IT4Sec Reports 132
http://dx.doi.org/10.11610/it4sec.0132

Моделиране, анализ, експериментална валидация и верификация на системи за информационна сигурност в корпоративна среда

Иван Гайдарски, Златогор Минчев

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, март 2019 г.

Иван Гайдарски, Златогор Минчев, Моделиране, анализ, експериментална валидация и верификация на системи за информационна сигурност в корпоративна среда, *IT4Sec Reports* 132, https://doi.org/10.11610/IT4Sec.0132

IT4Sec Reports 132 „Моделиране, анализ, експериментална валидация и верификация на системи за информационна сигурност в корпоративна среда“. Публикацията представя подход за изследване на сигурността на информационните системи в корпоративна среда. Решението включва концептуално UML мета-проектиране на архитектури, последвано от мулти-агентно системно моделиране и холистичен анализ на чувствителността. Получените резултати са валидирани посредством специализирана стохастична симулация, гарантирайки комбинирано използване и смесване на експертни, сензорни и машинно генерирани данни. В заключение е извършена и интерактивна верификация във виртуална корпоративна среда чрез фиктивен, футуристичен сценарий за динамично наблюдение на потребителите и технологиите. При това, с цел пълнота на изследването, са използвани DLP мониторинг за различните състояния на данните и атаките, в комбинация с избрано множество от потребителски оценки.

Ключови думи: проектиране на системи за информационна сигурност, DLP, UML архитектурно мета-проектиране, мулти-агентно моделиране и симулации, стохастична валидация, интерактивна верификация

IT4SecReports 132 Modelling, Analysis and Experimental Validation & Verification of Information Security Systems in Corporate Environment. The publication presents an exploration approach for studying data protection in security systems within corporate environment. The approach is including: conceptual UML architecture design, together with further multi-agent system-of-systems modeling and holistic sensitivity analysis. The obtained results are next validated via an ad-hoc stochastic simulation, assuring expert, sensors' and machine-generated data flows fusing and usage. Finally, an interactive verification is performed with virtual corporate environment and futuristic, fictitious scenario dynamic observations of both trainees & technologies. An implementation of DLP monitoring for multiple data states and attacks jointly with selected set of users' feedback assessments are given in conclusion, assuring comprehensiveness of the obtained results.

Keywords: Design of Information Security Systems, DLP, UML Architectural Meta-Design, Multi-agent Modelling & Simulation, Stochastic Validation, Interactive Verification

Благодарност:

Основната част от изследванията в настоящата работа са проведени с финансовата подкрепа на проект „Моделиране на архитектура на системи за информационна сигурност в организации“, Договор ДФНП 17-101/28.07.2017, Програма за подпомагане на млади учени и докторанти на БАН – 2017. Допълнителна благодарност за популяризиране на резултатите и събирането на данни в рамките на ученията CYREX 2018, авторите изказват на инициативата “Secure Digital Future 21” (http://securedfuture21.org).

ISSN 1314-5614

СЪДЪРЖАНИЕ

СПИСЪК НА ФИГУРИТЕ

I. ОБЗОР И АНАЛИЗ НА ЛИТЕРАТУРНИ ИЗТОЧНИЦИ И ГОТОВИ ПРОДУКТИ

Работата по тази задача включва обзор на съществуващата литература в областта на информационната сигурност (ИС), и конкретно – методите за проектиране на системи за информационна сигурност (СИС). В практиката са широко застъпени множество универсални стандарти за описание на системи за информационна сигурност, като:

- ISO 27000 [1], [2];
- COBIT на ISACA (Information Systems Audit and Control Association) [3], [4];
- “800 series" на NIST (The National Institute of Standards and Technology) [5].;

Съществуват и специални регулации за специфични сектори и индустрии:

- Gramm-Leach-Bliley Act (GLBA) [6] – финансов сектор;
- Sarbanes-Oxley Act (SOX) [7], [8] – публични компании в САЩ;
- Health Insurance Portability and Accountability Act (HIPAA) [9] – здравен сектор;
- Payment Card Industry (PCI) Data Security Standard (DSS) [10] – оператори на кредитни карти.

Намират и приложение специализирани стандарти като IEEE 1471 [11] и IEEE 42010 [12], описващи архитектури на системи чрез методите на концептуалното моделиране.

Определяне на системна рамка за описание на архитектурата на СИС и подходящи методи и средства за нейното реализиране

В зависимост от своя обхват и цели, системите за информационна сигурност могат да бъдат както специализирани, защитаващи конкретни компоненти от системата, като: firewalls, IDS (Intrusion Detection Systems), IPS (Intrusion Protection Systems), DLP (Data Leak Prevention) и други, така и комплексни, защитаващи информационните активи на организацията от изтичане, пробив, кражба или злоупотреба. Обикновено СИС от втория вид комбинират различни контроли за сигурност като изброените вече firewalls, IDS и DLP за постигане на цялостна защита на информацията, принадлежаща на дадената организация.

СИС може да се различават по посоката на векторите на атаките от които те защитават компонентите на информационната среда. Традиционният метод е посока отвън-навътре, защитавайки основно от атаки отвън – хакерски атаки, фишинг атаки и др. Целта е неутрализиране на тези атаки, така че атакуващата страна да не може да получи достъп до вътрешната мрежа и съответните информационни ресурси и активи. Такава защита са например защитни стени (firewalls), контролиращи каналите, осигуряващи мрежовият трафик. По-съвременен метод е защита от изтичане на информацията отвътре-навън. При тях се обръща специално внимание на т.нар. “инсайдъри” – вътрешни за организацията лица с достъп до чувствителна информация или ресурси. Типични контроли за ИС, използвани в тях са DLP системите, или системи за предпазване от изтичане на чувствителна информация като DeviceLock [13] и CoSoSys Endpoint Protector [14]. Чрез тях дори злонамереното лице да е получило достъп до чувствителна информация, е невъзможно тя да бъде изнесена извън организацията (системата). Разбира се двата метода могат да бъдат комбинирани с цел по-сигурна защита на информационните активи на организацията.

Някои от контролите за сигурност, използвани в СИС са проектирани за работа чрез локална инсталация в организацията. Такива са например firewalls, IDS, IPS и DLP решенията. Други контроли като Threat Intelligence Solutions или решения за ранна сигнализация от онлайн заплахи са типични сервизно-ориентирани решения, базирани извън организацията, обикновено в облака. Разбира се отделните контроли могат да бъдат базирани както вътре, така и извън пределите на организацията, в зависимост от конкретните цели на СИС.

Досегашният опит показва че мерките за информационна сигурност (ИС) в рамките на дадена организация обикновено са инцидентно базирани или касаят спазване на определени (единични) законодателни регулации, необходими за нейната нормална работа. В практиката намират приложение различни стандарти и регулации, като посочените по-горе.

Макар тези стандарти и регулации да претендират да включват в себе си най-важните аспекти на ИС, те са по-скоро набор от добри практики. Редки са случаите когато към ИС се подхожда методично и се спазват всички изисквания на стандартите. По този начин в практиката се подхожда „на парче“ за решаване на определени задачи от ИС, свързани с инцидент (изтичане на информация, атака към инфраструктурата, загуба на информация и др.) или с решаване на нововъзникнало предизвикателство – например приетия закон, касаещ защита и обработка на лични данни за граждани на ЕС, General Data Protection Regulation [15].

Подходи за развитие на СИС

Защитата на информационни активи е постепенен процес, който изисква координация, време и търпение. Обикновено този процес започна като всекидневни задача и усилие за подобряване на сигурността на отделни компоненти на СИС – подход „отдолу-нагоре“. При този подход не се следва предварително разработен и одобрен план, което прави невъзможно постигането на съответствия със стандарти и регулации, липсват редица важни и критични характеристики като мащабируемост, повтаряемост и съответно постигането на комплексни цели като цялостна защита на информационните активи на организацията. Тези цели могат да бъдат постигнати от другият подход – “отгоре-надолу”, в който проектът се инициира от мениджъри на високо ниво, създава се и се одобрява единна политика за информационна сигурност, процедури и процеси, които да диктуват целите и очакваните резултати. Този подход се характеризира с подкрепа от страна на висшето ръководство, осигурено финансиране, отчитане на изискванията на всички заинтересовани страни, както и участие на широк кръг специалисти, включително и външни за организацията.

Този подход е подходящ за създаване на референтна методология за разработване на СИС, основана на определяне на рамка за домейн анализ, която служи за изграждане на модели на СИС. Основни цели на тази рамка съвпадат с целите на рамката за архитектурно описание на системите в стандартите IEEE 1471 [11] и IEEE 42010 [12]. Те въвеждат понятия като: „Поглед“ – “View”, „Гледна точка“ – “Viewpoint”, „Заинтересовани страни“ – “Stakeholders”, и „Околна среда“ – “Environment”, свързани с описанието на архитектурата на системите. Тези концепции са приложими в анализа на домейна “Информационна сигурност” и осигуряват контекст за дефиниране на обща концептуална рамка, позволяваща изграждането на концептуални модели на СИС.

За архитектурно описание на СИС могат да бъдат използвани унифицирани езици за моделиране като UML [16], предоставящ инструменти за описание, анализиране,

моделиране и документиране на архитектурата на СИС. UML позволява на системните разработчици да описват изискванията към СИС и нейните компоненти, да скицират, модифицират и манипулират предложените архитектури, да използват многократно отделни компоненти на СИС, за комуникиране на информацията, събрана по време на разработката на системата. UML е обектно-ориентиран и осигурява стандартна нотация за анализ, проектиране и внедряване на системи.

UML се състои от няколко вида диаграми, които могат да варират според версията на езика и осигуряват различни изгледи на системния модел. Първият вид са т. нар. *Структурни диаграми – Structural Diagrams*, представящи статичната структура на системата. Включват следните основни типове: „Клас-диаграма“ – “Class Diagram”, „Обектна диаграма“ – “Object Diagram”, „Пакетна диаграма“ – “Package Diagram”, „Диаграма на съставна структура“ – “Composite Structure Diagram”, „Компонентна диаграма“ – “Component Diagram”, „Диаграма на внедряване“ – “Deployment Diagram”, „Профилна диаграма“ – “Profile Diagram”.

Вторият вид диаграми са *Диаграмите за поведение – Behaviour Diagrams*, включващи: „Диаграми на употреба“ – “UseCase Diagrams”, „Диаграми на действията“ – “Activity Diagrams” и „Диаграма на състоянието“ – “State chart Diagram”. Последният тип, също подклас на *Диаграмите за поведение* са „Диаграмите за взаимодействие“ – “Interaction Diagrams”, които включват: „Диаграма на последователност“ – “Sequence Diagram”, „Комуникационна диаграма“ – “Communication Diagram”, „Времева диаграма“ – “Timing Diagram” и „Диаграма за преглед на взаимодействие“ – “Interaction Overview Diagram”.

Чрез диаграмите на UML лесно може да бъде трансформиран концептуалния модел на СИС в системен дизайн на СИС.

