взаимосвързаността. Без тази свързаност, цялостната идея за IIoT бива прекъсната и преимуществата и са загубени.



Фиг.1. *Схема на движението на информация в Индустрия 4.0, уязвимите места, където обикновено системата бива атакуване и от които се снемат данни за анализ.*

3. МЕТОДИ НА ЕКСПЕРТИЗА ПРИ РАЗСЛЕДВАНЕ НА КИБЕР ПРЕСТЪПЛЕНИЯ. ТЕОРЕТИЧНО ОПРЕДЕЛЯНЕ НА ПОДХОДЯЩИ ЕКСПЕРТИЗИ ЗА IIOT СИСТЕМА.

Обработката на данните, за да се разбере кой какво престъпно деяние е извършил, както и с чие съдействие/знание, кога и как се е случило са основната цел на компютърния анализ на данни. Този анализ попада в границите на по-голяма концепция – откриване на електронни сведения – процеса на събиране на данни, документи или имейли, като подготовка за законови мерки, които от своя страна да доведат до процес.

Част от анализа е обект на правото и статията ще се придържа към инженерната част.

Компютърните устройства не само служат на своите потребители по предназначение, но също така пазят данни за активностите, които са обслужвали по време на работа. Тази информация може да бъде срещната под имена като дигитални детайли или дигитален отпечатък (по аналогия с физическия отпечатък, който еднозначно идентифицира конкретен човек). Веднъж влезли в електронна форма, почти всеки тип данни се анализира независимо и отделено от устройството и приложението, от които са създадени. Специализираните софтуери за анализи на кибер сигурност правят този процес възможен и по-лесен, но винаги присъства и човешкия фактор. Когато се инспектира дадено устройство, целия твърд диск се представя като единствен файл, който позволява търсене. Нарича се изображение (image) и всички скрити места от паметта са видими.

Важно начало на анализа, след като бъде възложен, е какъв е типът на системата и нейното приложение. В последствие къде и как са запазени данните, ако има такива.

Системите за съхранение (Твърдият диск, SSD, Flash.) е огромно информационно пространство, а при извличане на данни, понякога се извличат и детайли за предходни записи, които вече са унищожени. Знаем, че системите за съхранение всъщност не изтриват файл, а само преместват флага на записване върху място в паметта, на което вече може да има съществуващ запис. В последствие при процеса на четене се игнорира маскираният „несъществуващ“ файл. Проблеми при възстановяването на такъв файл идват едва след като в тази част на паметта бъде записана нова информация. [3]

Като основа може да се вземат известни методи за описание на IoT [1], надграждайки я с конкретно приложение и допълнителни характеристики за Индустриална среда на работа (Индустрия 4.0). Атрибутите на едно разследване в сферата на IoT са: фази на разследването; предпоставки, които правят определено разследване възможно; мрежи; източници на сведения; видове разследвания; модели на разследване; слоеве; средства, спомагащи разследването и обработващи данните.

При определяне на фазите на разследването, обикновено се започва с дефиниране на контекста, в който ще се изследва. Разследващият екип прилага разнообразни оценки на сигурността, ползвайки често софтуерни приложения. Някои предлагат възможност за събиране на голямо количество данни от различни локации. Различни законови рамки и норми трябва да се определят предварително, като например право на собственост (включително интелектуална), лични данни, местни и държавни закони за информационните технологии и комуникационните технологии (в различни страни има различни забрани и регулации за информационните комуникации). Следва снемане на различни по вид и големина доказателствени материали, Източниците също могат да варират, както и технологиите за събирането им. Те ще бъдат детайлно анализирани на последващ етап. Последната част е крайно заключение на експертите, на базата на информационния материал, с който разполагат. Предоставя се подходящо документиран и презентиран анализ пред заинтересованите юридически лица. Последна задача на експертите изготвили експертизата е да архивират информацията за последващи нужди.

3.1. Система за надзор и проследяване на доказателствата (Chain of custody)

Основен термин, използван за описанието на работата по експертизата е система за надзор и проследяване на доказателствата (на англ. Chain of custody). [16] Chain of custody (CoC), е хронологично подредена документация или

писмени сведения, които описват последователността от задържане, контрол, прехвърляне, анализи и унищожаване на физически или електронни доказателствени материали. [15]

Експертизата на дигитални доказателства включва – събиране, съхранение, доказване, идентифициране, анализиране и записване на информацията от местопрестъплението.

