БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

ИВАН КОСТАДИНОВ ГАЙДАРСКИ

МЕТОД И МОДЕЛИ ЗА РАЗРАБОТКА НА СИСТЕМИ ЗА ИНФОРМАЦИОННА СИГУРНОСТ В ОРГАНИЗАЦИИ

АВТОРЕФЕРАТ

на дисертация

за придобиване на образователната и научна степен „доктор“

по докторска програма „Компютърни системи, комплекси и мрежи“

професионално направление 5.3. Комуникационна и компютърна техника

Научен ръководител:
доц. д-р Румен Андреев

София, 2022 г.

Дисертацията е обсъдена и допусната до защита на разширено заседание на секция "Комуникационни системи и услуги" на ИИКТ-БАН, състояло се на 27.01 2022г.

Дисертацията се състои от увод, четири глави и заключение, декларация за оригиналност на резултатите, библиография и приложения.

Дисертационният труд е в обем от 142 страници, 48 фигури, 13 таблици, 139 цитирани литературни източника и 2 приложения.

Защитата на дисертацията ще се състои на ……г. от …… часа в зала …… на блок …… на ИИКТ-БАН на открито заседание на научно жури в състав:

1. ……
2. .....
3. .....
4. .....
5. .....

Резервни членове:
1. .....
2. .....

Материалите по защитата са на разположение на интересуващите се в стая 215 на ИИКТ-БАН, ул. "Акад. Г. Бончев", бл. 25А.

Автор: **Иван Гайдарски**
Заглавие: **Метод и модели за разработка на системи за информационна сигурност в организации**

Ключови думи: агентно, анализ, аспектно, архитектура, вектор, заплахи, защита, информация, инсайдъри, концептуално, метод, модел, моделиране, обектно-ориентирано, област, описание, околна, организация, проектен, разработка, реализация, системи, сигурност, симулация, среда, трансформация, уязвимости, UML

Обща характеристика на дисертационния труд

Актуалност на темата

Информацията е един от най-ценните активи на съвременните организации. Интелектуалната собственост, ноу-хау, патенти, списъци с клиенти и доставчици – тази информация е жизненоважна за всяка организация и формират нейното конкурентно предимство. Едно от най-важните предизвикателства пред тях е защитата на информацията във всички и форми – електронна и физическа. Информацията трябва да бъде надеждно защитена както от външни атаки – хакери или природни бедствия, така и от вътрешни – настоящи и бивши служители, партньори и доставчици. Тяхното право на достъп до ресурсите на организацията като системи, мрежи и данни изисква защитата от нерегламентираното изтичане на информация да се съобразява със стратегия, различна от тази при традиционната защита срещу външни за организацията заплахи [1, 2].

Главните заплахи в наши дни са свързани с данните и информационните активи. Колкото са по-ценни активите, на толкова повече атаки са изложени. Новите и съществуващите уязвимости водят до по-висока успеваемост на атаките. Поради това заплахите силно зависят от уязвимостите, които могат да бъдат експлоатирани от атакуващата страна. Всяка промяна в един от факторите води до увеличаване на обхвата му. Например, увеличаването на възможностите на агентите на заплахата респективно водят до по-успешна идентификация и експлоатация на уязвимосттите, и съответно до по-голяма успеваемост на атаките [25]. Въвеждането на нови информационни активи води до увеличаване на атакуемата повърхност, съответно до нови слабости/уязвимости, нови методи за атака и нови заплахи. Въвеждането на последните технологични новости води до слабости, които са свързани с технологичната незрялост, неправилна употреба, неправилна интеграция със съществуващите системи, ниска информираност на потребителите и др. Това създава почва за нови заплахи, насочени към тези активи [25]. За да бъдат редуцирани успешните атаки към информационните активи е необходимо да бъде извършен анализ на всички елементи във веригата уязвимости-заплахи - атаки.

В организациите се създават, приемат и одобряват единна политика за сигурност, процедури и процеси за информационна сигурност. Те са резултат от влиянието на различни фактори – територията, на която организацията развива дейност, регулаторни режими, специфични за дадения сектор изисквания, стандарти и добри практики. Един от основните фактори, с който трябва да се съобрази организацията е националното законодателство, действащо на територията на държавата, в която тя е регистрирана или оперира – данъчно законодателство, наказателен кодекс, разрешителни режими и други. В аспекта на Системите за Информационна Сигурност (СИС), в областта на нашия интерес са нормативните актове, формиращи основата на държавната политика в областта на кибер сигурността - сигурност в кибер пространството, дейности по кибер отбрана и по противодействие на кибер престъпността [57].

Особено внимание трябва да се обърне на обработваните от организацията данни – често те подлежат на допълнителни регулации, необхващащи останалата дейност на организацията. Например за организация, базирана в Япония, Регламент (ЕС) 2016/679 не обхаща локалните лични данни, които тя обработва, освен ако тя не принадлежат на граждани на ЕС. Различните организации могат да дефинират и използват различни типове чувствителни данни в зависимост от своите нужди, законодателната рамка, действащите регулаторни режими – например регулации, приети политики за сигурност, нужни сертификации, специфични данни при участие в

определени проекти или обединения от няколко организации.

В информационната сигурност се използват редица подходи за защита, всеки от които има определена област на приложение, отговаряща на въпроса „Къде?“ и определена функционалност - „Как?“. За пример можем да използваме многослойния модел на защита, състоящ се от няколко слоя - Външна мрежа, Мрежов периметър, Вътрешна мрежа, Компютърно оборудване, Приложения и Данни. Всеки защитен слой е подложен на различни по характер заплахи и за защита от тях разполага с определен набор от подходи за сигурност. За комплексната защита на организацията се комбинират подходите за информационна защита при мрежова комуникация и подходите за защита на данни при йерархична организационна комуникация. Към познатите ни подходи за информационна защита при мрежови комуникации можем да добавим и допълнителни подходи, като демилитаризирана зона, виртуална частна мрежа, одит, тестове за проникване, анализ на уязвимости, хеширане на пароли, филтриране по и други [29].

Всеки един от тези подходи има своята роля и особености при защитата на определени активи, намиращи се в определен слой, и изискващи определени усилия и ресурси. Информационната сигурност (ИС) е свързана със осигуряване на безопасността на тези активи. Най-добрият подход за това е да се разгледа всеки актив в контекста на свързания с него риск от загуба и неговата стойност. Основна цел на ИС е защита на информацията във всичките ѝ форми. В резултат на повсеместното проникане на информационните технологии, информационната сигурност има отношение към все повече аспекти на съвременния живот, като производство, работен процес, ежедневна комуникация, пазаруване или забавления [29]. Същото важи и за жизненоважните обекти от критичната инфраструктура, осигуряващи електричество, вода, телекомуникации, транспорт. Те са изцяло зависими от информационните технологии и най-вече от осигуряването на тяхната безопасност [33]. Информационната сигурност се отнася до защитата на активи – информация, хардуер, софтуер, процеси или комбинации от тях. За да се прецени какво да се защитава, първо трябва да се определи кои активи са ценни и за кого [4].

Проектирането и последващото внедряване на съвременна система за информационна сигурност (СИС) е от съществено значение за жизнеността на съвременната организация, която, освен че трябва да осигури защита на своите активи е необходимо и да се съобразява с редица нормативни и регулационни изисквания, добри практики и стандарти.

Цел и задачи на дисертацията

Целта на дисертацията е създаване на метод и модели за разработване на системи за информационна сигурност, осигуряващи защита от вътрешни заплахи в посока отвътре-навън на чувствителна информация за различни по характер и размер организации. Разработеният метод трябва да е приложим за създаване на СИС, реализиращ подход за защита на чувствителни данни чрез използване на платформа от тип СПИД, подходящ за приложение в различни по големина организации, като обекти от критичната инфраструктура, предприятия, боравещи с индустриални тайни, търговски или научно-изследователски организации.За постигането на тази цел са формулирани следните задачи:

1. Определяне и класифициране на подходи за управление на информационна сигурност и области на приложение;
2. Анализ на областта „Информационна сигурност“ като част от проблемната област на Система за Информационна Сигурност;
3. Описание на проблемната област на Системите за Информационна Сигурност в организации чрез концептуално моделиране;

4. Анализ и приложение на обектно-ориентиран подход при създаване на проектен модел на система за информационна сигурност на базата на създаден концептуален модел;
5. Определяне на подход за трансформиране на проектния модел на СИС в модел на реализация;
6. Симулиране на СИС и анализ на генерираните тестови данни.

Методология

За постигане на формулираните в дисертационния труд цел и задачи е използван обектно-ориентиран подход при проектиране и реализация на софтуерни системи „отгоре-надолу“. Това е методология, използвана широко от софтуерните инженери, при която се цели да се избегне зависимостта от включените в системата конкретни технически средства и се формулира метод за разработване, постигащ висока степен на формализация. Постигнатият резултат обикновено представлява стъпка към постигане на референтен модел за създаване на програмна система в определена област.

Списък с авторски публикации по дисертацията

Публикациите по дисертацията са докладвани и приети за публикуване в сборниците на три международни конференции, едно в специализирано международно списание с импакт фактор и едно в издание на международно академично издателство.

[1] Gaidarski I., Model Driven Development of Information Security System, Problems Of Engineering Cybernetics And Robotics, Bulgarian Academy Of Sciences, 2021, Vol. 76, pp. 47-62, p-ISSN: 2738-7356; e-ISSN: 2738-7364, DOI: 10.7546/PECR.76.21.04

[2] Gaydarski, I., Minchev, Z., Andreev, R.. Model Driven Architectural Design of Information Security System. Advances in Intelligent Systems and Computing, Madureira A., Abraham A., Gandhi N., Silva C., Antunes M. (eds) Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018)., 492, Springer, 2019, ISBN:978-3-030-17064-6, ISSN:2194-5357, DOI:10.1007/978-3-030-17065-3_35, 349-359.

[3] Gaydarski, I., Minchev, Z., Conceptual Modeling of Information Security System and Its Validation Through DLP Systems. Proceedings of BISEC 2017, Belgrade Metropolitan University, 2017, ISBN:978-86-89755-14-5, DOI: 10.13140/RG.2.2.32836.53123, 36-40

[4] Gaydarski, I., Minchev, Z.. Virtual Enterprise Data Protection: Framework Implementation with Practical Validation. Proceedings of BISEC 2018, October 20, Belgrade, Serbia, Belgrade Metropolitan University, 2019, ISBN:978-86-89755-17-6, DOI:10.13140/RG.2.2.19996.33925, 10-15

[5] Gaydarski I., Kutinchev P., Holistic Approach to Data protection - identifying the weak points in the organization.. Proceedings of BdKCSE’2017 (7 December, 2017 Sofia), САИ, 2018, ISSN:2367-6450, 125-135

Участие в проекти

В рамките на разработването на дисертационния труд докторантът е взел участие в следните научни проекти:

1. Научно-изследователски проект на тема: „Концептуално и симулационно Моделиране на Екосистеми за Интернет на Нещата (КоМЕИН)“, Договор № ДН 02/1 от 13.12.2016 г., Конкурс за финансиране на фундаментални научни изследвания – 2016 г., Математически науки и информатика;
2. Програма Млади учени и докторанти в БАН 2017, Научно направление „Информационни и комуникационни науки и технологии“, Научноизследователски проект вх. № 72-00-40-230/10.05.2017 г. на тема „Моделиране на архитектура на системи за информационна сигурност в организации.”.Договор N:ДФНП–17-101/ 28.07.2017. Финансиране: Програма за подпомагане на млади учени и докторанти на БАН–2017г.
3. Научно-изследователски проект на тема: „Информационни и комуникационни технологии за единен цифров пазар в науката, образованието и сигурността (ИКТвНОС)“, Договор N:ДО1-205/23.11.2018

Научни и Научно-приложни приноси:

1. Предложена е нова класификация на подходите за управление на ИС, в зависимост от вида комуникация и детайлно описание на фундамента на областта на информационната сигурност, основаващо се на нейните основни понятия;

2. Предложен е нов метод за разработване на системи за информационна сигурност в организации, който интегрира моделно-базирано разработване на СИС чрез прилагане на подхода „отгоре-надолу“ с нов метод за анализ на проблемната област на този вид системи. Характерно за предложеният метод е, че е технологично независим /условие да послужи за основа за създаване на референтна методология за разработване на този вид системи/; гъвкав /позволява разширяване на съществуваща СИС с нова функционалност/; подпомага постигането на оперативна съвместимост на СИС със съществуваща информационна система на организация чрез използване на един и същи подход за моделиране на двете системи;

3. Разработен е многослоен концептуален модел на проблемната област на системите за информационна сигурност като резултат от прилагането на две и повече от две гледни точки при нейното описание;

4. Конструирани са архитектурен и функционален модели на системите за информационна сигурност на базата на съществуващ концептуален модел на проблемното пространство с помощта на обектно-ориентирания унифициран език за описание на програмни системи UML;

5. Сравнителен анализ на съществуващи СПИД платформи за реализация на базата на изискванията, описани в модела на анализа;

6. Предложен е модел на реализация на СИС в организация, използваща СПИД платформа за реализация „Cososys Endpoint Protector 5.0.2.1“

7. Реализиран е симулационен модел на СИС на базата на обектно-ориентирано описание на архитектурата му чрез използване на агентно-базирано представяне в средите NetLogo и I-SCIP-SA; Симулационно изследване на архитектурата на СИС чрез извършване на стохастична валидация и интерактивна верификация.