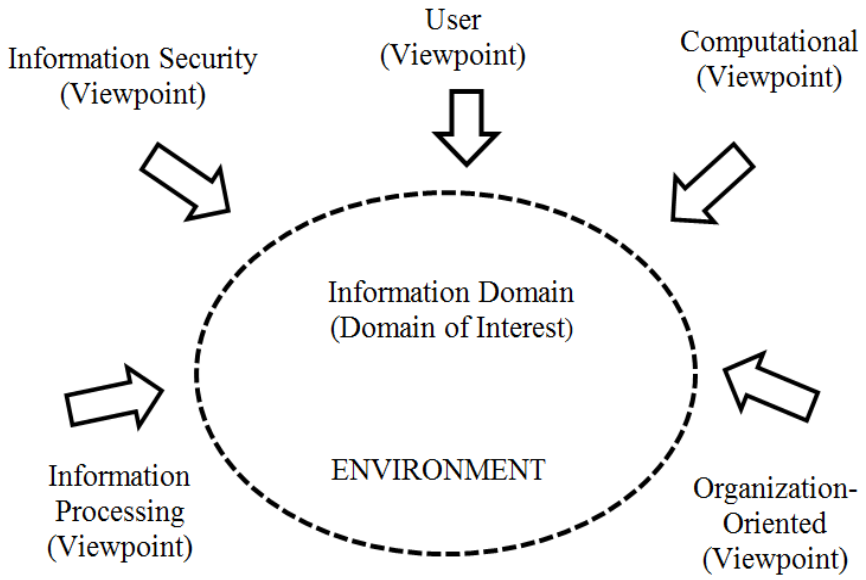
II. ОПИСАНИЕ НА АРХИТЕКТУРАТА НА СИС В ОРГАНИЗАЦИИ

Цялостният процес на развитие на СИС е свързан с трансформацията „модел-към-модел“. При това, един от най-удобните начини е да се използва обектно-ориентиран инструмент за описание, какъвто е езика UML. Архитектурният модел може лесно да бъде трансформиран от концептуален модел в UML модел, използвайки различните видове диаграми, предлагани в езика. За описание на системните концепции могат да се използват UML „Клас-диаграма“ – “Class Diagram”, за описание на динамичните аспекти на системата „Диаграма на действията“ – “Activity Diagram” и за внедряване на компонентите на СИС – „Диаграма на внедряване“ – “Deployment Diagram” [17].

Основната цел на СИС е да защитава и обезпечава информационните активи на организацията. Едни от основните изисквания към проектирането на СИС е да се гарантира постигането едновременно както на главната цел, така и на свойства като повторно използване на компонентите, оперативна съвместимост, мащабируемост и лесно внедряване [44].

Инженерно-ориентираното проектиране на системи или метода „отдолу-нагоре“ не е в състояние да гарантира постигане на всички цели. Тъй като подходът „отгоре-надолу“ за разработване на системи е много подходящ за тази цел, тук използваме този метод за моделиране на архитектурата на СИС. Необходимо е този подход да се нормализира чрез използване на насочващи модели, които да представят структурата на ИС в организации.

При създаване на рамка за архитектурно моделиране на системи за информационна сигурност (СИС, вж. Фиг.1) се използват основните понятия, свързани с концептуалния модел на описанието на архитектура на системи, определен в стандартите IEEE 1471 и IEEE 42010: „Система“, „Околна среда“, „Заинтересовани наблюдаващи“, „Линии на интерес“ – “Concerns”: „Области на интереси на различните заинтересовани наблюдаващи“, „Гледна точка“ – “Viewpoint”; „Модел на система“ – “View” [11], [12], [18].

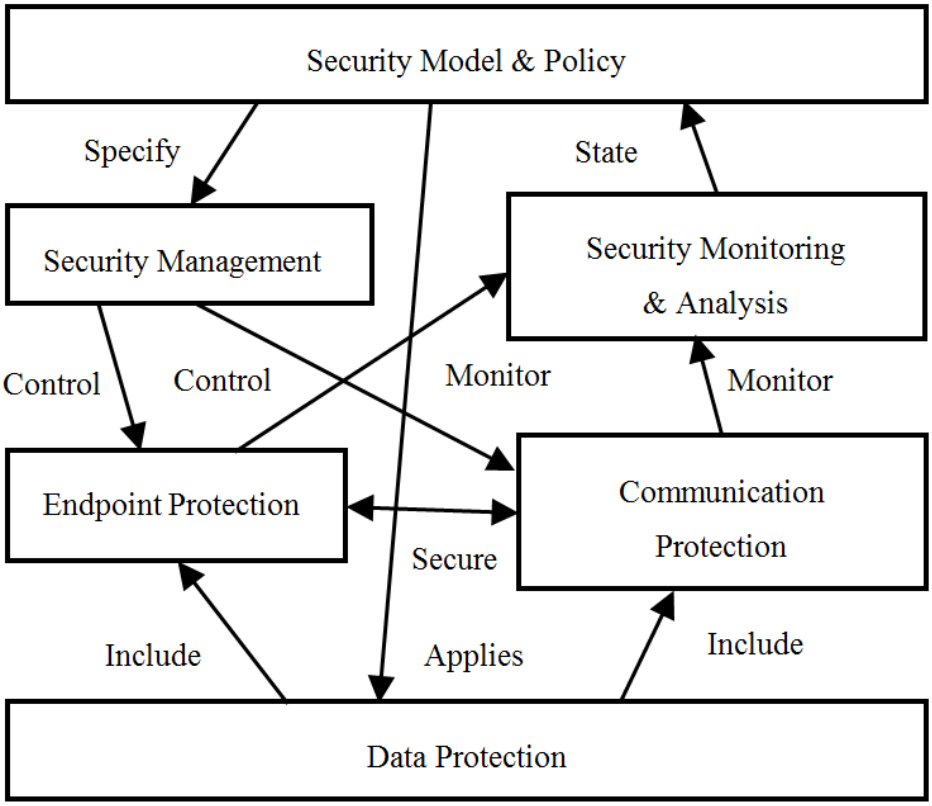


Фиг. 1. Архитектурна рамка за моделиране на СИС [19].

Мета-модел на СИС

Най-важните въпроси, на които трябва да отговори една система от гледна точка на информационната сигурност са: „Какво?“, „Как?“ и „Защо?“. От тази гледна точка предлагаме мета-модел на СИС (Фиг.2), състоящ се от шест концептуални блока: “Endpoint Protection”, “Communications Protection” („Какво?“), “Monitoring and Analysis”, “Management & Configuration” („Как?“), “Data Protection” и “Security Model & Policy” („Защо?“) [20].

Блокът “Endpoint Protection” („Защита на крайните точки“) е отговорен за защитните способности на устройствата. Основната функционалност, предоставена от този компонент, включва механизми за идентификация, кибер- и физическа сигурност. Блокът “Communication Protection” отговаря за защитата на комуникацията между крайните точки, чрез прилагане на различни методи като: удостоверяване и оторизиране на трафика, криптографски техники за цялостност и поверителност на данните и техники за контрол на информационния поток. След като крайните точки и комуникациите са осигурени, състоянието на системата трябва да бъде запазено през целия жизнен цикъл, чрез наблюдение, анализ и контрол на всички компоненти на системата, което се извършва от следващите два компонента – “Security Monitoring & Analysis” и “Security Management ”.



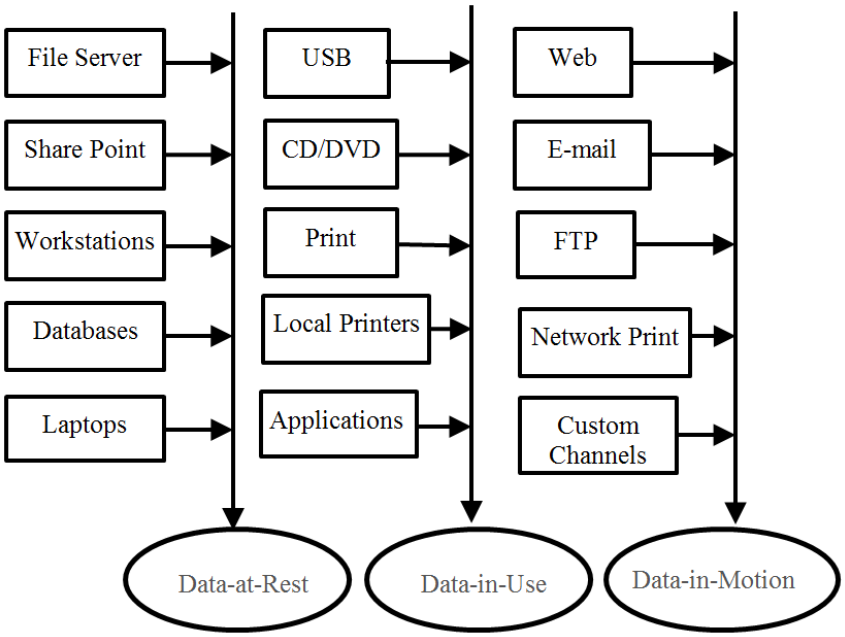
Фиг. 2. Мета-модел от гледна точка ИС [19].

Блокът “Security Model & Policy” определя как се прилагат политиките за сигурност, за да се гарантира „поверителността“ (“Confidentiality”), „целостта“ (“Integrity”) и „наличността“ (“Availability”) на системата. Той дирижира всички останали блокове за съвместна работа, разполагане и осигуряване на целите на системата. Блокът “Data Protection” директно и индиректно поддържа първите четири модула. Обхватът на блока се простира от „данните в покой” (“Data-at-Rest”) в крайните точки, през „данните в движение“ (“Data-in-Motion”), в комуникационните канали, до данните, събрани като част от функциите за мониторинг и анализ, както и всички данни за конфигурацията и управлението на системата [21], [22].

Във всеки един момент данните могат да бъдат в едно от трите състояния: „данни в покой“ (“Data-at-Rest”, на устройство за съхранение, твърд диск, мрежов дял), „данни в движение“ (“Data-in-Motion”, комуникации) или „данни в употреба“ (“Data-in-Use”, обработка в приложения) [23].

Предложеният от втори мета-модел (Фиг.3), се базира на гледната точка „Обработка на информация“ (“Information Processing”) в архитектурното описание на СИС, [19].

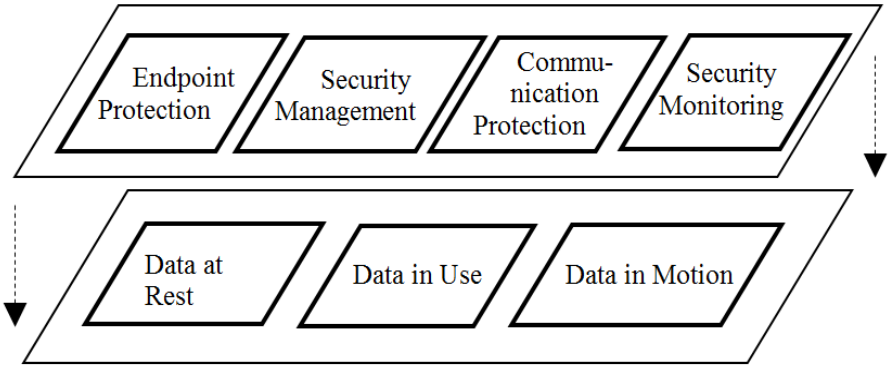
За да се защитят различните типове данни е необходимо да се внедрят специфични контроли за информационна сигурност (КИС) в основните блокове на мета-модела „Информационна сигурност“. Данните трябва да бъдат защитени срещу загуба, кражба, неоторизиран достъп и неконтролирани промени чрез прилагане на КИС, като например: контрол на „поверителността“ (Confidentiality), „целостта“ (Integrity), „контрол на достъпа“ (Access Control), изолиране и репликация [17], [18].