Експерт по разследване на компютърни престъпления следва определени етапи и процедури, когато работи по случай. Първо трябва да се разпознае престъплението и компютъра или други технически инструменти, които са били използвани за извършването му. Следва събирането на доказателства и изготвяне на подходяща хронологически описана документация за предприетите стъпки на разследване, която ще бъде внесена в съда заедно с доказателствените материали.(chain of custody). Следването на процедурите при тези разследвания е възможно най-стриктно, за да не се повлияе или наруши доказателствения материал, което в последствие да се използва като довод за невалидно доказателство.

Стъпки, които обикновено биват извършвани от експерта при разследването:

1. Събиране и снемане на доказателствения материал от местопрестъплението, както и транспортирането до подходяща лаборатория.
2. Представяне на информацията под формата на битове, като за всеки файл се изчислява хеш функция. Това гарантира интегритета на информацията.
3. Проверка на данните с цел проверка за извършено престъпление. Целият анализ се оформя в детайлен доклад.
4. Предоставяне на изготвения доклад на заинтересованите следователи и възложители на експертизата, които ще решат дали има основание за повдигане на обвинения.
5. Разследващия унищожава всички чувствителни клиентски данни.

От голямо значение е експертът да следва точните стъпки и процесът да не съдържа стъпка, която може да се разтълкува грешно или е неясна.

Правила на компютърната експертиза:

- Оригиналите на доказателствата да се изследват възможно най-малко, вместо това да се работи с копия.
- Следват се точни правила, без да се подправят доказателства.
- Винаги се създава алгоритъм на разследване и хронологично описание(chain of custody), който е задължителен за следване.
- Никога да не се използват непознати за експерта техники за обработка, ако се налага се въвежда друг експерт.
- Всеки тест, който води до промяна, или друга промяна върху доказателствата, се документира незабавно. [6, 14]

3.2. Специфики в IoT и IIoT системите, които да имаме предвид, когато разследваме потенциално злонамерено действие:

Интернет на Нещата е композиция от разнообразие от технологии, например сензори, мобилни устройства, виртуализации, облачни решения, RFID (радио-честотна идентификация), мрежово оборудване и изкуствен интелект. Тези технологии имат своята индивидуална роля в разследването на дигиталните доказателства. Основните IoT устройства, например сензори, се използват, за събиране на данни от местопрестъплението след атаката. Облачните и виртуализационни технологии предоставят различна поддръжка (при поискване, скалируема, еластична, с отдалечени изчисления) по време на цялото разследване. RFID е използвано почти изцяло при сензорни устройства за идентификация на обекти. Мрежовата екипировка като маршрутизатори и комутатори позволява следенето на пакети данни. Изкуственият интелект подпомага анализа на събраните данни (изключително важно при Industrial Big Data).

Мрежата в този контекст служи за описание какъв вид свързаност се използва за взаимовръзка на IoT устройствата на местопрестъплението. Тя играе важна роля по време на разследването и подсигурява покритие на района. Локална мрежа (LAN), Регионална Мрежа (MAN) и частна мрежа (PAN) са предимно използваните видове за взаимосвързаност при ограничено разстояние. Като пример може да посочим камерите за сигурност, инсталирани на улиците и в търговки центрове. Домашните електроуреди - хладилник, пералня, се свързват с така наречената домашна мрежа (HAN). А за устройства на голямо разстояние и нужда от Интернет връзка, се използва мрежи със широко разпространение (WAN).

1. Източник на сведения

Информацията, касаеща престъплението при IoT може да събере от различни местопрестъпления, фокусирайки се върху основни източници на данни, като домашни електроуреди, сензори, медицински импланти, вградени системи и автомобили. Въпреки, че паметта им е малка, ценна информация се изпраща до централен обработващ компютър, за да я препредава към мрежата. Данни каквито са системните регистри и временната кеш памет също могат да се използват като източник на информация. Този вид информация може да бъде извлечена чрез следене на множество устройства в мрежата, като маршрутизатори, комутатори и други.