Съдържание на дисертацията

Дисертационният труд е в обем от 142 страници, 48 фигури, 13 таблици, 139 цитирани литературни източника и 2 приложения. Състои се от увод, четири глави и заключение, декларация за оригиналност на резултатите, библиография и приложения.

В увода са разгледани актуалност на проблема, основни заплахи в киберпространството, регулации и законови рамки.

В Глава 1 са представени основните концепции и базовите принципи за осигуряването на ИС. Разгледани са различни подходи за управление на ИС, областите на тяхното приложение, както и основните научни области от значение за разработване на системи за ИС. Представен е наш метод за разработване на системи за информационна сигурност в организации, фазите от които се състои, моделите, които се конструират при прилагането му и неговите характеристики. Дефинирана е рамка за описание на архитектура на системата. Формулирани са основната цел и задачи на дисертацията.

В Глава 2 са дефинирани основните понятия в ИС чрез използване на наш метод за анализ на областта на СИС, при който се отчитат гледните точки на всички заинтересовани участници при нейното разработване. Целта е да се приложи подхода „отгоре-надолу при проектиране на такава система, което дава възможност да се достигне до решения, които не са свързани с конкретна реализация и могат да са насочващи при създаване на системи от този вид. В резултат, направеният анализ е основа за създаване на концептуален модел на проблемната област на СИС.

В Глава 3 е представен представен метод за проектиране на Системата за Информационна Сигурност, предназначена за организации и насочена към защита от изтичане на чувствителна информация отвътре-навън, т.е. в резултат от действие на вътрешни лица с легитимен достъп до ресурсите на организацията и до нейните данни. Разгледани са възможностите на обектно-ориентиран подход за създаване на проектен модел на СИС. Показан е начин за трансформиране на концептуалния модел на СИС в обектно-ориентиран проектен модел чрез използване на обектно-ориентирания език за описание UML.

В Глава 4 е описан подход за създаване на модел на реализация на СИС чрез предлаганата от нас методология за разработване на СИС. На базата на проектен обектно-ориентиран модел е изграден ОО модел на реализация, съобразен със съществуваща среда за реализация. Извършен е анализ на проблемната област и на базата на изграден концептуален модел, резултат от този анализ, са уточнени изискванията към архитектурата на разработваната СИС. Извършен е анализ на съществуващи платформи за реализация СПИД и избор на най-подходящата в съответствие с модела на анализа. Показано е как представеният от нас метод дава възможност за моделиране и реализация на нови аспекти от СИС без да се налага системата да се проектира отначало. Представени са и резултати от изпитания на разширена СИС. Създаден е агентно-базиран модел на реализация чрез трансформиране на обектно-ориентиран проектен модел. На базата на агентно-базирания модел е извършена симулация на работата на СИС чрез средите за симулиране NetLogo (v.6.0.4) и I-SCIP-SA. Извършен е анализ на базата на тестовите данни, както и на данни от реални ситуации..

Увод

Увода се състои от актуалност на проблема и основни заплахи в информационната сигурност. Разгледани са актуалните направления за изследване

на заплахи в киберпространството, както и заплахи за сигурността през последната година. Разгледани са и са систематизирани заплахи, свързани с КОВИД-19. Направен е преглед на основните регулации и законови рамки в областта на информационната сигурност – единна политика за сигурност, процедури, процеси и стандарти за ИС, приемани в организациите с цел съвместимост с регулаторни и законови изисквания, стандарти и добри практики за ИС. Направен е обзор на националното законодателство в облaстта на ИС, действащо на територията на държавата в която тя е регистрирана или оперира – данъчно законодателство, наказателен кодекс, разрешителни режими. Показана е структурата на дисертацията.

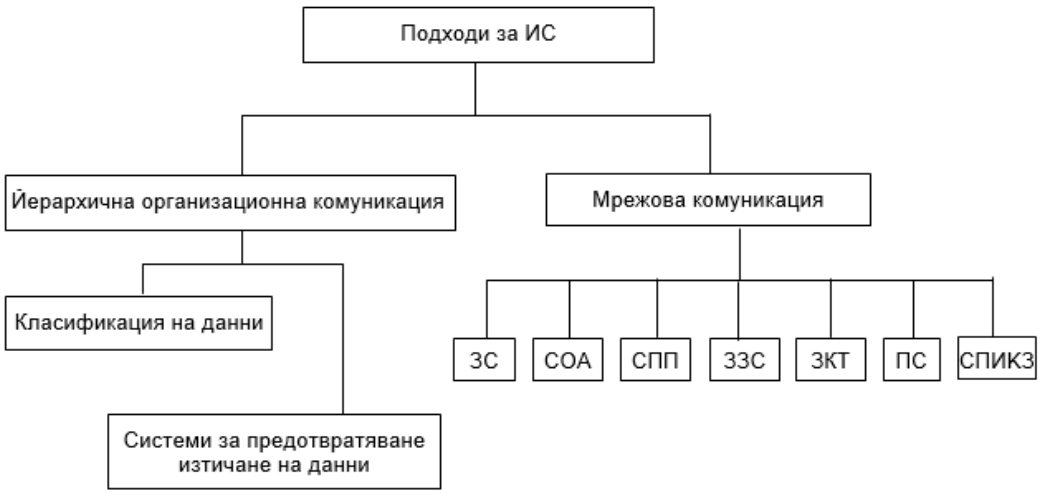
Глава 1. Базови принципи и метод за разработване на система за информационна сигурност

1.1 Базови принципи за осигуряване на информационна сигурност

В тази подточка са разгледани базовите принципи за осигуряване на информационна сигурност, известни като: Триада „Поверителност, Цялостност, Наличност“ (ПЦН Триада, CIA Triad), принципа на тройното А (ААА) и принцип на най-слабото звено. Разглеждаме и базовите защитни модели, като периметрова защита, известна като „Модел на близалката“(Lollipop model), многослоен модел, известен като „Луков модел“ (Onion model) и др.[2, 21].

1.2 Подходи за управление на информационна сигурност

В тази подточка са систематизирани съществуващите подходи за ИС в организации, в зависимост от вида на комуникацията. В организациите могат да се разграничат два вида комуникации, предопределящи подходите за ИС: комуникация на базата на равнопоставеност – „Мрежова комуникация“ (Мрежи от/в организации) и „Йерархична организационна комуникация“ (Фигура 3) [48].



Фигура 3. Подходи за ИС в зависимост от вида комуникация

1. Подходи за управление на ИС при мрежови комуникации:
    - Защитна стена (ЗС);
    - Системи за откриване на аномалии (СОА);
    - Системи за предотвратяване на проникване (СПП);
    - Защита от зловреден софтуер (ЗЗС);

- Защита на крайните точки (ЗКТ);
- Периметрова сигурност (ПС);
- Системи за предварителна информация за кибер-заплахи (СПИКЗ).

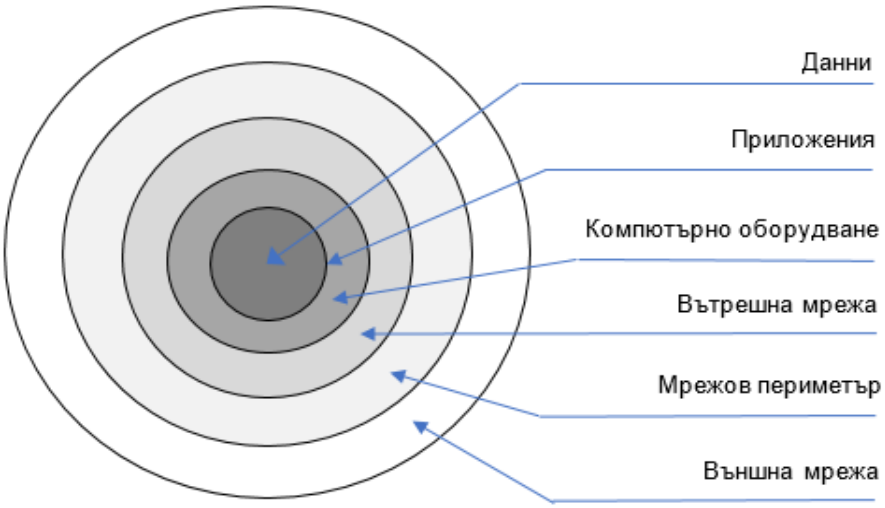
2. Подходи за управление на ИС при Йерархична комуникация в организация:

- Класификация на данни (КД);
- Системи за предотвратяване на изтичане на данни (СПИД).

Подходите за управление на ИС определят начина по който се реализират целите в една СИС.

1.3 Области на приложение на различните подходи за информационна сигурност

Тук са разгледани областите на приложение на различните подходи за защита. За илюстрация може да бъде използван многослойния модел на защита (Фигура 4), състоящ се от няколко слоя:



Фигура 4. Многослоен модел на защита

Всеки защитен слой е подложен на различни по характер заплахи и за защита от тях разполага с определен набор от подходи за сигурност (Таблица 1).

Области на приложение	Подходи за сигурност
Външна мрежа	Демилитаризирана зона, Виртуална частна мрежа, Създаване на дневници, Одит, Тестове за проникване, Анализ на уязвимости, Активна защита чрез примамки (Honepots)
Мрежов Периметър	Защитна стена, Прокси сървър, Създаване на дневници, Пакетна филтрация, Статична пакетна филтрация, Динамична пакетна филтрация, Тестове за проникване, Анализ на уязвимости, Активна защита чрез примамки (Honepots)
Вътрешна мрежа	СОА, СПП, Създаване на дневници, Одит, Тестове за

	проникване, Анализ на уязвимости.
Компютърно оборудване	Автентичност, Защита на крайните точки, Защитна стена, Хеширане на пароли, Създаване на дневници, Одит, Тестове за проникване, Анализ на уязвимости, СПИД.
Приложения	Филтриране по съдържание, Валидация на данни, Одит, Тестове за проникване, Анализ на уязвимости, КД.
Данни	Криптиране, Контрол на достъп, Архивиране на данни, Тестове за проникване, Анализ на уязвимости, Класификация на данни, СПИД, КД, структурни мерки за повишаване на устойчивостта (Resilience)

Таблица 1. Подходи за сигурност и области на приложение

За комплексната защита на организацията се комбинират подходите за информационна защита при мрежова комуникация и подходите за защита на данни при йерархична организационна комуникация. Освен вече познатите ни ЗС, СОА, СПП, ЗЗС, ЗКТ, ПС, СПИКЗ, КД и СПИД, са добавени няколко допълнителни подхода за сигурност [29]: Демилитаризирана зона (DMZ), Виртуална частна мрежа (VPN), Създаване на дневници (Logging), Одит (Auditing), Тестове за проникване (Penetration testing), Анализ на уязвимости (Vulnerability Analisys), Сървър - посредник (Proxy), Пакетна филтрация (Packet Filtering), Статична пакетна филтрация (Static packet Filtering), Динамична пакетна филтрация (Dynamic packet Filtering), Хеширане на пароли (Password Hashing), Филтриране по съдържание (Content Filtering), Валидация на данни (Data Validation), Криптиране (Encryption), Контрол на достъп (Access Controls), Архивиране на данни (Backup), структурни мерки за повишаване на устойчивостта (Resilience), Активна защита чрез примамки (Honepots).