Фиг. 3. Мета-модел от гледна точка „Обработка на информация" [19].

На тази основа се предлага многослоен концептуален модел на СИС (Фиг. 4), който съдържа мета-модели, представляващи съответно гледни точки на "Информационна сигурност" и "Обработка на информация" и взаимовръзките между тях:

- Блок "Endpoint Protection" – защитава данните в покой (Data-at-Rest) и употреба (Data-in-Use) в крайните точки, чрез подходящи КИС като: контрол на достъпа, пароли, антивирусен софтуер, одитни пътеки, физически мерки за сигурност.
- Блок "Communications Protection" – предпазва данните в движение (Data-in-Motion), чрез криптографски техники, мрежова сегментация, периметрова защита, шлюзове, защитни стени, IDS, контрол на достъпа до мрежата, deep packet inspection и анализ на мрежовите журнали;
- Блок "Security Management" – защитава конфигурационните данни, данните, резултат от мониторинг и анализ, както и оперативните данни чрез криптографски методи.
- Блок "Security Monitoring & Analysis" – отговорен за защитата на данните за текущото състояние на системата, както и за мониторинга на ключовите системни параметри и показатели на системата. Типичните КИС, използвани в този блок са криптографски техники.



Фиг. 4. Многослоен концептуален модел на СИС [19].

В зависимост от изискванията на различните заинтересовани страни, към концептуалния модел могат да бъдат добавени повече мета-модели за различните гледни точки, с цел задоволяване на техните изисквания към СИС. След това, полученият многослоен концептуален модел се трансформира в реална физическа реализация на СИС.

UML „Дизайн-модел“

За трансформиране на получения многослоен концептуален модел на СИС използваме инструментариума на UML. За описание на системните концепции се използва UML „Клас-диаграма“ – “Class Diagram”, за описание на динамичните аспекти на системата – „Диаграма на действията“ – “Activity Diagram”, а за внедряване на компонентите на СИС – „Диаграма на внедряване“ – “Deployment Diagram” [24].

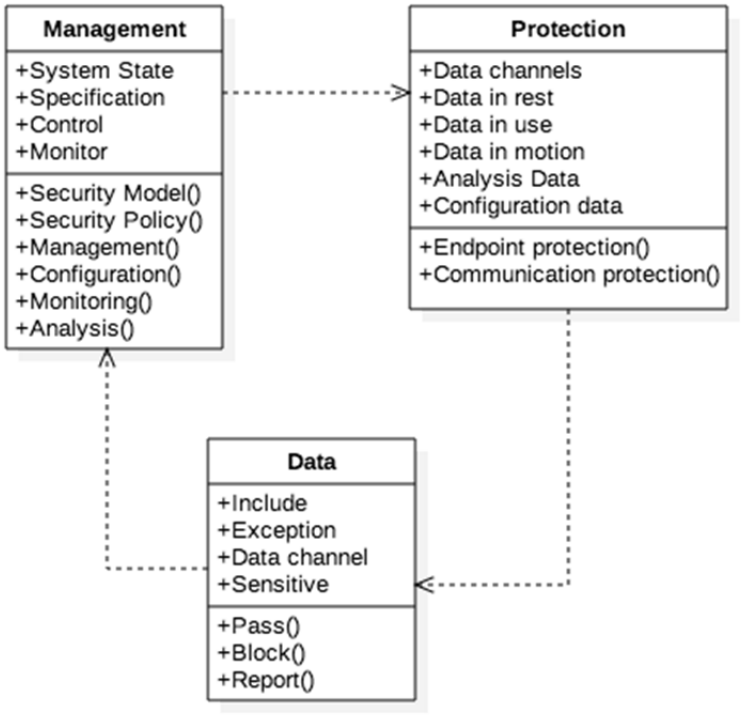
UML „Клас-диаграми“

Целта на „Клас-диаграмите“ – “Class Diagrams” е е да покажат статичната структура на класификаторите в системата. Диаграмата осигурява основна нотация, която може да се използва от други UML структурни диаграми. Клас-диаграмите се състоят от набор класове и връзки между класовете. Дефинираме три класа – *Management class*, *Protection class* и *Data class*:

- Класът *Management* притежава следните атрибути: “+System state”, “+Specification”, “+Control”, “+Monitor” и съответните методи: “+Security Model ()”, “+Security Policy ()”, “+Management ()”, “+Configuration ()”, “+Monitoring ()” и “+Analysis ()”.
- Класът *Protection* притежава следните атрибути: “+Data channels”, “+Data in rest”, “+Data in use”, “+Data in motion”, “+Analysis Data”, “+Configuration Data” и съответните методи: “+Endpoint Protection ()” и “+Communication Protection ()”.
- Класът *Data* притежава следните атрибути: “+Include”, “+Exception”, “+Data channel”, “+Sensitive” и съответните методи: “+Pass ()”, “+Block ()” и “+Report ()”.

Представянето на мета-модела на СИС чрез клас-диаграма е показано на Фиг. 5. Използваме същите понятия като в мета-модела от Фиг. 2, които са разделени като методи на трите основни класа. На блока “Security Model & Policy” отговарят методите “Security Model” и “Security Policy”, на блока “Management & Configuration” отговарят методите Management and Configuration, на блока Monitoring & Analysis отговарят методите Monitoring и Analysis в класа Management. На блоковете “Endpoint Protection” и “Communication protection” отговарят методите “Endpoint Protection” и “Communication” в *Protection* класа и накрая – блока “Data Protection” е представен с еквивалентните методи “Pass”, “Block” и “Report” в *Data* класа.

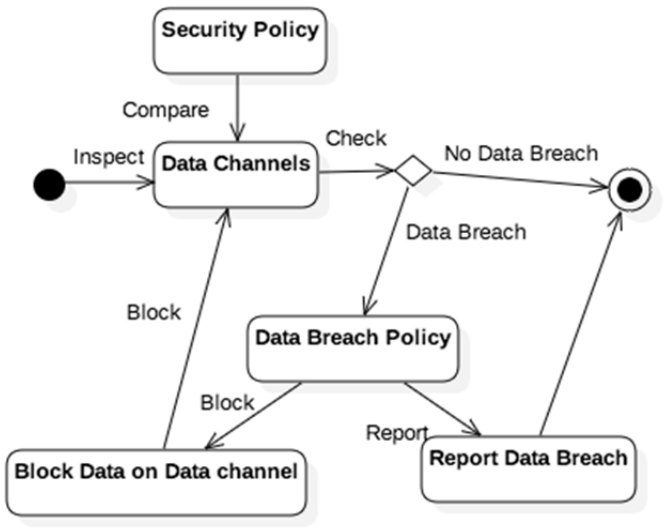
Всички тези методи изпълняват съответната функционалност като блоковете от мета-модела. “Security Model” и “Security Policy” дефинират и управляват останалите класове чрез атрибутите: “Specification”, “Control”, “Monitor” и “System state”. “Endpoint Protection”, “Communication Protection” и “Data Protection” методите осигуряват *класа Data* и *Protection*, и т.н.



Фиг. 5. UML „Диаграма на класовете“ [25].

UML „Диаграма на действията“

Диаграмата представя динамичното поведение на системата. На Фиг. 6 е представена „Диаграма на действията“ – “Activity Diagram” на един от методите на *Protection* класа – “Endpoint Protection”, които съответства на концепцията “Endpoint Protection” от мета-модела. Подобни диаграми на активността могат да бъдат създадени за всички методи от клас-диаграмата.



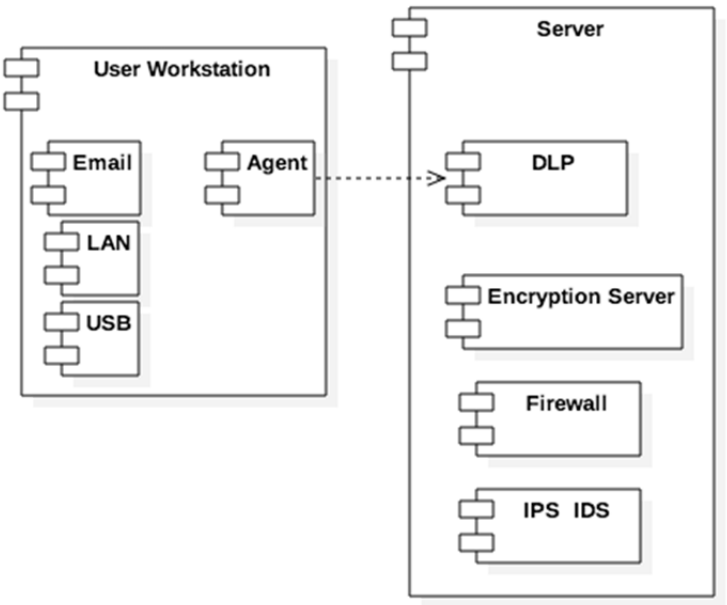
Фиг. 6. UML „Диаграма на действията“ [25].

Каналите за данни се проверяват за чувствителна информация чрез сравняване на данните с приетата политика за сигурност. Ако има съвпадение, се констатира изтичане на данни и нарушение, след което се инициират предвидените в политиката за сигурност действия. Те могат да бъдат документиране на нарушението и/или блокиране, така че изтичането на данни да бъде възпрепятствано.

UML „Диаграма на внедряване“

Чрез „Диаграмата внедряване“ – “Deployment Diagram” се моделира физическото внедряване на системните компоненти. За разлика от „Компонентните диаграми“, използвани за описание на отделните компоненти, „Диаграмите на внедряване“ показват как тези компоненти се разгръщат в реалната среда. Хардуерните компоненти (например DLP решения, защитни стени, уеб сървъри, пощенски сървъри, сървър за приложения) са представени като възли (nodes), софтуерните компоненти, които се изпълняват в хардуерните компоненти, са представени като артефакти. Трансформацията на мета-модела на СИС в UML „Диаграма на внедряване“ е показана на Фиг. 7. СИС е сложна система, съставена от голям брой компоненти, диаграмата е опростена и показва няколко хардуерни компоненти като DLP сървър, който е свързан със софтуерните агенти, работещи на работните станции на потребителите. Чрез агентите DLP сървъра наблюдава, контролира и управлява каналите за данни на крайните точки (работни станции и лаптопи) – LAN, Wi-Fi, Bluetooth, USB портове, електронна поща, чат комуникации и др. DLP системата е в състояние да контролира комуникационните канали, да активира и деактивира потока от данни през тях. Данните могат да бъдат инспектирани по съдържание, както е показано на Фиг. 7, като при констатиране на нарушение – неоторизирано изтичане на данни, то може да бъде блокирано и докладвано.

Чрез диаграмата на внедряване се илюстрира внедряването на всички необходими хардуерни и софтуерни компоненти като: Encryption System, Intrusion Detection Systems (IDS) и всички останали физически компоненти на СИС.