2. Режими на разследване

Режимът на разследване категоризира типът на разследване според времевата линия на разследване. Статичен режим е традиционно методът използван след идентифициране на атака в IoT системата. Като резултат на атаката, данните са вече компрометирани или изтрити. Статичният режим възстановява данните, използвайки универсалната серийна шина (universal serial bus) или сканирайки кашираните данни. Интернет на Нещата дигиталното разследване, както повечето такива, понякога изисква системата да е "жива" докато се снемат актуални данни като отворени мрежови връзки, дъмпове от паметта, работещи процеси и др. Този начин на работа е познат като динамичен режим.

3. Модели на дигитално разследване

Те трябва да са аналогични на стандартните модели на работа с доказателства. Целта е да бъдат признати в съдебната зала. Всички познати стандартни модели следват основни фази на разследване - определяне на контекста на работа, събиране на материали, разследване, анализ и представяне на данните в подходящ вид.

Моделът на разследване на дигиталните технологии (DFIM) е четирифазен, като основно цели да разкрие срити доказателства. Той не е насочен към физически доказателства, което не е винаги удачно при Интернет на Нещата системите. Както е обяснено нагоре в статията, Индустрия 4 е кибер-физична, ето защо физичната част на разследването трябва да се има предвид, когато се анализира дигиталната.

IoT разследванията се състоят от 4 слоя на работа: устройство, мрежа и облачен слой. (обикновено в литературата се разглеждат три слоя.. но е добре да се добави четвърти – човешкия фактор)(При разследването на ниво устройство, разследващият събира данни предимно от устройства, при които данните са прецизно запазени в локалната памет.

Мрежовият слой събира данни от мрежовите устройства, за да осъди или обвини заподозрения. Устройствата тип Интернет на Нещата обикновено комуникират чрез разнообразие от технологии, както вече беше описано в статията. За разследване тук служи запис на действията в мрежата (log), кашираната памет и други. Повечето устройства имат ограничена памет и капацитет за обработка на данни, затова използват облачни хранилища за данните си. Разследването на облачните устройства е друг дял, който служи за събиране на данни за атаката. [1, 11, 14]