1.4 Основни научни области от значение за разработката на системи за информационна сигурност

Тук са представени основните научни области, необходими за разработката на ефективни системи за информационна сигурност: информационна и кибер-сигурност, проектиране на системи, анализ на данни, големи масиви от данни, машинно самообучение, изкуствен интелект, софтуерно инженерство, и системен анализ.

Разгледани са подробно области като софтуерно инженерство и системен анализ, принципите на които използваме за разработка на нашия метод за проектиране на СИС в организации. Особено внимание е отделено на процеса на разработване на системи (Фигура 5), състоящ се от основни компонента и връзките между тях, разгледани в контекста на разработване на СИС:

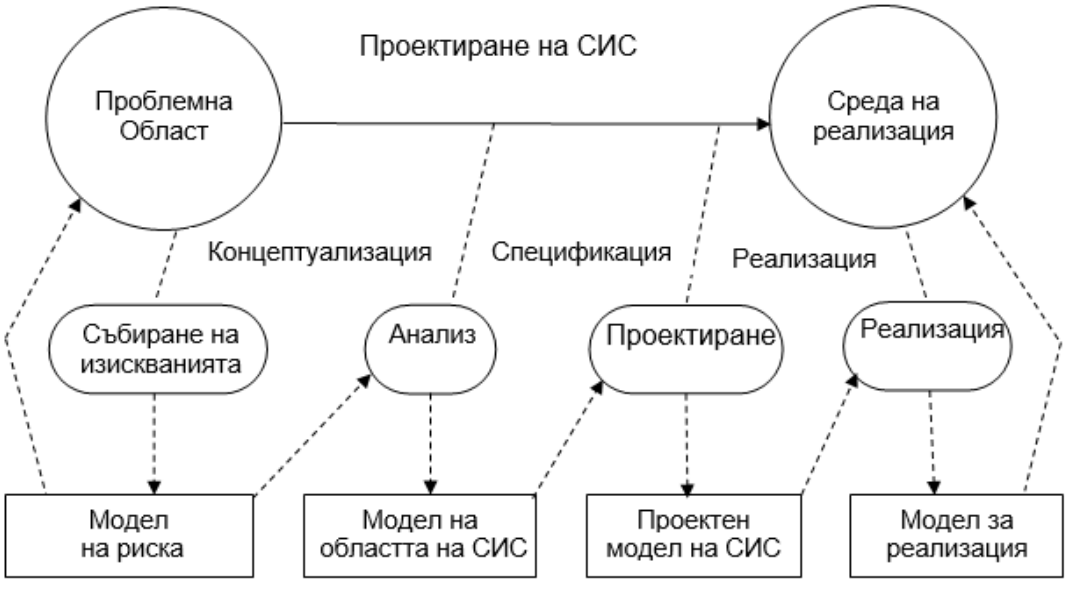
- Проблемна област - дефинира областта в която се решава проблема на СИС;
- Проблем - реализация на определен начин на функциониране на СИС, която трябва да заработи в дадена среда;
- Среда на реализация - представлява условията при които се реализира СИС;
- Етапи - Това са етапите през които трябва да премине разработката на СИС;
- Създаване на модели на СИС на различни етапи от разработката;
- Трансформиране на моделите от един вид в друг.

Различават се следните етапи на разработване на СИС:

- Събиране на изискванията – определяне на възможните рискове според разбирането на потребителите;
- Анализ - изследване на проблемната област от различни гледни точки на заинтересованите страни;
- Проектиране – проектиране на структурата и процесите в системата;
- Реализация – съобразяване на осъществяването на СИС с конкретната среда за реализация.

Моделите, чрез чиято трансформация се достига до реализацията на конкретна СИС са:

- Модел за описание на риска, които се управлява със СИС, на база на събраните изисквания към системата;
- Модел на областта на СИС – модел, получен в резултат на анализа на проблемната област;
- Проектен модел на СИС - описание на архитектурата и функционалността;
- Модел на реализация - модел за реализация на проектираната СИС в зависимост от условията при която тя ще работи.



Фигура 5. Цикъл на разработване на системи

1.5 Метод за разработване на системи за информационна сигурност в организации

Методът се състои от следните фази (Фигура 6):

1. Определяне на рамка за описание на архитектурата на СИС, съгласно стандартите IEEE 1471 [67, 88, 89] и IEEE 42010 [67, 89]. Рамката се формира от множеството от гледни точки на заинтересованите страни/наблюдатели.

2. Анализ на проблемната област на СИС, за определяне на изискванията към системата от различни гледни точки. На базата на този анализ се формират изискванията към СИС.

3. Изграждане на концептуален модел на проблемната област от различни гледни

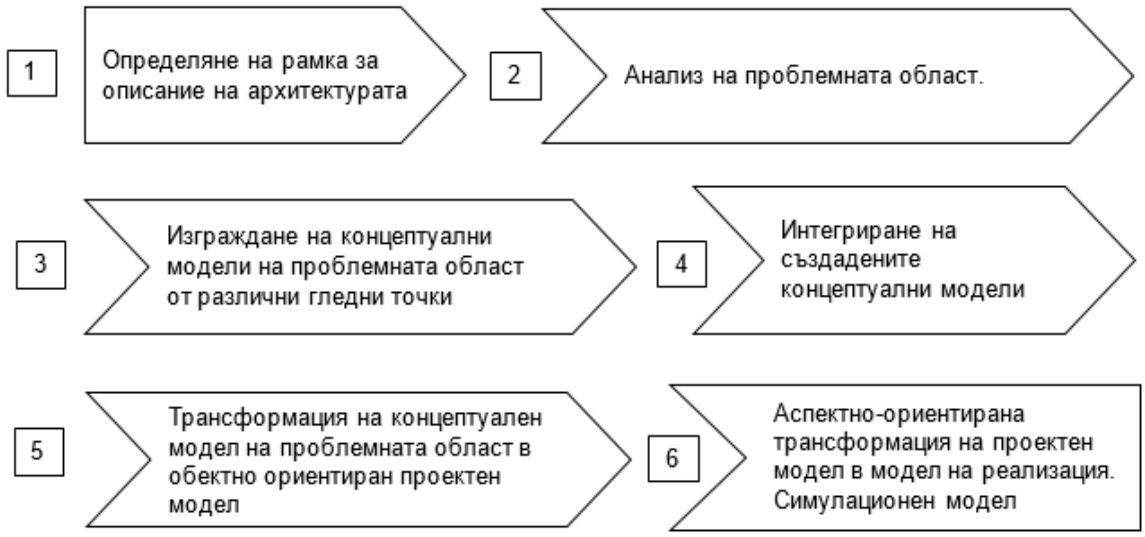
точки. Създаване на обобщен и детайлизирани концептуални модели.

4. Интегриране на концептуалните модели, създадени от различни гледни точки. Подходът на концептуалното моделиране позволява лесно и унифицирано представяне на ниво концепции на СИС от различни гледни точки. Това улеснява комуникацията между наблюдателите на разработваната СИС, които са свързани със съответните гледни точки.

5. Трансформация на концептуален модел на проблемната област в обектно ориентиран проектен модел.

6. Аспектно-ориентирана трансформация на проектен модел в обектно-ориентиран модел на реализация и агентно-базиран симулационен модел.

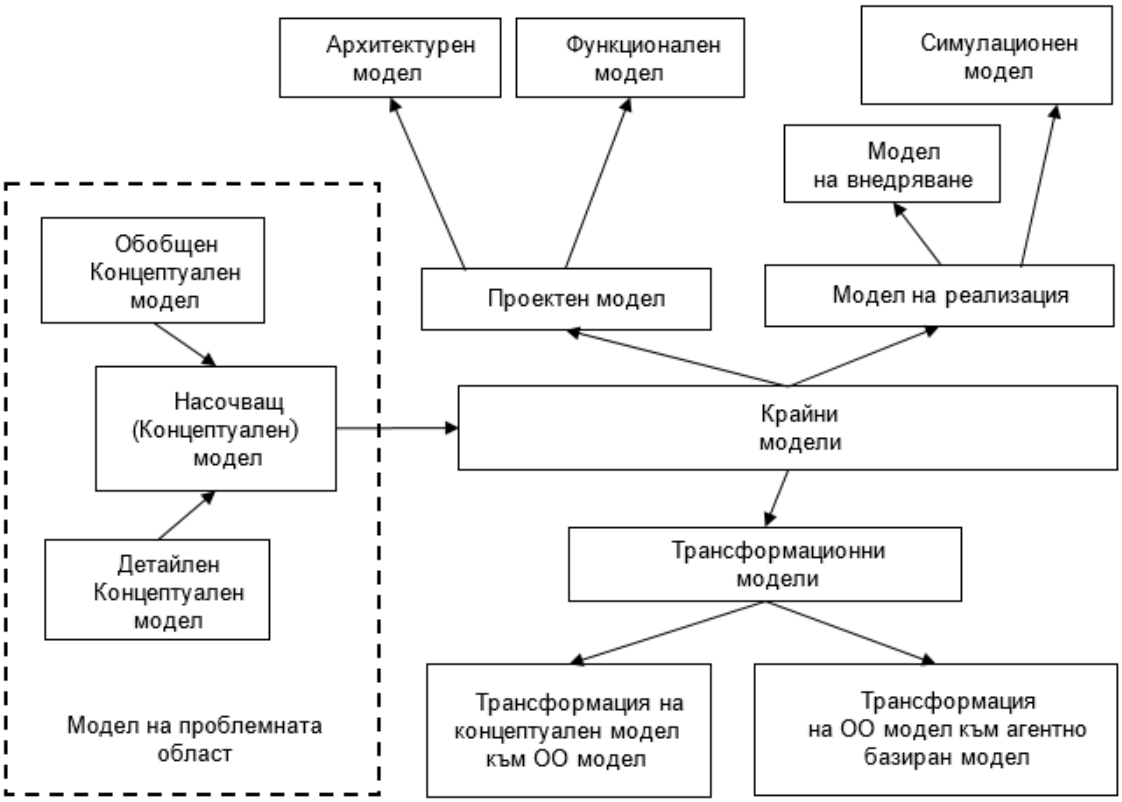
Моделите, които се конструират при прилагане на метода са показани на Фигура 7 [135,136]. На базата на анализ на проблемната област се конструира концептуален модел, наречен "Насочващ модел", чрез който се представя желаната архитектура на системата. Носочващият модел не е свързан с конкретна реализация, а служи за описание на основните компоненти от архитектурата на системата. Концептуалния модел отразява проблемната област от различни гледни точки. От своя страна този модел се състои от "Обобщен модел" и "Детайлен модел".



Фигура 6. Метод за разработване на СИС

На неговата база, след съответна трансформация се създават следващите два основни модела - "Проектен модел" и "Модел на реализация". Проектният модел е обектно-ориентиран и се състои от "Архитектурен" и "Функционален" модели, които представят описанието, съответно на архитектурата и функционалността на системата. "Модела на реализация" представя конкретна реализация на системата и може да се осъществи по два начина - чрез симулация на реална система ("Симулационен модел") и чрез използването на конкретни съществуващи системи, представляващи платформи за реализация на СИС, като СПИД ("Модел на внедряване"). Проектният модел и модела на реализация, са представители на крайните модели, които описват системата за целите на нейното разработване.

Чрез трансформационните модели, се представят трансформациите между моделите - "Трансформация на концептуален модел към ОО модел" и "Трансформация на ОО модел към агентно базиран модел".