***Фиг. 7. UML „Диаграма на внедряване“* [25].**

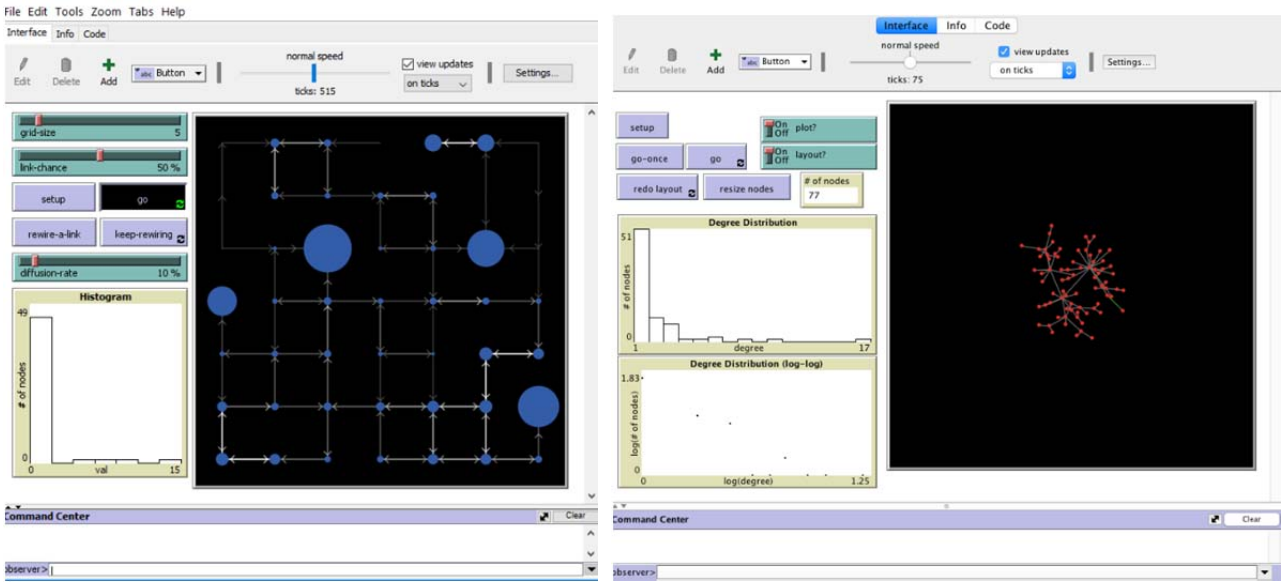
Представеният UML дизайн-модел, имплементиран чрез предложените три типа UML диаграми („Клас-диаграма“, „Диаграма на действията“ и „Диаграма на внедряване“) дава добра основа за обекно-ориентирано статично и динамично мултиаспектно трансформиране на многослойния концептуален модел СИС. По-детайлно изслеване на този дизайн-модел е направено в следващата точка, където е извършена и смесена симулационна оценка на предложените до тук идеи.

III. СИМУЛАЦИЯ НА АРХИТЕКТУРЕН МОДЕЛ НА СИС

Реализацията на тази задача бе извършено на базата на агентно- и мулти-агентно ориентирано моделиране в средите NetLogo и I-SCIP-SA, позволяващи смесена (експертна, сензорна и машинна) оценка на предложените архитектурни мета идеи.

Експерименти в средата NetLogo

NetLogo [26], [27] е мулти-агентна крос-платформена симулационна среда за симулиране на сложни системи във времето. Тя е предназначена за образователни цели и научни изследвания и се използва в широк кръг от дисциплини. Средата NetLogo е основана на агентно-базирани модели за симулиране на действията и взаимодействията на множество автономни агенти (индивидуални или колективни субекти като организации или групи), работещи едновременно. Това дава възможност да се изследват връзките между модели на микро ниво, които възникват от при тяхното взаимодействие и оценка на въздействието им върху системата, като цяло. На базата на мета-модела от Фиг. 2 е създаден агентно-ориентиран модел в средата NetLogo (v.6.0.4). Резултатите от симулациите на този модел са показани на Фиг. 8. Като цяло са изследвани взаимодействията между отделните блокове, а именно: “Protection Agent”, “Comms Agent”, “Breaching Agent”, “Policy Agent”, “Reporting Agent”, “Storing Agent”, “Monitoring Agent”, “Services Agent” и “Processing Agent”. Чрез използване на елементи от Теория на игрите, като и клас от методите Монте Карло за работа със случайни извадки, имплементирани в средата NetLogo, е осъществено представянето на агентите и са реализирани интеракциите между тях.



Фиг. 8. Екранни снимки от симулация в среда на NetLogo.

Като се отчита факта, че за момента средата NetLogo, по същество, е затворена и не е предвидено динамичното използване на външни източници на данни (сензорни, експертни и др.), получените модели имат основно изследователско значение за проучване на организационната страна на архитектурите на СИС по отношение на агентно-базираното и представяне.

Експерименти в средата I-SCIP-SA

С цел по-голяма близост до реалността, позволяваща смесено изследване на предложените архитектурни решения на СИС бе разработен мулти-агентен модел [28] от тип „система-от-системи“ [29] в средата I-SCIP-SA [30]. При това бе приложен опита от [31] и организацията от модела, предложен в [25] и реализиран в [32], аналогични на изследванията в средата NetLogo. Целта бе да се създаде възможност за идентифицирането на бъдещи заплахи – вътрешни и външни в ИС, използвани в корпоративна среда, в съответствие с различните състояния на използваните данни (вж. Фиг. 4) с активното участие и на човешкия фактор. Машинно, резултатите са представени посредством организацията „обект-връзка“ [33] и предоставят възможност за извършването на релевантни начални и крайни холистични, класификационни оценки на агентите в изследваните модели.

Обектите, представящи агенти (графично означени като именувани, заоблени правоъгълници) имат функционалности както за междуагентна комуникация, така и за визуализация на външни (записани или получавани в реално време) данни.

Междуагентните комуникационни канали са отбелязани с двупосочни стрелки, етикирани със стойностите на теглата (оцветени в жълто) и времевите стъпки (оцветени в синьо), отнесени към правите (*Influence*) и обратните (*Dependence*) връзки между обектите в модела.

Данните за теглата на междуагентните връзки, образуващи трендове могат да произхождат от различни симулационни резултати в смесената реалност, които са получени като резултат от решаването на математически модели и външни източници, както в реално време, така и след провеждане на симулациите [31], [34], [35], [36].

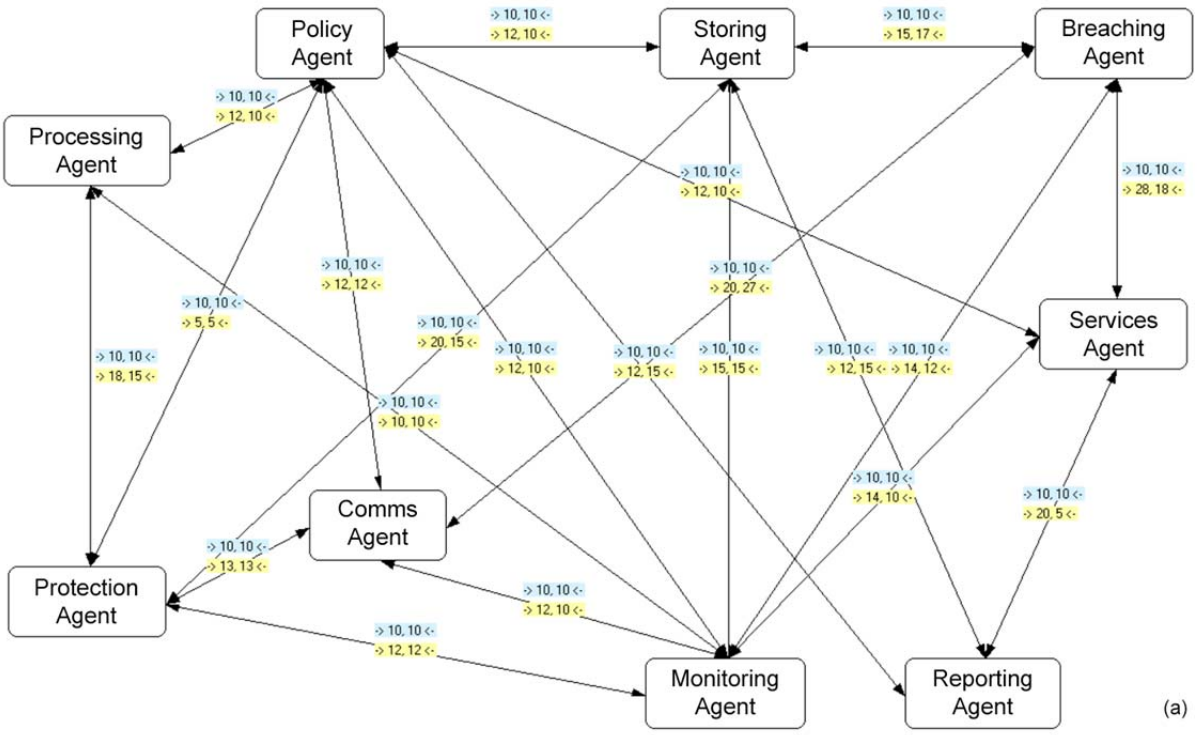
Множеството на източниците на данни може да използва: сензори, API функции за директна връзка или използващи записи във файлове с различен произход (вкл. експертен или друг симулационен резултат), които осигуряват възможност за проактивен системен анализ и холистична оценка на обектите в модела (в реално време или след симулацията), в съответствие с различните състояния на данните („данни в движение“, „данни в употреба“, „данни в покой“).