4. ИНСТРУМЕНТИ ЗА РАЗСЛЕДВАНЕ И АНАЛИЗ

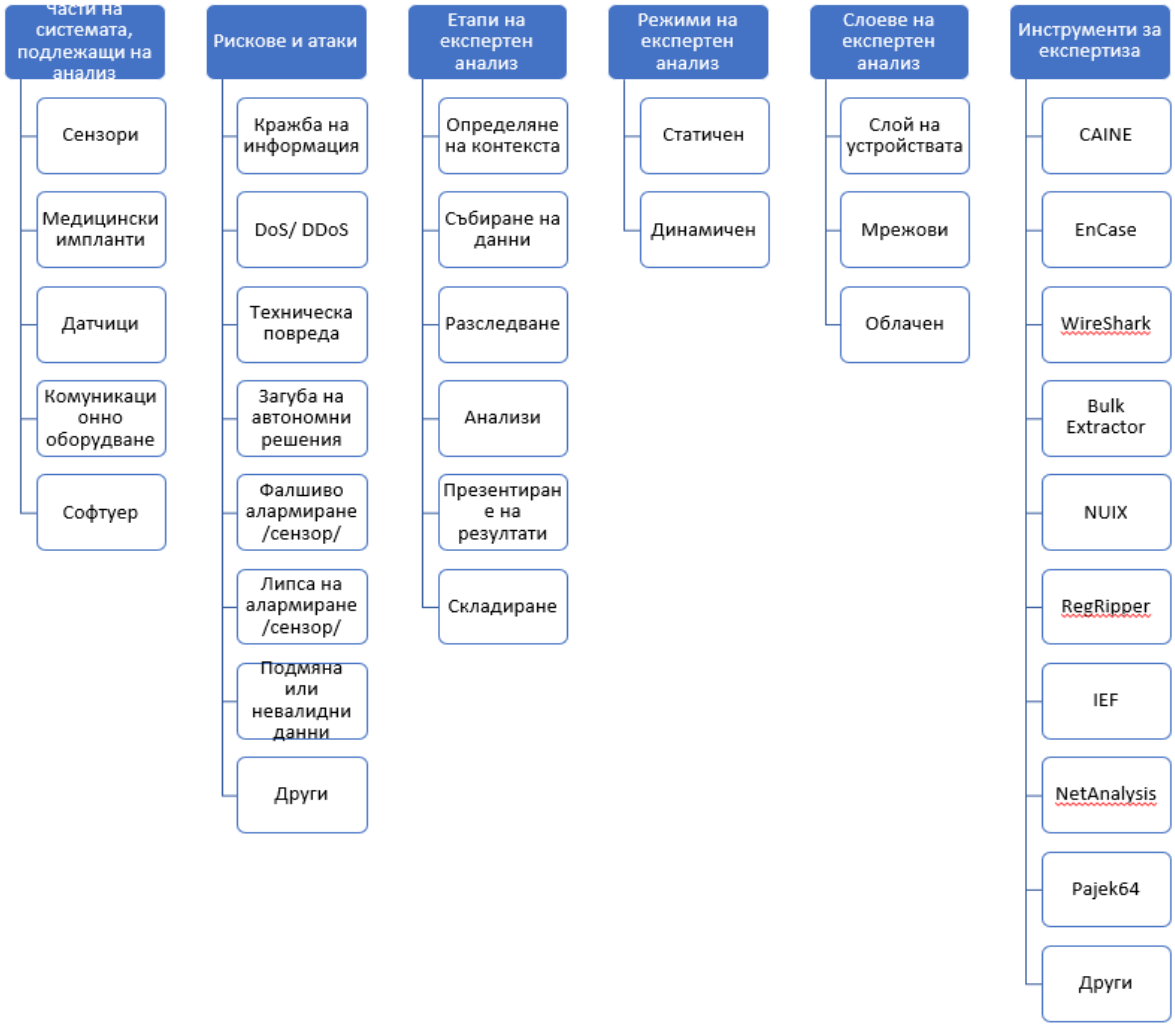
Разследването на престъпление срещу една Интернет на Нещата система се извършва само от добре обучени експерти по сигурността, които имат познания в техническата материя и знаят законовата рамка. Много от трудностите, които се внасят от спецификата на разследването, когато злонамерените действия са при Интернет на Нещата системи, са детайлно описани в статията до момента. Сложността е ясно забележима. Ето защо експертите, които се занимават с тези разследвания се нуждаят от специални инструменти, които да подпомогнат работата им.

Computer Aided Investigative Environment (CAINE) например е интерактивен инструмент с "отворен код", който поддържа повечето от фазите на разследването. EnCase се използва за анализ на снимки, данни и файлове. Анализ на процеси и др. Wireshark е основно използван при разследване на мрежовата дейност. Проблем при него може да бъде работата с голям набор данни. Bulk Extractor подпомага сканирането и изтеглянето на информация като номера на карти, телефони, имейл и уеб адреси. NUIX се използва за големи количества данни, които да се обработят така, че по-късно експертите да могат да ги използват. RegRipper сканира Windows регистрите. IEF анализира история на браузери, чатове и операционната система. NetAnalysis служи по подобен начин за интернет историята. Pajek64 служи за голям обем мрежова информация.

Обработката на данните се отнася за начинът на изчисляване, по който разследването бива извършено. При централизирана обработка, доказателствените материали се складират в един силно подсигурен сървър, който може да бъде достъпен от различни локации само от разследващи, на които е даден достъп. Това е евтин и много сигурен модел на работа. Разпределената обработка на данни е тази, при която данните са разпръснати на няколко сървъра. Бързодействието е голям плюс, но за сметка на сигурността и нуждата от широк канал на предаване на данни. [1]

Всеизвестно е, че всички познати инструменти за експертиза при разследване на дигитални данни за престъпление, са ограничени. Смята се, че е трудно да отговарят адекватно на непрестанното развитие на технологиите и атаките към тях. Съвременните инструменти не успяват да отговорят добре на изискванията на IoT и IIoT за хетерогенност (множество различни технологии и симбиоза от комуникационни протоколи). Ето защо трябва да се изгради колаборация от няколко анализиращи програми и инструменти. Също така да се заложи на подходящ софтуер и хардуер, които да отговорят на изискванията на избраните инструменти за експертиза и обема данни, които ще се разследват. Множеството способи за разследване имат своите спецификации на работа