Фигура 7. Модели за разработване на СИС

Характеристики на метода:

- Методът е моделно базиран, в резултат на прилагане на подход „отгоре-надолу“;
- Прилага се трансформация от „модел към модел“;
- Аспектно-ориентирана трансформация на проектен модел към модел на реализация в зависимост от две области на интерес на реализатора на системата: обектно-ориентиран подход и агентно-базиран подход.
- Технологично независим, което създава условия да е основа на референтна методология за разработване на СИС

Подходът „отгоре-надолу“, който се прилага при разработване на система за информационна сигурност е подход от общото към частното /конкретното/. Той дава възможност да се прилага и разглежда обща политика, процедури и процеси за ИС с цел постигне на определени цели, Той е подходящ за създаване на референтна методология за разработване на СИС, основана на определяне на рамка за тяхното проектиране, тъй като е технологично независим..

1.6 Дефиниране на рамка за описание на архитектура на системата

Осъществяването на първия етап, се базира на указанията за създаване на рамка за архитектурно описание на системи, представени в стандартите IEEE 1471 [88] и ISO/IEC/IEEE 42010 [89].

Тези стандарти въвеждат понятия, свързани с начина на описание на архитектурата на една система [67]: Околна среда (Environment), Заинтересована страна (Stakeholder), Област на интерес (Concern), Изглед (View), Гледна точка (Viewpoint),

Архитектура на системата (System Architecture), Архитектурно описание (Architectural description), Рамка на създаване на архитектурно описание (Architectural framework), Архитектурен изглед (Architectural View), Архитектурна гледна точка (Architectural Viewpoint), Вид на модела (Model kind).

Тези концепции са приложими при анализа на областта “Система за Информационна сигурност” и осигуряват контекст за дефиниране на обща концептуална рамка, позволяваща изграждането на концептуални модели на СИС. На Фигура 8 е показана областта на интерес на СИС, която се използва за рамка за анализ на областта на система за Информационна сигурност в настоящата дисертация.

Разработването на комплексни системи включва множество участници - всеки със своя собствена перспектива. Това са така наречените „заинтересовани страни“. Всяка заинтересована страна притежава съответни умения, отговорности, знания и опит, които определят отношението и изискванията към системата. При система, в която се използват различни технологии (софтуерни, хардуерни) и има разнообразни нормативни и регулаторни изисквания е неизбежно пресичането или припокриването на различните перспективи на участниците в процеса на нейното разработване. Допълнително усложняващо обстоятелство е факта, че знанията на заинтересованите страни се представят по различни начини. Различните изисквания се отнасят до различни етапи от разработването на системата и всяко от тях може да бъде подчинено на различни стратегии. Така една от важните задачи в процеса на разработка на системата е координацията на заинтересованите страни и унифицираното представяне на техните изисквания и приноси към системата.
Този проблем се решава чрез предлагания от нас метод за разработка на системи за информационна сигурност в организации.

Фигура 8. Област на интерес на СИС

Методът отчита и унифицира изискванията на различните елементи и гледни точки в областта на интерес на системата за информационна сигурност, която разглеждаме:

- Гледна точка „Информационна Сигурност“ – включва основните понятия в информационната сигурност (Заплахи, Уязвимости, Източници, Мотивация и

др.), както и основните подходи за реализиране на информационна сигурност в организации;
- Гледна точка „Риск анализ“ - чрез риск анализа се определят изискванията към СИС;
- Комуникационна гледна точка – определя начина на комуникиране, предопределящ подхода за защита на информацията.
- Технологична гледна точка. Тази гледна точка включва различни подходи при информационните и комуникационни технологии като обектно-ориентиран подход, агентен подход и други.
- Гледна точка „Обработка на информация“– включваща трите основни видове данни, дефинирани съгласно информационната сигурност – Данни в покой (Data-in-Rest), Данни в движение (Data-in-Motion) и Данни в употреба (Data-in-Use).

1.7 Заключение

В главата са представени основните базови принципи и защитни модели за осигуряване на информационна сигурност. Представените подходи за управление на ИС в организации, са разделени в две групи, в зависимост от вида на комуникацията в организацията, предопределящи съответните подходи за ИС: комуникация на базата на равнопоставеност – „Мрежова комуникация“ (Мрежи от/в организации) и „Йерархична организационна комуникация“. Показани са областите на приложение на различните подходи за информационна сигурност.

Представени са основните научни области от значение за разработване на системи за информационна сигурност. Обърнато е специално внимание на системния анализ и цикъла за разработване на системи. Основните компонента и връзки между тях, са разгледани в контекста на разработване на СИС.

Представена е рамка за архитектурно описание на системи, на базата на стандартите IEEE 1471 и ISO/IEC/IEEE 42010.

Дефинирани са основната цел и задачи на дисертацията.

Глава 1 описва изпълнението на задача 1, дефинирана в "Цел и задачи на дисертацията":

- Определяне и класифициране на подходи за управление на информационна сигурност и области на приложение;

В резултат на научноизследователската дейност са постигнати следните научни и научно-приложни приноси:

1. Предложена е нова класификация на подходите за управление на ИС, в зависимост от вида комуникация и детайлно описание на фундамента на областта на информационната сигурност, основаващо се на нейните основни понятия;
2. Предложен е нов метод за разработване на системи за информационна сигурност в организации, който интегрира моделно-базирано разработване на СИС чрез прилагане на подхода „отгоре-надолу“ с нов метод за анализ на проблемната област на този вид системи.

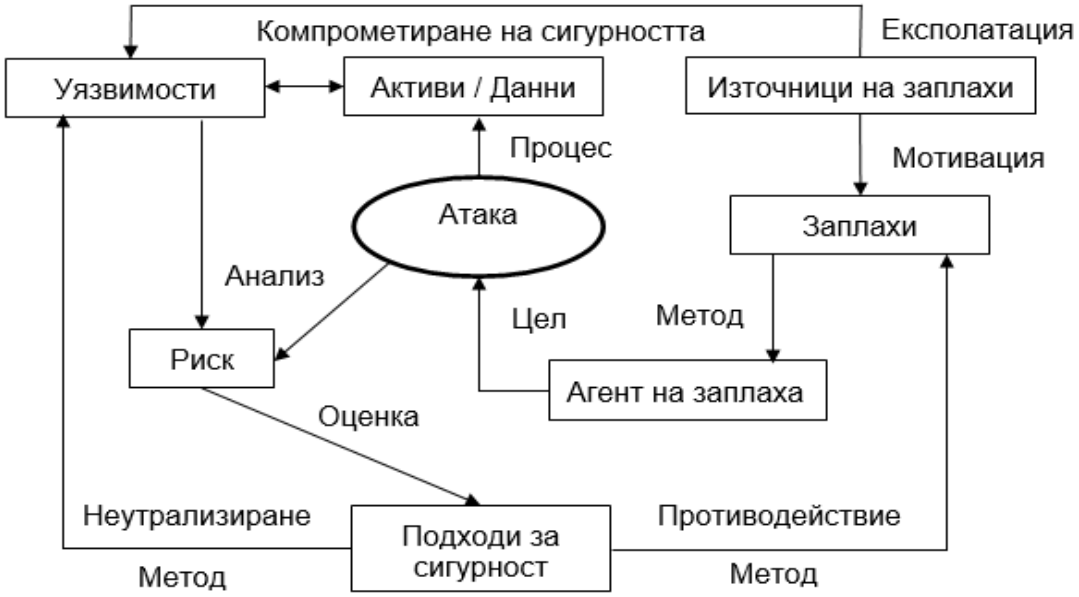
Глава 2. Анализ на проблемната област

2.1 Информационна сигурност - основни понятия и подходи за реализиране

В тази точка са разгледани основните понятия и подходи за реализиране на ИС.

2.1.1 Основни понятия в информационната сигурност

Тук представяме фундамента на областта на информационната сигурност, описан чрез нейните основни понятия (Фигура 9).



Фигура 9. Уязвимости, заплахи и атаки

Дефинираме основните понятия на ИС: „Събитие“, „Сигнали / Аларми“, „Инцидент“, „Нарушение“ (Breach), „Уязвимост“ (Vulnerability), „Заплаха“ (Threat), „Агент на заплаха“ (Threat Agent), „Атака“, „Изтичане на данни“ (Data Breaches), „Загуба на данни“ (Data Loss).

2.1.2 Уязвимости. Заплахи. Източници и агенти на заплахата

В тази поддточка подробно са разгледани понятията „Уязвимости“, „Заплахи“, „Източници“ и „Агенти на заплахата“ и тяхната взаимовръзка.

2.1.3 Вектори, цели и характер на заплахата

Тук са разгледани понятията „Вектор”, „Цел” и „Характер на заплаха”. Според вектора на заплаха, заплахите могат да се класифицират на външни и вътрешни.

„Външни заплахи“

Посоката на атаката при външните заплахи е отвън навътре, срещу защитените информационни активи. При външните заплахи се използва принципа на най-слабото звено. Атакуващата страна се опитва да намери пропуски в защитата чрез които да проникне в защитената мрежа, сървъри или работни станции и да поеме контрол върху информационните активи или инфраструктура. Такива са например: хакерски атаки, DoS атаки, Червеи (Worms), Троянски коне (Trojans), Бот-Мрежи (Botnet), Атаки за отказ на услуга - DoS и DDoS атаки, Заплаха тип Drive-by Exploits, и Инжектиране на код (Code Injection Attacks) [25].

„Вътрешни заплахи“

Инцидент, причинен от вътрешна заплаха възниква, когато вътрешно лице - служител, партньор или доставчик с оторизиран достъп до чувствителна за организацията информация или система, целенасочено или случайно злоупотреби с този достъп, като това води до отрицателни за организацията последствия. Съществуват множество причини за инциденти, свързани с вътрешни заплахи.

- Небрежно поведение на вътрешните лица;
- Доставчици и външни контрактори;
- Прекалено строги политики за киберсигурност – „Security Fatigue“;
- Кражба на електронна идентичност;
- Злонамерени потребители.

Вътрешните заплахи могат да се разделят на няколко основни групи според техния източник: Човешка заплаха, Активност на потребителите и Бизнес-приложения

2.1.4 Атаки и противодействие

В тази поддточка подробно са разгледани категориите атаки, техния механизъм и подходите за неутрализирането им.

2.1.5 Подходи за информационна сигурност

Подходите за информационна сигурност (ПИС) представляват мерки под формата на действия, процеси или процедури, предприети за защита на информационната система от атаките срещу Поверителността, Целостта и Наличността на информационната система. Целта е редуциране на риска, свързан с информационната сигурност [12]. Подходите са организационни, технологични и технически, и се прилагат в съответствие със спецификата на дейността на Субекта [15] (Наредба за минималните изисквания за мрежова и информационна сигурност). Според времето на своето действие, ПИС може да се групират логически в няколко категории [2, 12, 13]: Превантивни, Разкриващи, Възпиращи, Корективни, Възстановителни и Компенсативни.
ПИС могат да имат различна физическа реализация [2,12,13,14]: ПИС за физическа сигурност, Административни, Технологични, Оперативни и Виртуални.

2.2 Риск анализ

В тази точка разглеждаме понятията риск, управление на риска, оценка на риска.и методи за оценка на риска. Като част от оценката на риска са разгледани и процесите на идентифициране на заплахи и уязвимости и оценка на активите. Описани са и процесите на потискане на риска и периодичен процес на оценка

2.3 Видове комуникации

Тук са разгледани видовете комуникация в организацията от гледна точка на подходите за осъществяване:

- *„Йерархична организационна комуникация“* - комуникация в рамките на дадена организация основана на йерархичната структура на организацията;
- *„Мрежова комуникация“* - комуникация, осигуряваща равнопоставеност между участниците в нея.

В зависимост от спецификата на двата вида комуникация се използват различни подходи за информационна сигурност. В настоящата дисертация е разгледана йерархичната организационна комуникация и съответните подходи за защита чрез Системи за предотвратяване изтичането на данни (СПИД), познати още и като Data Leak Prevention.

От гледна точка на комуникационните процедури и тяхното формализиране се различават формална и неформална комуникация:

- *Формалната комуникация* следва както йерархичната структура на организацията, така и хоризонталната комуникация между служителите. Тя се съобразява със зададени шаблони, характерни за организацията, като приоритет имат съобщенията спускани от ръководството надолу по структурата;
- *Неформална комуникация* е ежедневната комуникация между служителите. Тя не следва зададени шаблони, нито строга йерархия, но има жизненоважно значение за организацията, защото чрез нея се извършват всекидневните задачи.