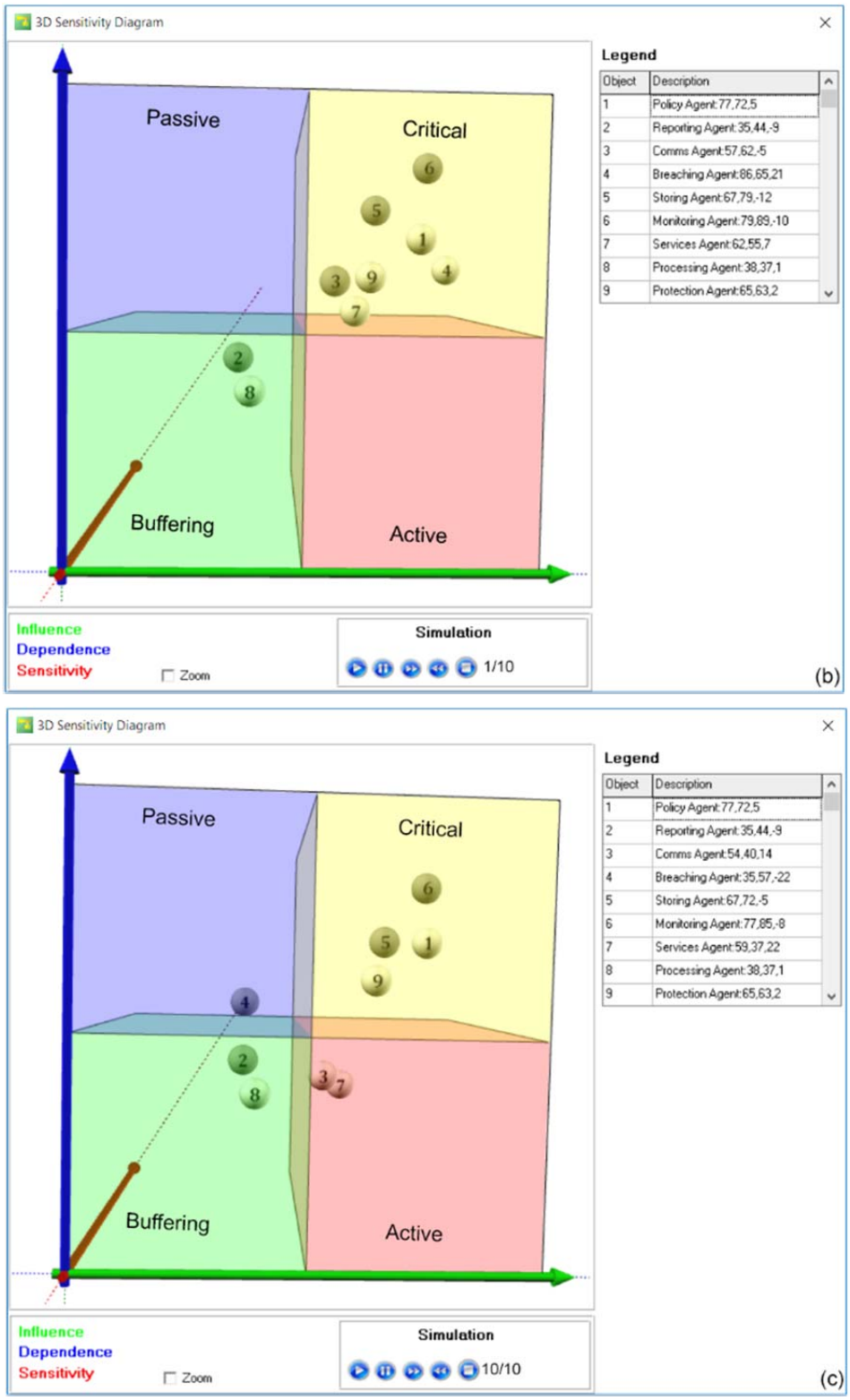
Резултатите от системния анализ са интерпретирани и агрегирани по различни начини (вж. например [34], [35], [36]), като тук се използва “3D Диаграма на чувствителността” – “3D ДЧ”, осигуряваща класификация на агентите (означени като индексирани 3D сфери) в четири сектора (*Активни – Active*, *Пасивни – Passive*, *Критични – Critical* и *Буферни – Buffering* обекти, имащи съответно – „пасивна“ – $z < 0$ или „активна“ роля – $z \geq 0$ по отношение на сектора в който са разположени), в съответствие с обработката и смесването на първоначалните експертни допускания и резултантните симулационни резултати (за *Влияние – Influence – x, Зависимост – Dependence – y* и *Чувствителност – Sensitivity – z*, измерени в проценти от интервала [0, 1]).

Предложеното решение предоставя възможност за проактивно участие на човешкия фактор в процеса на вземане на решения, гарантирайки цялостно разглеждане

и оценка на ролите на DLP агентите и проблемните места, възникващи при това. Мулти-агентната комуникация, в системния модел използва различни организационни стратегии от типа: „лидерство“ – “prominence”, както и „преговори“ – “negotiation” [28], в зависимост от избраните симулационни сценарии.

Представеният модел на DLP система за проактивно изследване на изтичанията на данни съдържа девет агента с различни роли: “Processing Agent” – „Обработващ агент“, “Policy Agent” – „Агент по политиките“, “Storing Agent” – „Складиращ агент“, “Breaching Agent” – „Агент по изтичанията“, “Services Agent” – „Агент по услугите“, “Protection Agent” – „Агент по защитата“, “Comms Agent” – „Агент по комуникациите“, “Monitoring Agent” – „Мониториращ агент“, “Reporting Agent” – „Докладващ агент“. Между тях са идентифицирани двадесет и една комуникационни връзки (вж. Фиг. 9а) описващи различни сценарии за изтичане на данни в корпоративна среда. Моделът е базиран на идеите от [25], както и някои емпирични данни от [37], [38], водещи до множество, начални критични агентни класификации (вж. Фиг. 9б), които са успешно решени в десет стъпки (вж. Фиг. 9с), отдавайки лидерска роля на „Агент по изтичанията“ – “Breaching Agent” [32].





Фиг. 9. Мулти-агентен модел на DLP система за проактивно изследване изтичания на данни в корпоративна среда (a) с допълнителни класификационни начални (b) и финални (c) оценки на агентите в 3D ДЧ [32].

Допусканията в модела, дават следната стартова класификация на агентите в 3D ДЧ: *Буферни – Buffering*, $z < 0$: „Докладващ агент“ – “Reporting Agent” – 2, $z \geq 0$: „Обработващ агент“ – “Processing Agent” – 8; *Критични – Critical*, $z \geq 0$: „Агент по политиките“ – “Policy Agent” – 1, „Агент по изтичанията“ – “Breaching Agent” – 4, „Агент по услугите“ – “Services

Agent" – 7, „Агент по защитата" – "Protection Agent" – 9, $z < 0$: „Агент по комуникациите" – "Comms Agent" – 3, „Складиращ агент" – "Storing Agent" – 5, „Мониториращ агент" – "Monitoring Agent" – 6.

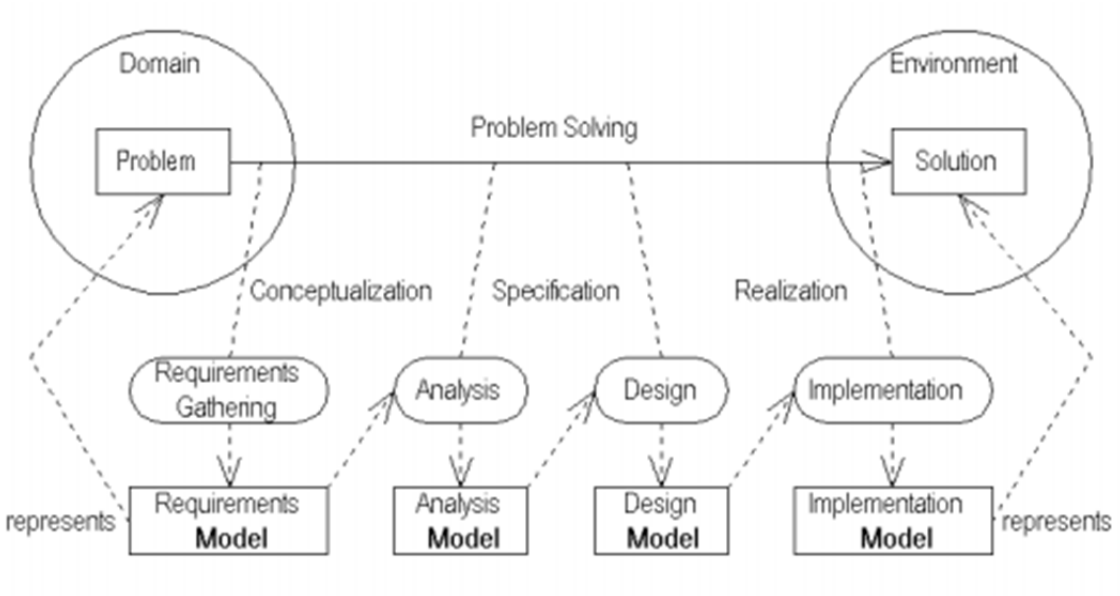
На базата на някои промени в ролята и теглата на „Агент по изтичанията" – "Breaching Agent", е предложена финална класификация на агентите в 3D ДЧ: *Буферни – Buffering*, $z < 0$: „Докладващ агент" – "Reporting Agent" – 2, $z \geq 0$: „Обработващ агент" – "Processing Agent" – 8; *Пасивни – Passive*, $z < 0$: „Агент по изтичанията" – "Breaching Agent" – 4*; Активни – Active,* $z \geq 0$: „Агент по комуникациите" – "Comms Agent" – 3, „Агент по услугите" – "Services Agent" – 7; Критични – Critical, $z \geq 0$: „Агент по политиките" – "Policy Agent" – 1, „Агент по защитата" – "Protection Agent" – 9; $z < 0$: „Складиращ агент" – "Storing Agent" – 5, „Мониториращ агент" – "Monitoring Agent" – 6.

Получените резултати от анализа на мулти-агентния модел на DLP система за проактивно изследване на изтичанията на данни в корпоративна среда показват ясна необходимост от балансиране, осигуряващо разширен контрол върху използваните комуникации и услуги. Това обаче крие и редица неясноти, тъй като въвеждането на нови технологични решения може да доведе до неочаквани изтичания на данни и пробиви в сигурността. Следователно, мониторинга, постанализа и складирането на данни в комбинация с евристичната защита в реално време остават критични за успешната защита на съвременната корпоративна среда, при отчитане особеностите на използваните потоци от данни.

В следващата част от изследването ще бъдат разгледани ключовите функционалности за изграждане на релевантен прототип на СИС, основан на комерсиално достъпни DLP решения, позволяващи динамична настройка на политиките за сигурност с цел ограничаване на изтичанията на данни.

IV. СЪЗДАВАНЕ НА ПРОТОТИП НА СИС

Изпълнението на тази задача бе осъществено на база изпълнение на жизнения цикъл за проектирането на СИС (вж. Фиг.10).



Фиг. 10. Жизнен цикъл на проектиране на СИС.

По дефиниция, СИС може да се разглежда като организирана колекция от компоненти или подсистеми, интегрирани за постигане на дадена цел, които трябва да бъдат гарантирани в технологичен и потребителски контекст.

Тя има различни входове, в нея се извършват определени бизнес процеси, и се произвеждат резултати, които заедно осигуряват постигането на целите на организацията при отчитане на нуждите й за гарантирана ad-hoc информационна сигурност [21], [25].

Както е видно от Фиг. 10, основните етапи от проектирането на СИС по жизнения цикъл, могат да бъдат агрегирани около следните процеси:

- Събиране на изисквания (Requirements Gathering) – в резултат се създава модел на изискванията;
- Анализ на изискванията (Analysis) – в резултат се получава анализ-модел, описващ платформено-независимо решение, отговарящо на модела на изискванията;
- Процеси на проектиране (Design) – като резултат се проектира дизайн-модел, отговарящ на анализ-модела, но проектиран чрез специфични платформи и продукти;
- Процеси на изграждане на системата (Implementation) – като резултат се реализира модел на физическа система, която удовлетворява дизайн модела. Тук ще отбележим, че изграждането на системата включва и процесите по тестване и внедряване, отбелязани по-нататък.
- Процеси на тестване (Testing) – проверяват дали дадена система отговаря на дефинираните за нея изисквания;
- Процеси на внедряване (Deployment), осигуряващи достъп на потребителите до системата [39].

От своя страна, всеки процес води до създаване на съответния модел, който отговаря на предходните изисквания и е основа за следващия модел [39], [40].

На базата на реален практически опит в сферата на осигуряването на сигурността в ИС от корпоративен тип [19], бе решено да се използва решение от тип DLP (Data Leak Prevention), чиито компоненти и принцип на действие са еквивалентни на мета-модела от Фиг. 3.

Решенията за предотвратяване изтичанията на данни от тип DLP са предназначени за предотвратяване на опити за нерегламентирано изнасяне, модифициране, унищожаване или получаване на неоторизиран достъп и използване на данните, без да се прекъсват нормалните бизнес процеси.