и следователно експертите се нуждаят от развиване на способностите си.[18]



Фиг.2. *Схема на участниците, методите и инструменти за анализ.*

5. ЗАКЛЮЧЕНИЕ

В статията:

- Са изследвани иновативните решения и плюсовете при Индустрия 4.0 и IIoT. Както и проблемите на сигурността в същите.
- Съпоставени са Индустриални Интернет на нещата с Интернет на нещата в дома и други добре известни технологии. Направен е паралел между тях.
- Въз основа на сходствата си с други технологии и използвайки вече познати методи за анализ на данни при киберпрестъпления, е направен анализ на инструменти, които могат да бъдат използвани за разследване при Индустрия 4.0.

Фигура 1 показва схематично как е изградена една система в Индустрия 4.0, къде може да има злонамерено действие и съответно се направи експертен анализ за киберпрестъпление.

БИБЛИОГРАФИЯ

[1] Ibrar Yaqooba, Ibrahim Abaker Targio Hashemb, Arif Ahmeda, Internet of Things Forensics: Recent Advances, Taxonomy, Future Generation Computer Systems, September 2018

[3] Reynaldo Anzaldua, Linda Volonino, *Computer Forensics For Dummies,* For Dummies, October 2008

[4] Carolina A. Adaros Boye, *Understanding Cyberrisks in IoT,* Business Expert Press, May 2019

[5] Alasdair Gilchrist, *Industry 4.0: The Industrial Internet of Things,* Apress, June 2016

[6] J. Wiles, A. Reyes , J. Varsalone, The Best Damn Cybercrime and Digital Forensics Book Period, 2007

[7] Уикипедия: Индустрия 4.0, https://bg.wikipedia.org/wiki/Индустрия_4.0

[8] Shaider Electric articles about newest technologies, https://www.se.com/bg/bg/work/campaign/innovation/industries.jsp

[9]. ДАВИД Холдинг, https://www.david.bg/internet-na-neshtata-iot

[10] *От индустриалния „Интернет на нещата“ към „Свързано предприятие“. Част I и Част I I*, Ротек ООД, 18.07.2016 г., https://www.инженер.bg/kip/reviews/интернет-на-нещата-свързано-предприятие

[11] Calum McClelland, *The Industrial Internet of Things - What's the Difference Between IoT and IIoT?, Dec. 2016*, https://www.leverege.com/blogpost/difference-between-iot-and-iiot

[12] Уикипедия: Кибер-физична система, https://bg.wikipedia.org/wiki/Кибер-физична_система

[13] *Industrial IoT vs SCADA: Which is More Powerful?,* https://www.biz4intellia.com/blog/industrial-iot-vs-scada-which-is-more-powerful/

[14] *Smart Forensics for the Internet of Things (IoT)*, https://securityintelligence.com/smart-forensics-for-the-internet-of-things-iot/

[15] Wikipedia: Chain of Custody, https://en.wikipedia.org/wiki/Chain_of_custody

[16] Chain of custody - употреба на термина в български документи, https://www.linguee.com/english-bulgarian/translation

[17] *Forensics for the Internet of Things (IoT)*, https://securityintelligence.com/investigating-iot-crime-in-the-age-of-connected-devices/

[18] a. Alenezi, H. Atlam, R. Alsagri, M. Alassafi*, IoT Forensics: A State-of-the-Art Review, Challenges and Future Directions,* May 2019

За автора:

Невена Гугуткова, nevena.petrova@tu-sofia.bg
магистър инженер, докторант
катедра Теория на механизмите и машините
Машинно-технологичен факултет
Технически университет – София

Невена Гугуткова, nevena.petrova@bg.ibm.com
Разработчик софтуерни предложения – екип IP услуги,
Мрежова стратегия, архитектура и инженерство,
Ай Би Ем България.

About the author:

Nevena Gugutkova, nevena.petrova@tu-sofia.bg
Master of Engineering, PhD student
Department of Theory of mechanisms and machines
Faculty of Industrial Technology
Technical University of Sofia

Nevena Gugutkova, nevena.petrova@bg.ibm.com
Application Developer - IP Services Squad
Network Strategy, Architecture and Engineering,
IBM Bulgaria