2.4 Технологична гледна точка при проектиране на СИС

В тази подточка са разглеждани различни технологични подходи за разработването на система за информационна сигурност: Обектно-ориентирания подход, Агентен подход и Мулти-агентни системи.

2.5 Обработка на информация

Тук са разгледани видовете данни, обработвани, използвани и създавани от организациите. Всяка организация индувидуално определя кои данни са жизненоважни за нейното функциониране и кои са второстепенни или поддържащи. По дефиниция чувствителните данни са тези данни, които дадена организация не може да си позволи да загуби, да бъдат разкрити или да станат достояние на неоторизирани лица.

В зависимост от това как данните се използват, съхраняват или пренасят от различните системи и приложения се разграничават 3 основни състояния:

- Данни в покой;
- Данни в движение;
- Данни в употреба.

2.6 Заключение

Представеният анализ на областта на системите за информационна сигурност е част от приложения подход за разработване на такива системи, известен като „отгоре-надолу“. Той дава възможност да се разглежда и прилага обща политика, процедури и процеси за ИС с цел постигне на определени цели. Подходящ е за създаване на референтна методология за разработване на СИС, основана на определяне на рамка за тяхното проектиране.

Направен е опит да се осъществи един цялостен поглед върху СИС от няколко гледни точки: Информационна Сигурност, Риск анализ, Обработка на информацията, Подходящи компютърни технологии за разработване на системата и възможни видове комуникация – обект на информационна защита. Всяка гледна точка представлява перспектива, в която трябва да се разглежда областта на съществуване на системата. Най-голямо внимание и най-детайлно е описана областта на информационната сигурност, тъй като тя е фундамента на системите за информационна сигурност.

Взаимосвързаността на отделните гледни точки довежда до интересни резултати. Например съвместното прилагане на комуникационната гледна точка и тази на информационната сигурност довежда до създаване на нова квалификация на подходите за управление на информационната сигурност, която е представена в глава 1 на дисертационния труд. Взаимозависимостта между гледните точки Информационна сигурност и Обработка на информацията довежда до въвеждането на нови понятия и нов аспект за оценка на информацията – чувствителност. Същото може да се каже и за влиянието на гледната точка Информационна сигурност върху

технологията, известна като Агентен подход.

Глава 2 описва изпълнението на задача 2, дефинирана в "Цел и задачи на дисертацията":

- Анализ на областта на Информационна сигурност като част от проблемната област на Система за Информационна Сигурност;

В резултат на научноизследователската дейност за определяне и класифициране на подходи за управление на информационната сигурност и при анализа на информационната сигурност като част от областта на системите за информационна сигурност са постигнати следните научни и научно-приложни приноси:

1. Предложен е нов метод за разработване на системи за информационна сигурност в организации, който интегрира моделно-базирано разработване на СИС чрез прилагане на подхода „отгоре-надолу“ с нов метод за анализ на проблемната област на този вид системи. Характерно за предложеният метод е, че е технологично независим /условие да послужи за основа за създаване на референтна методология за разработване на този вид системи/; гъвкав /позволява разширяване на съществуваща СИС с нова функционалност/; подпомага постигането на оперативна съвместимост на СИС със съществуваща информационна система на организация чрез използване на един и същи подход за моделиране на двете системи;
2. Предложено е детайлно описание на фундамента на областта на информационната сигурност, основаващо се на нейните основни понятия.

Глава 3 Проектиране на система за информационна сигурност в организации. Модел на анализа. Проектен модел.

В тази глава е описан метод за проектиране на система за информационна сигурност чрез създаване на Модел на анализа и Проектен модел. Концентрираме се в проектирането на СИС, предназначена за организации и насочена към защита от изтичане на чувствителна информация отвътре-навън от вътрешни лица с легитимен достъп до ресурсите на организацията и до нейните данни.

3.1 Системна рамка за описание на архитектурата на системи за информационна сигурност в организации

Разработването на СИС преминава през следните етапи (Фигура 5):

1. Уточняване на изискванията към СИС,
2. Системен анализ на изискванията и конструиране на модел на анализа съвпадащ с модел на проблемната област
3. Създаване на проектен модел на СИС,
4. Изграждане на модел на реализация.

В тази подточка е представен процеса на дефиниране на системна рамка за описание на архитектурата на СИС. Системната рамка за определяне на проблемната област на СИС и в последствие архитектурата на системата определя границите, в които тя се разработва системата. Референтната методология за разработване на СИС, предлагана от нас е основана на рамката за архитектурно описание на програмни системи, описана в стандартите IEEE 1471 и IEEE 42010. Архитектурното описание поставя началото на създаване на проектен модел на СИС. Той се използва при реализация на реална СИС, при проектирането на която се отчитат и унифицират изискванията на различните гледни точки в областта на интерес на СИС. Базовите концепции, залегнали в основата на рамката за анализ на областта на система за Информационна сигурност са представени в т.1.6 - Околна

среда, Заинтересована страна, Област на интерес, Изглед, Гледна точка, Архитектура на системата, Архитектурно описание, Рамка на създаване на архитектурно описание, Архитектурен изглед, Архитектурна гледна точка, Вид на модела са приложими при анализа на областта Информационна Сигурност. Те определят общата концептуална рамка, позволяваща многоаспектно описание на проблемната област и определяне на архитектурата на СИС чрез използване на възможностите на концептуалното моделиране [99, 100, 101].

3.1.1 Описание на подхода

Същността на нашия подход е първоначално създаване на обобщен модел, а след това на неговата основа и детайлен модел на проблемната област на СИС. Така ние се абстрахираме от излишните подробности и се фокусираме върху съществените характеристики на системата. Процесът на концептуално моделиране зависи от рамката, в която се формират основните понятия.

Част от изискванията към системата за информационна сигурност се формират от околната среда, определяща условията при които тя ще оперира. Тези изисквания се дефинират въз основа на предложеният от нас метод за анализ на Проблемната област и определят модел на анализа. Този анализ взима предвид гледните точки на всички заинтересовани участници в разработването на СИС, гарантирайки комплексност на подходите за ИС. Моделът на проблемната област съвпада с модела на анализа. Този модел представя желаната архитектура на системата. Трябва да се прави разлика между архитектура на системата и описание на архитектурата, т.е. архитектурен модел. Докато определянето на архитектурата на системата отразява модела на анализа, то архитектурният модел е част от проектния модел.

За целите на проектирането на базата на създаден концептуален модел се конструира описание на архитектурата и функционалността на СИС, които са компоненти на Проектния модел. Изграждането на Проектния модел се базира на използването на обектно-ориентиран подход и обектно-ориентиран език за описание Unified Modeling Language (UML), предоставящ инструменти за описание, анализиране, моделиране и документиране на архитектурата и функционалността на СИС [97, 98].

Проектният модел се състои от архитектурен модел и функционален модел, описвани със съответните диаграми в UML. При конструирането на този модел, концептуалният модел се трансформира в обектно-ориентиран проектен модел. Моделът на реализация може да се осъществи по два начина - чрез агентен подход, позволяващ симулация на реалната система, или чрез използването на конкретни съществуващи системи, представляващи среда за реализация на СИС. Такива са например системите за предотвратяване изтичане на данни СПИД като DeviceLock [95] и Cososys Endpoint Protector [96].

3.2 Модел на анализа

В тази точка е представено създаването на модела на анализа. Системата се проектира в дадена Проблемна област (ПО) в която се представят проблемите и задачите за реализиране от СИС. В резултат на анализ на ПО се достига до описание на проблемната област и създаване на Модел на проблемната област (МПО), което е по същество и модел на Анализа. Моделът на проблемната област и Моделът на анализа са еквивалентни. Този модел представя желаната архитектура на системата.

Към МПО на СИС се поставят следните изисквания:

1. В съответствие с начина на формиране на понятия концептуалното моделиране предопределя поне два етапа при създаване на модела на проблемната област: конструиране на обобщен модел и конструиране на детайлен модел;
2. Архитектурата на СИС трябва да съответства на описанието на Проблемната област, където са определени задачите, които трябва да изпълнява системата;

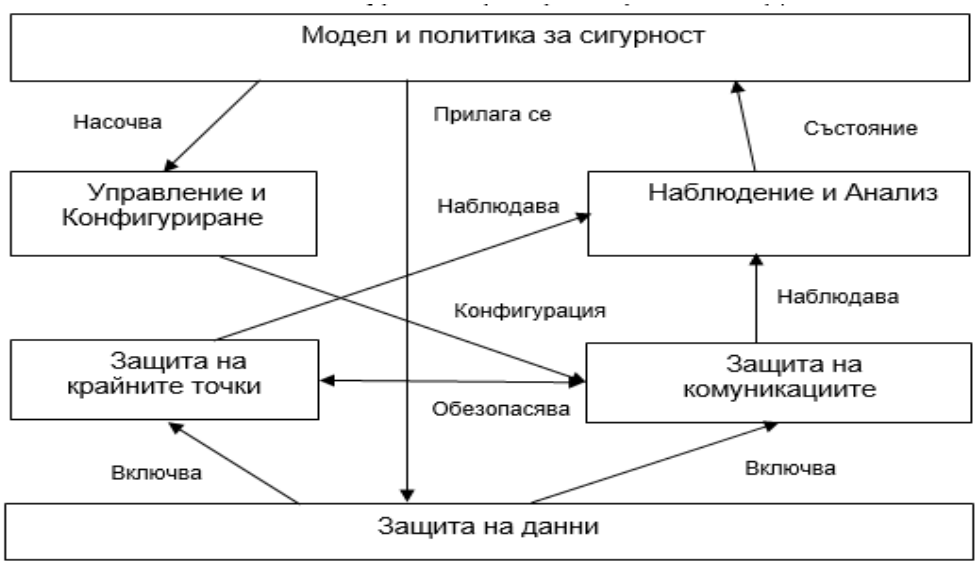
Резултатът от използване на концептуалното моделиране при създаване на Модел на анализа е концептуален модел, който представлява в своята същност абстракция, Всяка една концепция се разглежда като отделен компонент. Затова този модел представя и архитектурата на СИС.

3.2.1 Обобщен модел на проблемната област на СИС

В резултат на извършения анализ на проблемната област на СИС може да се обобщи, че най-важните въпроси, на които трябва да отговори една система от гледна точка на информационната сигурност са: „Какво защитаваме?“, „Защо защитаваме?“, „Как защитаваме?“ и „Къде защитаваме?“. Системната рамка за представяне на архитектурата на СИС е от съществено значение за разработването на системата, защото посочва основните компоненти, необходими за постигане на поставените и цели [20, 125].

Компонентите на обобщения модел съвпадат със задачите от ПО на проектираната система за информационна сигурност. Те отразяват съответните елементи от анализа на областта Информационна Сигурност. На тази база предлагаме мета-модел, представляващ обобщен модел на проблемната област на СИС. Моделът се състои от шест компонента, отговарящи на основните концепции, които представят областта ИС (Фигура 14) :

- “Защита на крайните точки” (Къде защитаваме?),
- “Защита на комуникациите” (Къде и Какво защитаваме?),
- “Защита на данни” (Какво защитаваме?),
- “Наблюдение и Анализ”,
- “Управление и Конфигуриране” (Как защитаваме?),
- “Модел и политика за сигурност” (Защо защитаваме?).