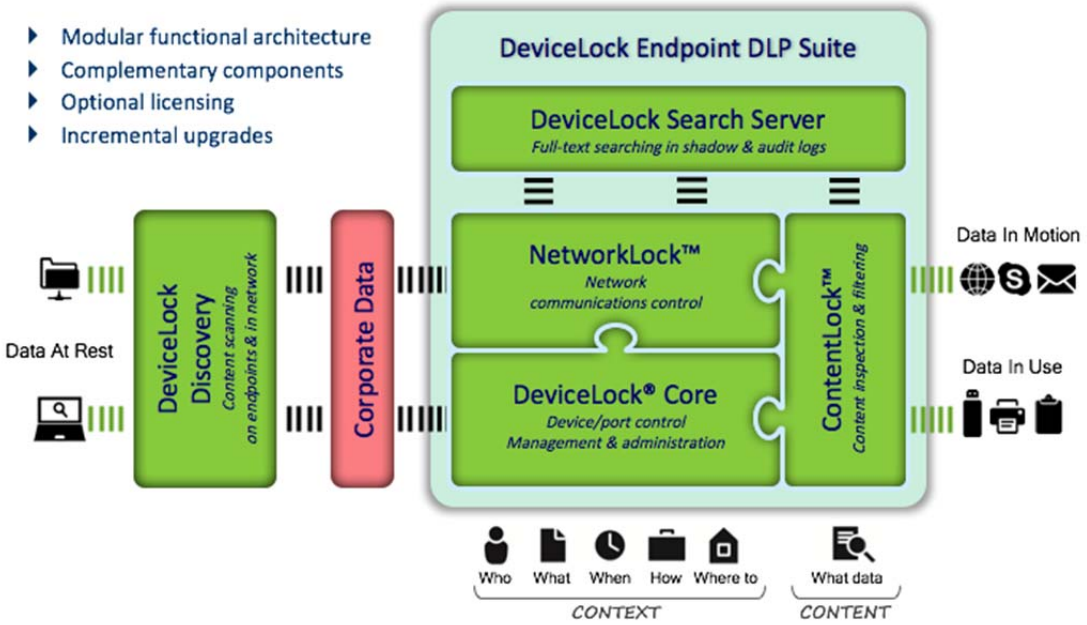
Основната задача на DLP системите е да запазят чувствителната информация вътре в системата или защитената мрежа на организацията, недопускайки неоторизираното й изтичане навън, независимо от причината за това.

Използваното в настоящото изследване конкретно решение е DeviceLock EndPoint DLP Suite, v.8.2 [13], чиято основна идея е показана на Фиг. 11.

Фиг. 11. DeviceLock EndPoint DLP Suite [13].

Решението е базирано на клиент-сървър архитектура. Върху контролираните крайни точки (работни станции, лаптопи и сървъри) се инсталират клиенти, наречени „агенти“, които комуникират с централния сървър и контролират комуникационните и информационните канали в съответствие с предварително дефинирана и централизирана политика за сигурност. DLP Suite, v.8.2 е в състояние да инспектира съдържанието на данните протичащи през комуникационните канали и по този начин да идентифицират чувствителна информация, зададена предварително с помощта на речници с ключови думи.

Веднъж идентифицирани, чувствителните данни могат да бъдат блокирани, а действията докладвани. Решението работи със всички видове данни от мета-модела на Фиг. 3: “Data-in-Use”, “Data-in-Motion” и “Data-at-Rest” (вж. Фиг. 12).



Фиг. 12. DeviceLock EndPoint DLP Suite – модули [*13*].

В последната точка са разгледани някои статистически решения за проверка на направените хипотези върху предложената мулти-агентна архитектура и при използване на избрания прототип на СИС. При това са генерирани и анализирани тестови данни, които са използвани за вероятностна валидация и интерактивна потребителска верификация в реални условия с фактически потребителски активности във смесена корпоративна среда.

V. ГЕНЕРИРАНЕ И АНАЛИЗ НА ТЕСТОВИ ДАННИ

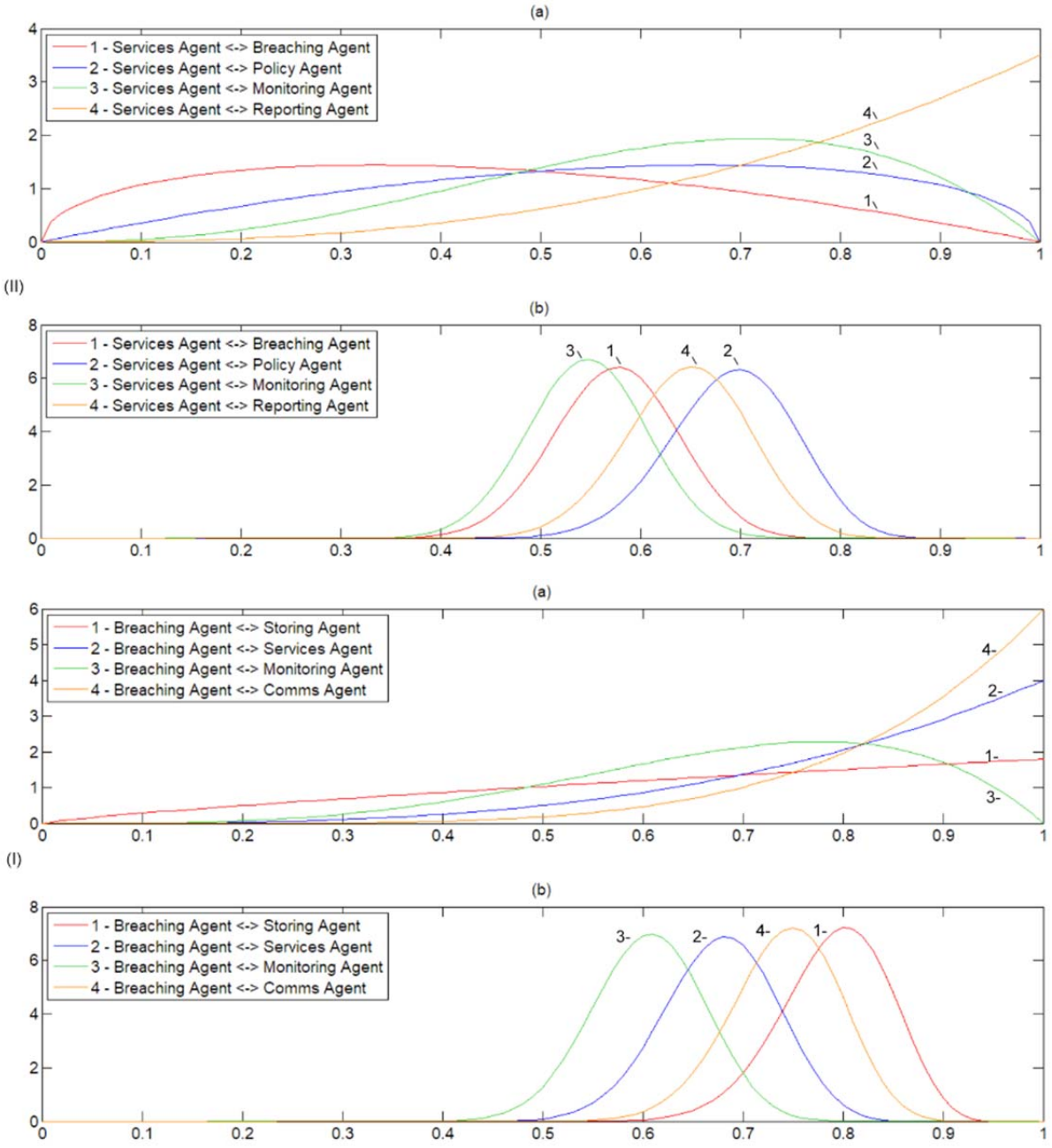
Изпълнението на тази задача бе организирано, върху избрана мулти-агентна архитектура на СИС, на две стъпки: (а) стохастична валидация на очакванията за изтичания на данни, посредством експертни допускания и машинно генерирани ad-hoc селекции за изтичания на данни; (б) интерактивна верификация във виртуална корпоративна среда с избрания прототип на СИС и вектори на кибер атаки, реализиращи очакванията за изтичане на корпоративни данни по определен сценарий за проиграване.

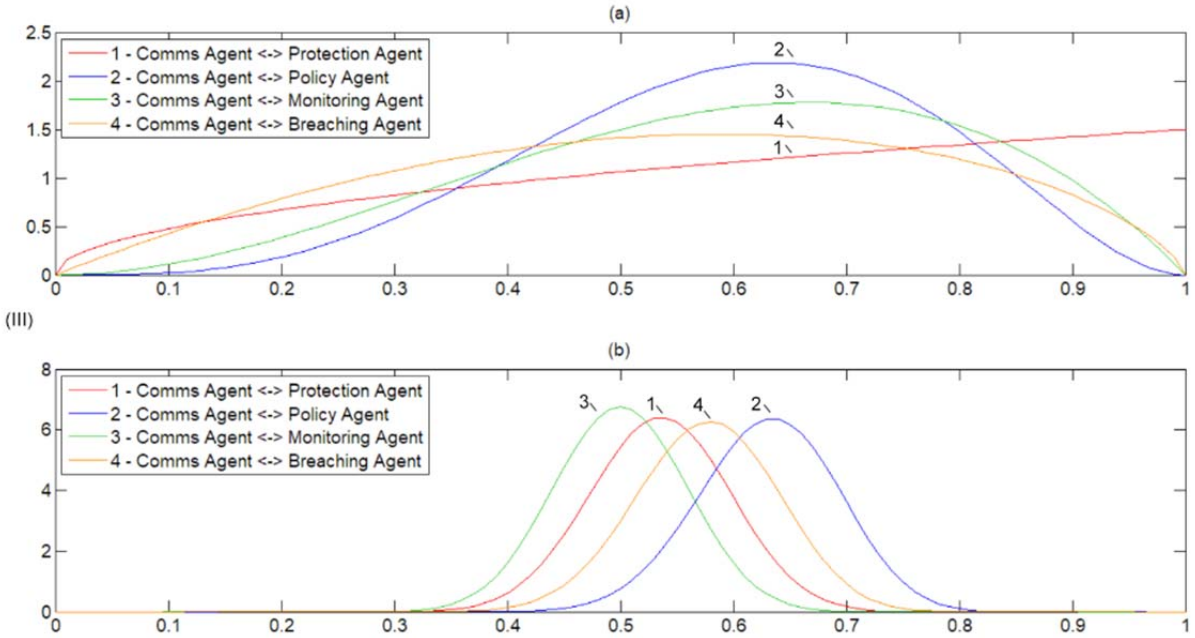
Стохастична валидация

Проактивно стохастично решение за смесена валидация върху предложения системен модел (вж. Фиг. 9) е представено в тази част. То е основано на идеите от [35], но използва различен контекст и процедура за пресмятане на вероятностните стойности. Предвид факта, че реалните корпоративни системи за информационна сигурност са нелинейни и нестационарни, тяхното поведение е труднопредсказуемо в определени ситуации. По същество, се дефинира бета вероятностно разпределение за всяка от използваните връзки между агентите в модела. Формата на разпределенията се определя експертно, в съответствие с техните очаквания за бъдещите тенденции. Идеята тук е взаимствана от добре познатите разглеждания на социалната динамика, предложени от Форестър [41], които в последствие са усъвършенствани в работата на Медоус и к-в [42]. В настоящото решение са използвани и някои модификации на параметрите „алфа“ и „бета“

на фамилиите от вероятностни криви, подобно на [35]. По-нататък, се извършва апостериорно машинно преоценяване за бъдещето на тенденциите във вероятностните разпределения, приложени върху връзките между агентите в модела. Новите стойности се изчисляват с използване на Бейсов подход по отношение на избрано сценарийно множество за еволюционно развитие. Основната идея е следната: Z (X, Y); Z_j (X_j, Y_j, T_i, S_k) = P ($X_j|D_l|L_m|A_n|T_i|S_k$) x P ($Y_j|D_l|L_m|A_n|T_i|S_k$), където: P (…) – Бейсова вероятност, X_j – влияние, Y_j – зависимост, Z_j – чувствителност на j-я агент в модела, D_l – l-то състояние на данните, l = {Use, Motion, Rest}, L_m – m-то от множеството на изтичанията на данни (вж. напр. [38]), A_n – индекса на потърсения n-и агент, T_i – продължителността на i-я времеви период за динамично изследване на модела, S_k – избрания k-и еволюционен сценарий от множеството на експерименталните сценарии (вж. напр. [25], [35]).

Графично представяне на предложената идея за априорните и апостериорни оценки на вероятностите върху бета разпределения (чрез смесена експертно-машинна валидация в среда на Matlab R2011b) за връзките на: “Breaching Agent” и свързаните с него: “Services Agent” и “Comms Agent” от модела на Фиг. 9а е показано на Фиг.13.





Фиг. 13: Вероятностна смесена валидация на очакванията за: "Breaching Agent" (Панел I), "Services Agent" (Панел II) и "Comms Agent" (Панел III), по отношение на априорните (a) и апостериорните (b) промени в трендовете за системния модел от Фиг. 9a [32].

Представените резултати от вероятностната валидация на системния мулти-агентен DLP модел за изследване на изтичанията на данни в корпоративна среда дават най-високи приоритети ($P < 0.9$) на: "Storing Agent", "Reporting Agent" и "Policy Agent", контрастиращи с по-ниско приоритетните, но значими ($P > 0.4$) агенти: "Monitoring Agent", "Services Agent" и "Protection Agent". Тези факти очертават доста релативистична картина на корпоративната информационна среда за сигурност, предвид факта че има известни припокривания, паралелности и непълноти по отношение използването на "Breaching Agent", "Comms Agent" и "Services Agent" едновременно като референтни и активно оценявани.

Представеното решение за смесена валидация позволява отчитането на различни времеви динамики в модела на основата на мулти-агентната сегментация на общата комплексност в изследваната система от системи. Реалните процеси протичащи паралелно в корпоративна среда и свързаните с тях участници са трансформирани цялостно в машинната среда чрез мулти-агентно представяне, което осигурява гъвкавост и удобство при работа. Все пак, някои трудности и неясноти по отношение на еволюционната динамика при комуникацията между агентите и тяхното ролево разделение остават субективни и не напълно определени, предвид прогнозния характер на валидацията и наличието на случайни събития непредвидени в модела, които могат да окажат съществено влияние в реалността. Ето защо, бе извършена и верификация на получените резултати във виртуална корпоративна среда с цел проверка на направените прогнози.

Интерактивна верификация

Верифицирането на резултатите от стохастичните симулации бе проведено емпирично, с използване на интерактивна симулация в трансформирана реалност, организирана в рамките на учението CYREX 2018 [34], [43]. Използван беше въображаем

сценарий, който се играе в продължение на 180 минути от обучаемите в няколко интернационални екипа с участие на над 30 представители от България, Македония и Турция с включени наблюдатели от ИКТ бизнеса, съсловни и експертни организации у нас и в чужбина. Като резултат бе направена експериментална многокритериална оценка на вероятностната динамика на избрани потоци от данни в перспектива, по отношение влиянието на цифровата трансформация в дигиталната ера в контекста на проиграванията сценариен скрипт.

Включени бяха четири атакуващи вектора (социален инженеринг, индустриален шпионаж, злонамерен софтуер и насочени атаки) и седем основни екипа, организирани по следния начин: start-up компания – *Digital Creativity*, разработваща иновативно решение за разплащане, базирано на цифрови копия от реални човешки качества и способности.

Иновативните решения са закупени от по-голяма корпорация – *Moon Digital Solutions*, която има планове за нахлуване в колонията на планетата New Life. Дейно участие взима хакерската група – *Stellar Ghost*, която модифицира технологията на *Digital Creativity*, променяйки поведението на роботите на New Life към агресивно и добавяйки им бойни умения. Други участници са: *Galactic World* – междугалактическа асоциация, отговорна за регулирането на цифровите технологии, която използва друга малка компания – *QHR Selection*, за да се намеси в ситуацията и да спре терористичните планове на хакерите. Последния участник е *Stellar Media* – PR компания, отразяваща медийно ситуацията.

Екипите на играещите имаха възможност да използват няколко вида устройства: фаблети, таблети, настолни и мобилни компютри, отворени облачни услуги за съхранение и споделяне на данни, криптиране, чатове, социални медии, мултимедийни съобщения, електронна поща и система за мониторинг на споделяната от участниците информация от клас DLP, достъпвани директно или с чрез криптирани QR кодове.

Експериментът бе организиран в затворена група на социалната мрежа Facebook, а така също и чрез използването на приложения като WhatsApp и Viber. Достъпът на участниците до използваните облачни услуги беше организиран чрез VPN.

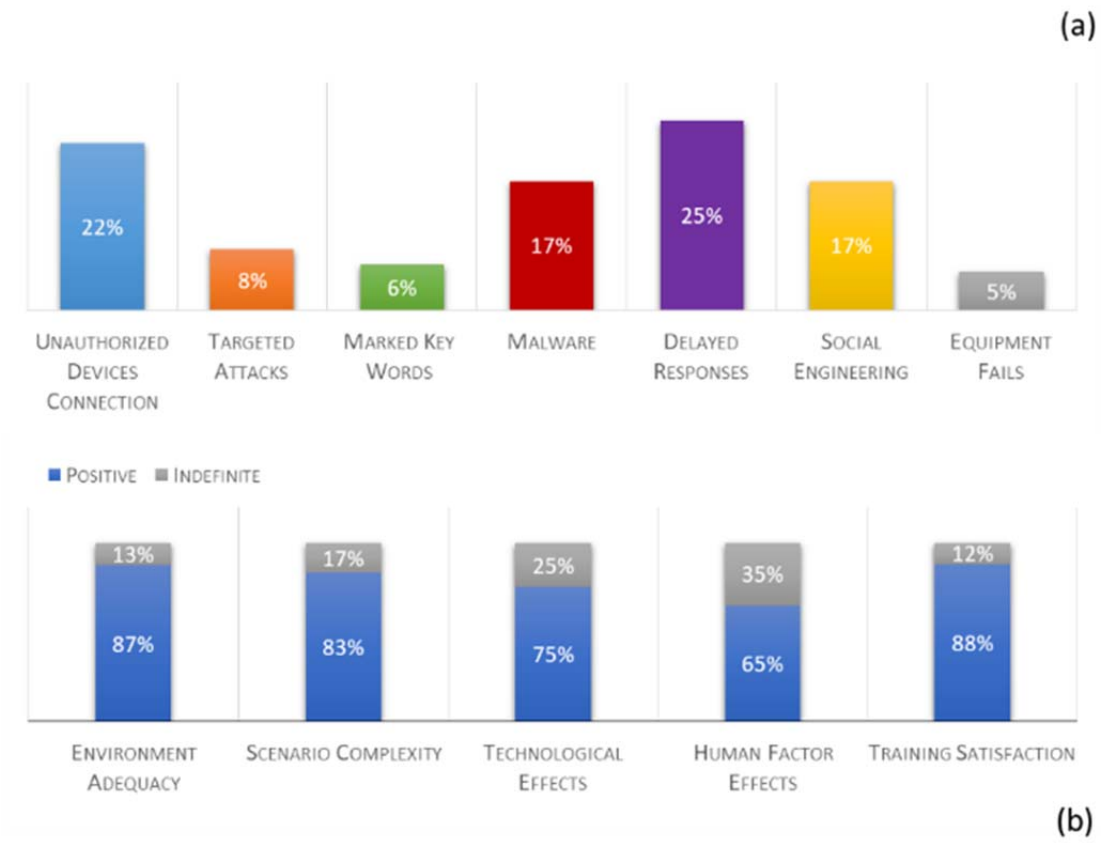
Поведението на играчите беше наблюдавано по отношение динамиката на техните действия по скрипта на сценария, като самата регистрация бе организирана дистанционно, използвайки система за мониторинг и видеозапис, както и COTS DLP CoSoSys My Endpoint Protector, v. 4.7.4.7 [14]. DLP решението е в състояние да контролира различните типове данни: „данни в движение“ (Data-in-Motion) и „данни в покой“ (Data-at-Rest). Въз основа на архитектурата „клиент-сървър“, средата предоставя на своите клиенти-агенти, инсталирани на крайните устройства на потребителите, и управлявани от отдалечен сървър, контрол върху всички комуникационни канали на крайните устройства, използвани в учението. DLP решението анализира съдържанието на данните, преминаващи през комуникационните канали, и ги сравнява с ключови думи, предварително дефинирани в специални речници, разпознавайки по този начин чувствителни данни, като осъществява и допълнителен контрол върху операциите с тях. Използваното DLP решение позволява и дефиниране на ad-hoc политики за информационна сигурност.

Трябва да се отбележи, че като цяло, реализирания подход за наблюдение на потребителите предостави възможност за по-задълбочен анализ на обучаемите относно техните когнитивни и поведенчески реакции.

Фиг. 14. Моменти и архитектура на CYREX 2018 [34].

Емпирична по характер, осъществената рамка на CYREX 2018 беше количествено оценена (вж. Фигура 15) от участниците (използвайки данни, както за положителните, така и за неопределените стойности на група индикатори, измерени в проценти). На базата на идеите, отбелязани в [25], бяха избрани пет ключови индикатора: “Environment Adequacy” – „Адекватност на средата“, “Scenario Complexity” – „Комплексност на сценария“, “Technological Effects” – „Технологични ефекти“, “Human Factor Effects” – „Ефекти от човешкия фактор“ и “Training Satisfaction” – „Удовлетвореност от обучението“. Освен това, бяха използвани и обобщените, нормализирани данни, регистрирани от DLP решението за изтичане на информация, чрез мониторинг на седем възможни атакуващи вектора: “Unauthorized Devices Connection” – „Неоторизирано свързване на устройства“, “Targeted Attacks” – „Насочени атаки“, “Marked Key Words” – „Маркирани ключови думи“, “Malware” – „Атаки чрез зловреден софтуер“, “Delayed Responses” – „Забавени отговори“, “Social Engineering” – „Социален инженеринг“ и “Equipment Fails” – „Отказ на оборудването“.