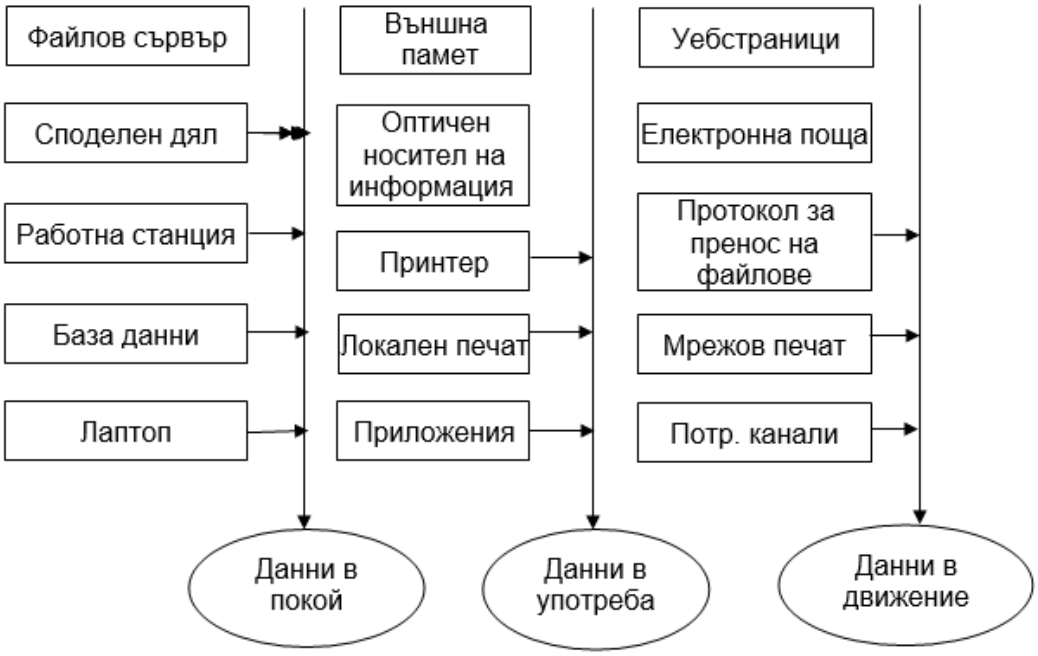


Фигура 14. Обобщен концептуален модел на проблемната област на СИС

Във всеки един момент данните могат да бъдат в едно от трите състояния: „Данни в покой“ (съхранен на запаметяващо устройство, архив или мрежов дял), „Данни в движение“ (данни участващи в комуникация, данни за състоянието на даден модул) или „Данни в употреба“ (всички данни използвани или обработвани в приложения) [23]. За формално представяне на данните в СИС създаваме мета-модел (Фигура 15), които се базира на гледната точка „Обработка на информация“ в областта на интерес на СИС (Фигура 8) [19]. За да се защитят различните типове данни е необходимо да се внедрят специфични подходи за информационна сигурност в основните блокове на мета-модела от гледна точка „Информационна сигурност“. Данните трябва да бъдат защитени срещу загуба, кражба, неоторизиран достъп и неконтролирани промени чрез прилагане на ПИС, като например: контрол на Поверителност, Цялостност, контрол на достъпа, изолация и репликация [17, 18].

С цел да се вземат предвид изискванията на всички заинтересовани страни, т.е. различните гледни точки, нашият подход позволява създаването на произволен брой концептуални мета-модели, които могат да бъдат комбинирани в една система. Резултата е многослоен концептуален мета-модел на СИС който съдържа мета-модели, представляващи съответните гледни точки.

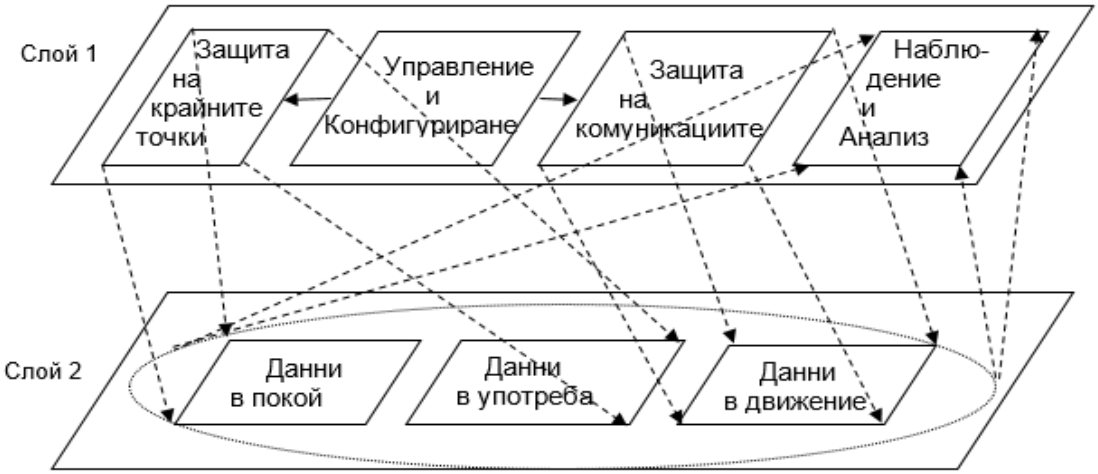
Показаният на Фигура 16 многослоен мета-модел представя гледните точки “Информационна сигурност” и “Обработка на информация” и взаимовръзките между тях. Като структура получения концептуален мета-модел съответства на Многослойния модел на защита от Фигура 4.



Фигура 15. Мета-модел “Обработка на информация”

Съвкупността от подходите за ИС, използвани в модела осигурява изпълнението на базовите принципи за информационна сигурност като „ПЦН Триада“, „Принцип на тройното А“ и „Принцип на най-слабото звено“. Основната цел е защита на данните в организацията. Поради сложността на защитата на всички възможни данни, ние се фокусираме в защита на чувствителните за организацията данни, които се дефинират в зависимост от околната среда в която се проектира системата. Отчитат се нормативни, законови, регулаторни и други изисквания и усилията се свеждат до защита на сравнително малки по обем, но критични за работата на организацията

данни. Отчитат се нормативни, законови, регулаторни и други изисквания и усилията се свеждат до защита на сравнително малки по обем, но критични за работата на организацията данни. Тези данни са дефинирани като чувствителни и целта на СИС е да бъдат защитени. Отделните компоненти на мета-модела изпълняват различни функционалности по защита.

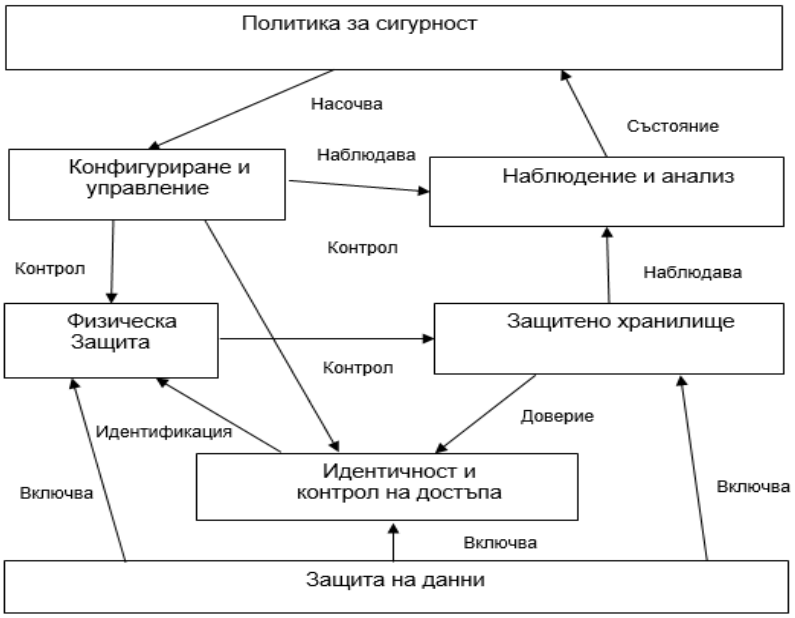


Фигура 16. Многослоен концептуален модел на СИС

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

3.2.2 Детайлно представяне на проблемната област

Тук е разгледано детайлното представяне на проблемната област**.** На основата на обобщения модел на СИС се създава детайлен модел на проблемната област на СИС. Разглеждаме детайлните концептуални модели на две от показаните концепции – *„Защита на крайните точки“* (Фигура 17) и *„Защита на комуникациите.* (Фигура 18).

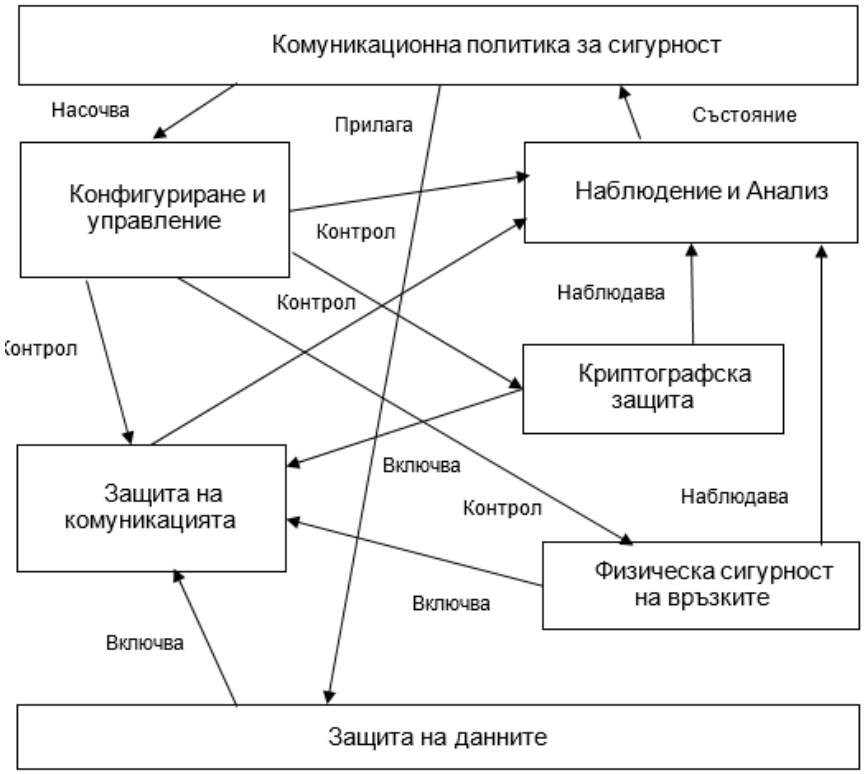


Фигура 17. Детайлен концептуален модел на концепцията „Защита на крайните точки“

Крайните точки са елементи на СИС, които имат изчислителни и комуникационни възможности: устройства, работни станции, сървъри, елементи на комуникационната инфраструктура, облачна инфраструктура и др. Те имат различни функции и изисквания за сигурност и тяхната защита може да бъде постигната със специфични подходи за информационна сигурност /ПИС/.

За да осигури Наличността, Поверителността и Цялостността на крайната точка, концепцията *„Защита на крайните точки“* трябва да осигури изпълнението на определени функционалности, които се осигуряват от компонентите показани на Фигура.17.

Концепцията *„Защита на комуникациите*“осигурява сигурност на свързаните крайни точки и комуникационните канали. На Фигура 18 е показан детайлен модел на концепцията.



Фигура 18. Детайлен концептуален модел на концепцията „*Защита на комуникациите*“

3.3. Проектен модел на системи за информационна сигурност. Архитектурен и функционален модел

Подход за създаване на проектен модел

На базата на архитектурното описание на системата за информационна сигурност може да бъде създаден проектен модел на системата. Той дава възможност за реализация на реална СИС, като при нейното проектиране се взимат предвид и се обобщават изискванията на различните гледни точки в областта на интерес на СИС. Подходът на проектиране на СИС е базиран на трансформация „модел-към-модел“. В нашият случай осъществяваме трансформацията:

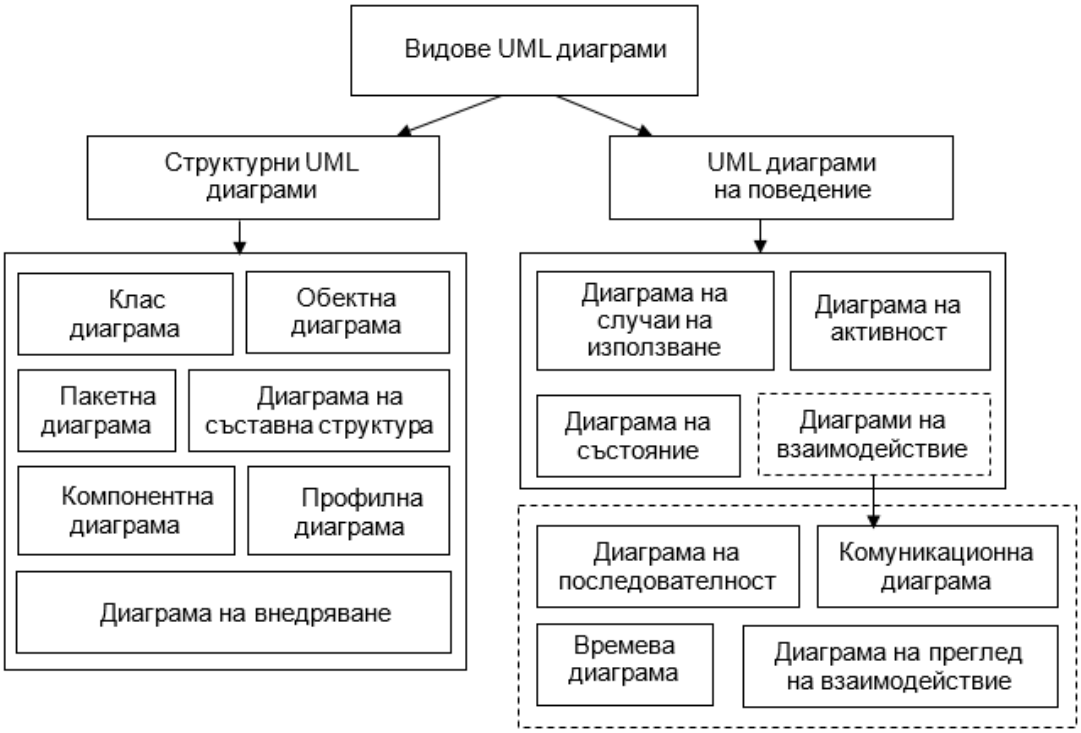
концептуален модел → обектно-ориентиран (ОО) модел

Най-подходящият начин за описание на ОО моделите е използването на обектно-ориентиран инструмент за описание, какъвто е обектно-ориентирания език UML. Този език 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 разработването на системата. UML осигурява стандартна нотация за анализ, проектиране и внедряване на системи.

3.3.1 Обектно-ориентиран подход чрез използване на обектно-ориентиран език UML

В тази подточка са описани общата функционалност и възможности на езика за описание UML, както и основните видове диаграми (Фигура 20). Чрез различните UML диаграми, може да бъдат представени различни изгледи на системния модел.



Фигура 20. Видове UML диаграми

Чрез структурните диаграми (Structural Diagrams), може да бъде представена статичната структура на системата. Те 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).

Чрез „*Диаграмите за поведение*“ *(Behaviour Diagrams),* могат да се представят взаимодействието и моментните състояния на компонентите в модела, както и да се покаже как те се изменят с течение на времето. Чрез тези диаграми може да се проследи как системата действа в реална среда и да се наблюдава ефекта от дадени операции или събития. Този вид диаграми включват „Диаграми на употреба“ (UseCase Diagrams), „Диаграми на активност“ (Activity Diagrams), „Диаграма на състояние“ (State chart Diagram).

Последният тип UML диаграми са „Диаграмите за взаимодействие“ (Interaction Diagrams). Те са подклас на „Диаграмите за поведение“ и се използват за описание на взаимодействията между различните елементи в модела. Това взаимодействие е част от динамичното поведение на системата. Такива диаграми са: „Диаграма на

последователност“ (Sequence Diagram), „Диаграма за Сътрудничество“ (Collaboration Diagram), „Комуникационна диаграма“ (Communication Diagram), „Времева диаграма“ (Timing Diagram), „Диаграма за преглед на взаимодействие“ (Interaction Overview Diagram).

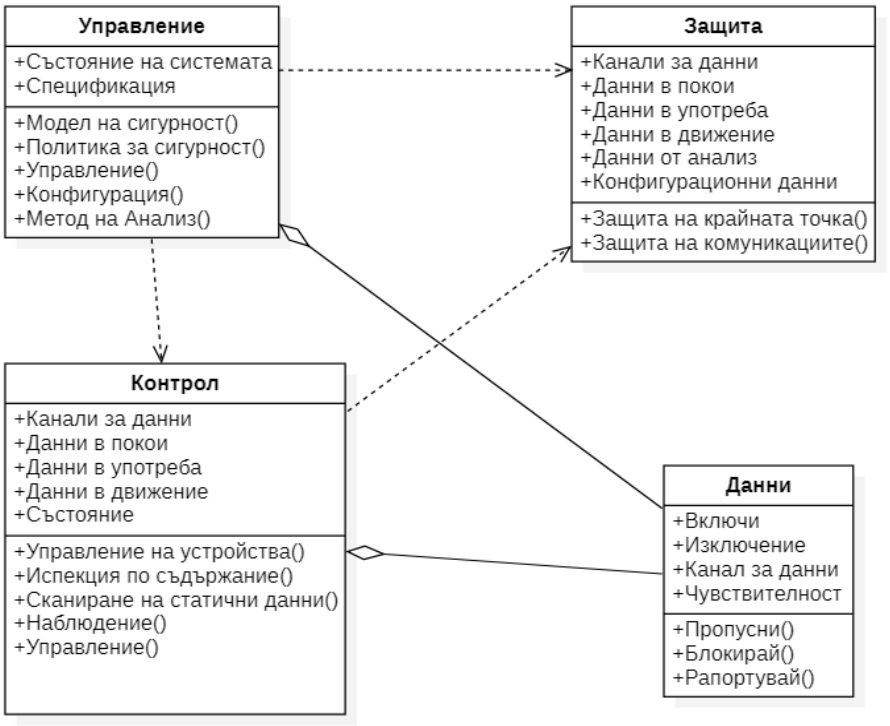
3.3.2 Архитектурен модел на системи за информационна сигурност

Архитектурният модел на СИС се представя чрез статични UML диаграми. За да се отрази трансформацията на обобщения модел на проблемната област на СИС от Фигура 14 в ОО модел използваме „Клас-диаграма“. За представяне на обектно-ориентираните модели на детайлните модели на концепциите „Защита на крайните точки“ (Фигура 17) и „Защита на комуникациите“ (Фигура 18) използваме „Диаграми на съставна структура“. По-детайлното описание н архитектурата на проектния модел изисква използването и на „Обектна диаграма“ и „Профилна диаграма“ което в момента не е задача на дисертационния труд.

На базата на останалите статични диаграми – „Пакетна диаграма“, „Компонентна диаграма“ и „Диаграма на внедряване“ се изгражда Модела на реализация.

UML „Клас-диаграма“

Целта на „Клас-диаграмата“ е да покаже статичната структура на класификаторите в системата. Диаграмата осигурява основна нотация, която може да се използва от други UML диаграми. Клас-диаграмата се състои от набор класове и връзки между класовете [97]. Концепцията на СИС, представена чрез обобщения мета-модел (Фигура 14) може да бъде описана чрез „Клас-диаграма“, както е показано на Фигура 21. Използваме същите понятия като в мета-модела, разделени като методи на четирите основни класа.



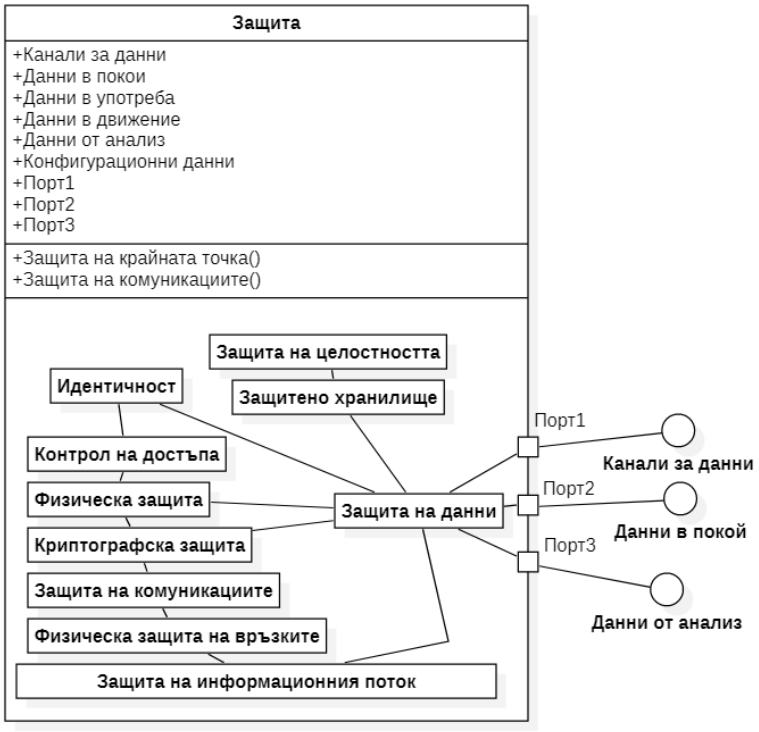
Фигура 21. UML „Клас диаграма“ на СИС

На компонентите „Защита на крайните точки” и “Защита на комуникациите” отговарят методите “Защита на крайната точка” и „Защита на комуникациите” в класа „Защита“, компонента „Защита на данни” е представен с еквивалентните методи „Пропусни”, „Блокирай” и „Рапортувай” в класа „Данни“. Клас „Контрол“ е агрегация от

компонентите „Защита на крайните точки”, “Защита на комуникациите”,„Защита на данни” и „Управление и Конфигуриране“.

UML „Диаграма на съставна структура“ на клас “Защита”

Чрез този вид диаграма се представя вътрешната структура на съответния клас. Класът „Защита“ включва методите “Защита на крайната точка” и “Защита на комуникациите”, осъществяващи защитата на данни както в крайните точки, така и в процеса на комуникация. Структурата на класа, изразена чрез диаграма на съставна структура е показана на Фигура 22.



Фигура 22. UML „Диаграма на съставна структура” на клас “Защита“.

3.3.3 Функционален модел на системи за информационна сигурност

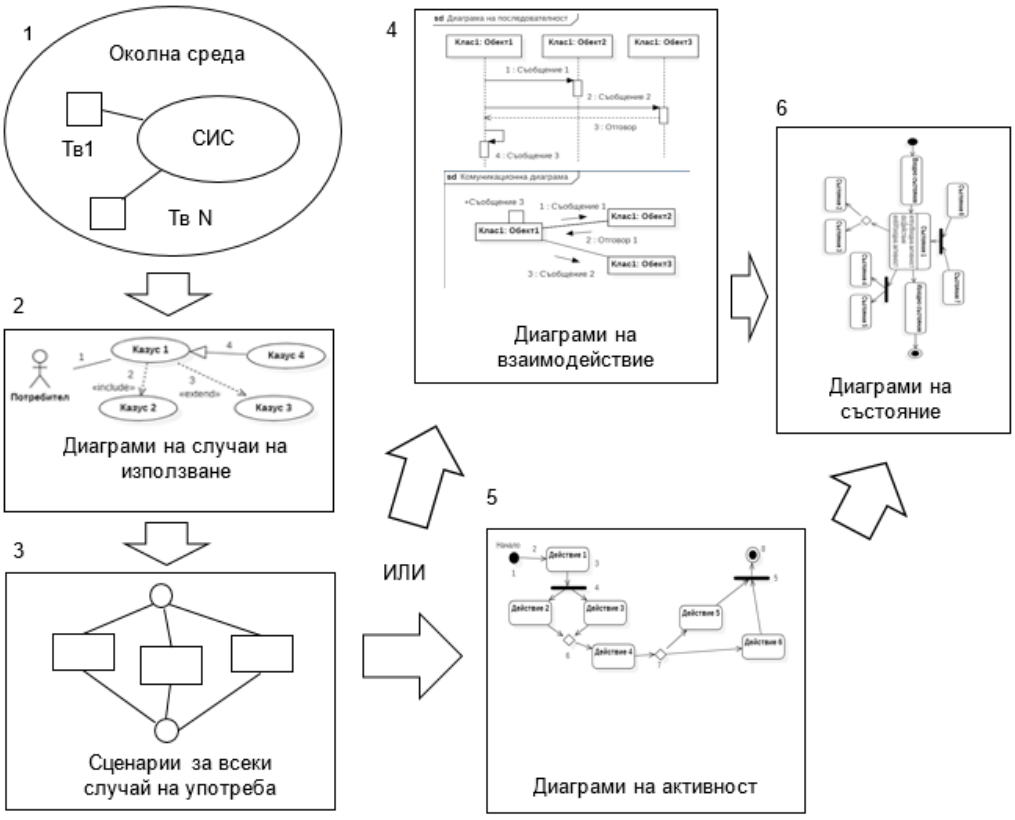
Функционалният модел на СИС може се представи чрез динамични UML диаграми: Диаграми на поведение и Диаграми на взаимодействие. Чрез тях може да се опишат различни аспекти от динамичното поведение на системата и взаимодействието на различните елементи на системата един с друг или с външни субекти. Те са удобни за описание на резултатите от динамичния анализ на системата за информационна сигурност (Фигура 23). Целта на анализа е да се идентифицират възможните варианти на взаимодействие, те да бъдат описани формално и да бъдат заложени в проектираната система, така че тя да реагира на взаимодействието според заложените при нейното проектиране цели.