Резултатите от CYREX 2018 дават занижена оценка за индикатора “Human Factor Effects” – „Ефекти от човешкия фактор“ (<< 70%) поради скрития мониторинг на участниците, който не е предварително обявен. Подобна е ситуацията и с резултатите от изтичането на данни, използвайки вътрешни участници (insiders) за инсталиране на специфични ключови думи в комуникациите на екипите, заедно с провокирането на неочаквани атаки от типа “Equipment Fails” – „Отказ на оборудването“ и DDoS насочени атаки с успеваемост << 10%, осигурявайки >> 20% видими закъснения спрямо сценария и атаки от типа “Unauthorized Devices Connection” – „Неоторизирано свързване на устройства“ (USB памети и други периферни устройства за съхраняване на данни). По-очевидните атаки от от типа “Malware” – „Атаки чрез зловреден софтуер“ и “Social Engineering” – „Социален инженеринг“, дават над 15% видимост в CYREX 2018, гарантирайки успешно покритие за нерегистрираните случаи на изтичания на данни.



***Фиг. 15. Резултати от DLP мониторинга за векторите на атака (а) и обобщена оценка от участниците (б) за CYREX 2018* [25].**

VI. ДИСКУСИЯ

В съвременното корпоративно общество на дигиталната ера, нуждите от адекватни мерки за защита на данните и противодействие на техните нерегламентирани изтичания стават все по-големи.

Представеното холистично решение може да се разглежда като адрес не само към корпоративната, а изобщо към организационната работна среда. При това е важно да бъдат спазвани приетите стандарти и регулации, като се проектират архитектури на системите за информационна сигурност с възможност за посрещане на нови, непланирани предизвикателства, като се прибави и емпиричен опит, натрупан от практиката.

Приложеното решение за концептуално UML мета-проектиране на архитектури с използване на различни класове диаграми, позволява статично и динамично разглеждане на функционалностите на системите за информационна сигурност. По-детайлни изследвания на очакванията за изтичания на данни са извършени симулационно, на основата на смесени агентно- и мултиагентно- ориентирани решения, осигуряващи голяма гъвкавост и близост до реалността.

Предложените практическа валидация и верификация на избрана комерсиално достъпна DLP система с гъвкави функционалности, адаптирани към мета архитектурите, дават възможност за реално съчетаване на експертни, сензорни и машинно симулирани данни. При това остава възможно и тяхното сравнение с проектираните архитектурни функционалности, по отношение на реалните вектори за атака в смесена, футуристична виртуална среда за избрани сценарийни комбинации.

Това позволява не само да бъдат ограничени изтичанията на данни в бъдеще, но и да се подобрят вътрешните политики за сигурност, обработката на чувствителна информация, законовите, подзаконовите разпоредби и директивите за лична неприкосновеност в работната среда на съвременното дигитално общество.

Никоя организация не може да бъде достатъчно сигурна, за да посрещне неочакваните изтичания на данни и уязвимости на своите информационни системи, без постоянно наблюдение и адекватен, проактивен, холистичен анализ на риска. Успешното постигане на проактивна, цялостна корпоративна сигурност в бъдещето е сложна задача, която изисква хибридно съчетаване както на човешките, така и технологичните усилия с цел гарантиране на устойчив напредък към ново ниво на сигурност в дигиталната ера, където технологиите ще стават все по-интелигентни.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] J. Hintzbergen, K. Hintzbergen, A. Smulders, and H. Baars, “Foundations of Information Security Based on ISO27001 and ISO27002,” 3rd Edition, Van Haren Publishing, 2015.

[2] “ISO 27001 Official Page,” Available: https://www.iso.org/isoiec-27001-information-security.html [Accessed: 12-March-2019].

[3] “COBIT Security Baseline: An Information Survival Kit,” 2nd Edition, IT Governance Institute, 2007.

[4] “COBIT resources,” Available: http://www.isaca.org/COBIT/Pages/default.aspx [Accessed: 12-March-2019].

[5] “NIST Special Publications (800 Series),” Available: https://csrc.nist.gov/publications/sp800 [Accessed: 12-March-2019].

[6] “Gramm-Leach-Bliley Act (GLBA) Resources,” Available: www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act [Accessed: 12-March-2019].

[7] S. Anand, “Sarbanes-Oxley Guide for Finance and Information Technology Professionals,” 2nd, Wiley, Edition, 2006

[8] “Sarbanes-Oxley Act,” Available: https://www.sec.gov/about/laws/soa2002.pdf [Accessed: 12-March-2019].

[9] R. Herold and K. Beaver, “The Practical Guide to HIPAA Privacy and Security Compliance,” 2nd Edition, CRC Press, 2014

[10] “PCI Security Standards,” Available: https://www.pcisecuritystandards.org/pci_security/ [Accessed: 12-March-2019].

[11] “IEEE Std 1471,” IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, 2000

[12] “ISO/IEC/IEEE 42010:2011 – Systems and Software Engineering – Architecture Description,” Available: https://www.iso.org/standard/50508.html [Accessed: 12-March-2019].

[13] “DeviceLock Web Page,” Available: www.devicelock.com/products/ [Accessed: 12-March-2019].

[14] “CoSoSys Endpoint Protector Web Page,” Available: https://www.endpointprotector.com/ [Accessed: 12-March-2019].

[15] “EU General Data Protection Regulation,” Official Web Page, Available: http://ec.europa.eu/justice/data-protection/reform/index_en.htm [Accessed: 12-March-2019].

[16] “The Unified Modeling Language (UML) Web Page,” Available: https://www.uml-diagrams.org/ [Accessed: 12-March-2019].

[17] A. Dennis, B. Wixom, and D. Tegarden, “System Analysis & Design – An Object-Oriented Approach with UML,” 5th Edition, John Wiley & Sons, 2015, pp. 19-52.

[18] R. Hilliard, “Aspects, Concerns, Subjects, Views,” First Workshop on Multi- Dimensional Separation of Concerns in Object-Oriented Systems (OOPSLA’99), pp. 1-4, 1999.

[19] I. Gaydarski and Z. Minchev, “Conceptual Modeling of an Information Security System and Its Validation through DLP Systems,” In Proc. of BISEC 2017, Belgrade, Serbia, October 18, 2017, pp. 36-40.

[20] R. Hilliard, “Lessons from the Unity of Architecting,” in I. Jacobson and H. Lawson (Eds) “Systems Context,” 7 Systems, 2016, pp. 225-250.

[21] J. Killmeyer, “Information Security Architecture: An Integrated Approach to Security in the Organization,” CRC Press,Taylor & Francis Group, LLC, 2006, pp. 203-240.

[22] “Industrial Internet of Things Volume G4: Security Framework,” Available:

http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf, May 2017, pp. 46-61. [Accessed: 12-arch-2019].

[23] M. Rhodes-Ousley, “Information Security the Complete Reference,” 2nd Edition, The McGraw-Hill, 2013, pp. 303, 234-238.

[24] A. Dennis, B. Wixom, and D. Tegarden. “System Analysis & Design – An object-oriented approach with UML,” 5th Edition, John Wiley & Sons, 2015, pp. 19-52.

[25] I. Gaydarski, Z. Minchev, and R. Andreev, “Model Driven Architectural Design of Information Security System,” 14th International Conference on Information Assurance and Security (IAS 2018), Porto, Portugal, December 13-15, 2018 (in press for Advances in Intelligence Systems and Computing, Springer, 2019)

[26] S. Tisue and U. Wilensky, “NetLogo: A simple environment for modeling complexity,” Presented at the International Conference on Complex Systems 2014, Boston, May 16 – 21, 2014.

[27] “NetLogo - Center for Connected Learning and Computer Based Modeling,” Northwestern University, Evanston, Illinois, USA, Available: http://ccl.northwestern.edu/netlogo/ [Accessed: 12-March-2019].

[28] K. Sycara, “Multiagent Systems,” AI Magazine, 19, No. 2, 1998, pp. 79-92.

[29] F. Vester, “The Art of Interconnected Thinking – Ideas and Tools for Dealing with Complexity,” München, MCB – Verlag, 2007.

[30] Z. Minchev, “Methodological Approach for Modelling, Simulation & Assessment of Complex Discrete Systems,” In Proc. of National Informatics Conference Dedicated to 80-th Anniversary of Prof. Petar Barnev, Sofia, Bulgaria, Institute of Mathematics & Informatics, Bulgarian Academy of Sciences, 2016, pp. 102-110.

[31] L. Boyanov and Z. Minchev, “Cyber Security Challenges in Smart Homes,” In Proceedings of NATO ARW “Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework,” Ohrid, Macedonia, June 10-12, Published by IOS Press,

NATO Science for Peace and Security Series - D: Information and Communication Security, Vol.38, 2013, pp. 99 – 114.

[32] I. Gaydarski and Z. Minchev. “Challenges to Data Protection in Corporate Environment,” In Z. Minchev (Ed) “Future Digital Society Resilience in the Informational Age,” Chapter 8, Sofia, Institute of ICT, Bulgarian Academy of Sciences, SoftTrade, December, 2018 (in press).

[33] P. Chen, “The Entity-Relationship Model-Toward a Unified View of Data,” ACM Transactions on Database Systems 1, 1976, pp. 9-36.

[34] Z. Minchev, “Data Relativities in the Transcending Digital Future,” In Proc. of BISEC 2018, Belgrade, Serbia, October 20, 2018 (in press)

[35] Z. Minchev, G. Dukov, et al. “Cyber Intelligence Decision Support in the Era of Big Data,” In ESGI 113 Problems & Final Reports Book, Chapter 6, Fastumprint, 2015, pp. 85-92.

[36] Z. Minchev, “Security Challenges to Digital Ecosystems Dynamic Transformation,” In Proc. of BISEC 2017, Belgrade, Serbia, October 18, 2017, pp. 6-10.

[37] I. Gaydarski and Z. Minchev, “Virtual Enterprise Data Protection: Framework Implementation with Practical Validation,” In Proc. of BISEC 2018, Belgrade, Serbia, October 20, 2018 (in press)

[38] “Data Breach Investigations Report,” 11th Edition, Verizon, 2018, [Online] Available: https://goo.gl/NtpXQ1 [Accessed: 12-March-2019].

[39] S. Alhir, “Understanding the Model Driven Architecture (MDA),” Methods & Tools 11, no. 3, 2003, pp. 17-24.

[40] R. Breu, R. Grosu, F. Huber, B. Rumpe, and W. Schwerin, “Systems, Views and Models of UML,” In M. Schader, A. Korthaus (Eds.) “The Unified Modeling Language, Technical Aspects and Applications,” Physica Verlag, Heidelberg, 1998, pp. 3-8.

[41] J. Forrester, “World Dynamics,” Cambridge, Massachusetts, Wright-Allen Press, 1971.

[42] D. Meadows, J. Randers, and D. Meadows, “Limits to Growth: The 30-Year Update,” Chelsea Green Publishing Company, 2004.

[43] CYREX 2018 Web Page, Available: http://securedfuture21.org/cyrex_2018/cyrex_2018.html [Accessed: 12-March-2019].

[44] I. Gaydarski, P. Kutinchev, and Z. Minchev, “Modelling & Deployment of Data Protection Component of Information Security Systems,” In Proc. of First International Interdisciplinary Conference on Information and Cyber Security-Global, ICICSG’2017, Istanbul, October 20, 2017. (in press)