СИС функционира в определена Околна среда (1). Освен че тя предоставя условията за функциониране на системата, в нея се извършва и взаимодействието (интеракцията) на СИС с различни субекти – точки на взаимодействие (Тв1 .. ТвN) от Фигура 23. Тези външни за системата субекти взаимодействат с нея по различни начини, извличайки полза от СИС. Начините на взаимодействие могат да бъдат описани с набор от диаграми на случаи на използване (2). Тези диаграми стоят в основата на динамичния анализ и съответно на функционалния модел на СИС.

За всяко взаимодействие на СИС със външен субект/обект може да бъде

съставена както базова диаграма на случаи на използване, описваща основното взаимодействие и поведение, така и разширени диаграми на случаи на използване, свързани с базовата диаграма и разширяващи базовата. Допълнителните диаграми наследяват базовите диаграми и добавят нови аспекти към основното взаимодействие. Така се формира набор от диаграми на случаи на използване, свързани с един или повече субекти и описващи възможно най-пълно взаимодействието на системата с тях. За всеки случай на използване се описват съответните сценарии (3), описващи взаимодействието и очакваната реакция на системата. Всеки сценарии може да бъде анализиран чрез използването на UML диаграми на поведение. Те могат да бъдат диаграми на взаимодействие (4) (Диаграма на последователност, Комуникационна диаграма, Времева диаграма, Диаграма на преглед на взаимодействие) или Диаграми на активност (5). Изборът на (4) или (5) зависи от спецификата на системата и на околната среда, така че най-пълно да бъде описано нейното поведение. Следващата стъпка е описание чрез диаграми на състояние (6), чрез които описваме промяната на състоянието на основните елементи на СИС, обобщавайки динамичното и поведение.

Полученият набор от UML диаграми, описващи резултата от динамичния анализ на системата формира Функционалния модел на проектираната система. Всяка диаграма описва отделни функционалности на системата, показвайки че подхода е приложим.



Фигура 23. Подход за създаване на функционален модел чрез динамични UML диаграми

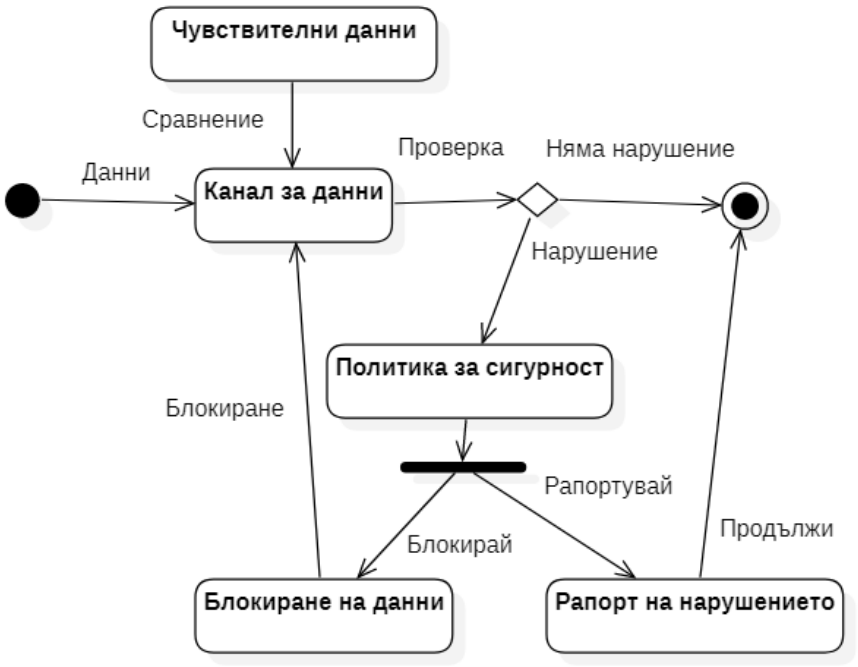
В настоящата подточка е показано как чрез различните динамични диаграми може да се опишат различни сценарии на взаимодействие на СИС с външни за нея субекти. Така например с „Диаграма на случай на използване“ удобно могат да бъдат описани разлчни начини на комуникация, например изпращане на електронна поща

до външен за организацията получател.

Следващите UML диаграми, формиращи функционалния модел са диаграми на взаимодействие, описващи взаимодействието на класовете „Управление“, „Контрол“ и „Данни“ и класовете „Управление“, „Контрол“ и „Защита“. Класовете са част от Клас-диаграмата от архитектурния модел на СИС (Фигура 21). Чрез този вид диаграми лесно се отразяват специфични взаимодействия на отделните класове, например инспекцията на потока от информация, преминаващ през даден комуникационен канал за съдържание на чувствителни за организацията данни или проверка на спазването на политиката за сигурност от отделните потребители.

Чрез „Диаграми на последователност“ се визуализира времевата последователност на взаимодействията между елементите на системата, осъществени чрез съобщения между тях.

Освен с диаграмите на взаимодействие, динамичното поведение на системата, представено със сценариите и случаите на използване могат да се анализират чрез диаграми на активност. На Фигура 28 е представена диаграма на активност на един от методите на клас „Защита“ – “Защита на крайна точка”, показваща проверка дали информацията, преминаваща през даден канал за данни е чувствителна според критериите на организацията. Подобни диаграми на активността могат да се създадат за всички методи от клас-диаграмата. По този начин е възможно да се опишат подробно различни случаи за взаимодействие със системата.



Фигура 28. UML Диаграма на активност на метода “Защита на крайна точка”

3.4 Заключение

В трета глава е представен подход за проектиране на Системата за Информационна Сигурност, предназначена за организации и насочена към защита от изтичане на чувствителна информация отвътре-навън, т.е. в резултат от действие на вътрешни лица с легитимен достъп до ресурсите на организацията и до нейните данни. За определянето на архитектурата на системата се използва представената в глава 2 системна рамка, която ни помага да се уточни проблемната област на СИС и да се извърши съответния анализ.

Представен е модел на анализа, който съвпада с модела на проблемната област. Изграждането на модела се основава на възможностите на концептуалното моделиране. В резултат е създаден обобщен концептуален модел на проблемната област на СИС. Показано е как обобщеният модел може да се трансформира в многослоен, когато се вземе под внимание анализа на повече от една гледни точки спрямо проблемната област на системата. Представеният многослоен мета модел отразява гледните точки „Информационна Сигурност“ и „Обработка на информацията“. На основата на обобщения концептуален модел се конструира детайлен концептуален модел на отделните негови компоненти. Показани са детайлни описания на концепциите „Защита на крайните точки“ и „Защита на комуникациите“.

Процесът на създаване на проектен модел на СИС е базиран на осъществяване на трансформацията „от модел към модел“. В случая се използва концептуалния модел на проблемната област на системата за създаване на обектно-ориентиран /ОО/ проектен модел. За целта се използва обектно-ориентиран инструмент за описание на модели – формалния език UML. Този език осигурява стандартна нотация за проектиране и внедряване на системи. Показано е, че той позволява на системните разработчици да представят изискванията към СИС и нейните компоненти в проектен модел на системата, който се състои от архитектурен модел и функционален модел. Представено е как могат да се моделират отделни аспекти на архитектурния модел, основани на съответните концептуални модели чрез използване на следните UML диаграми: „Клас-диаграма“ и „Диаграма на съставна структура“. Чрез моделиране на отделни аспекти на функционалния модел е показано как може да се състави обектно-ориентиран функционален модел, базиран на създадените концептуални модели на проблемната област. За целта се използват следните UML диаграми: „Диаграма на активност“, „Диаграма на състоянието“, „Диаграми на преглед на взаимодействие“, „Диаграма на случай на употреба“ , „Диаграма на последователност“.

Чрез приложения метод за анализ на проблемната област, възможностите за концептуално моделиране и подхода за осъществяване на трансформацията „от модел към модел”, разгледани в Глава 3 успешно се изпълняват задачи 3 и 4, дефинирани в "Цел и задачи на дисертацията":

- Описание на проблемната област на Системите за Информационна Сигурност в организации чрез концептуално моделиране;
- Анализ и приложение на обектно-ориентиран подход при създаване на проектен модел на система за информационна сигурност на базата на създаден концептуален модел.

В резултат на научноизследователската дейност за създаване на методология за разработване на СИС чрез модел на анализа и проектен модел се постигат следните научни и научно-приложни приноси:

1. Разработен е многослоен концептуален модел на проблемната област на системите за информационна сигурност като резултат от прилагането на две и повече от две гледни точки при нейното описание;

2. Конструирани са архитектурен и функционален модели на системите за информационна сигурност на базата на съществуващ концептуален модел на проблемното пространство с помощта на обектно-ориентирания унифициран език за описание на програмни системи UML;

Глава 4. Подходи за създаване на модел на реализация на системи

за информационна сигурност в организации

Съгласно възприетата методология за разработване на СИС, на базата на проектния модел трябва да се създаде модел на реализация, които може да се използва за две цели:

- Създаване на модел на реализация, съобразен със съществуваща среда за реализация;
- Симулиране работата на проектираната СИС;

За постигането на първата цел, като част от предложеният от нас метод, се извършва анализ на проблемната област и на базата на изградения концептуален модел, резултат от този анализ се избира платформа за реализация. Целта е да се запази подхода на обектно-ориентираното моделиране. В резултат трябва се създаде обектно-ориентиран модел на реализация, които съответства на разработения ОО проектен модел.

За постигането на втората цел се използват средите за симулиране NetLogo (v.6.0.4), и I-SCIP-SA, работещи на базата на създаване на агентно или мулти-агентно ориентирани модели. Това изисква обектно-ориентирания проектен модел, описан със средствата на UML да бъде трансформиран съгласно изискванията на агентния подход.

4.1 Сравнителен анализ на съществуващи платформи СПИД на базата на модел на анализа

Политиката за информационна сигурност касае по различен начин отделните работни места в организацията. Служителите на различни позиции (работни места) използват различни данни и имат съответния регламентиран достъп до тях. Това се описва в приетата в организацията политика за информационна сигурност, на базата на длъжностната им характеристика. В политиката за ИС се описва и какви операции с тези данни са разрешени и какви не са за даденото работно място. Изрично е описан достъпът до чувствителни за организацията данни за съответните позиции.

Основната цел на СПИД е опазването на данни от изтичане извън организацията. СПИД представят гъвкава платформа за реализация на приетата политика за информационна сигурност по отношение на защита на данните. Те предлагат подходящи инструменти за описание, изпълнение и контрол на:

- Различни типове данни,
- Дефиниране и работа с чувствителни за организацията данни,
- Разрешени и забранени операции с различни типове данни от съответните работни места,
- Описание на различни сценарии за работа с данните,
- Описание на регулации за работа с данни и тяхното спазване и контрол.
- Анализ на спазването на политиката за сигурност в организацията.

СПИД имат възможност за адаптиране към различните работни места според изискванията на политиката за информационна сигурност.

4.1.1 Приложения на предложеният от нас метод за уточняване на архитектурата на СИС

Проектираната от нас СИС е предназначена за организации и насочена към защита от изтичане на чувствителна информация в посока отвътре-навън от вътрешни лица с легитимен достъп до данни и ресурси на организацията. Архитектурата на системата се уточнява от различните гледни точки на отделните

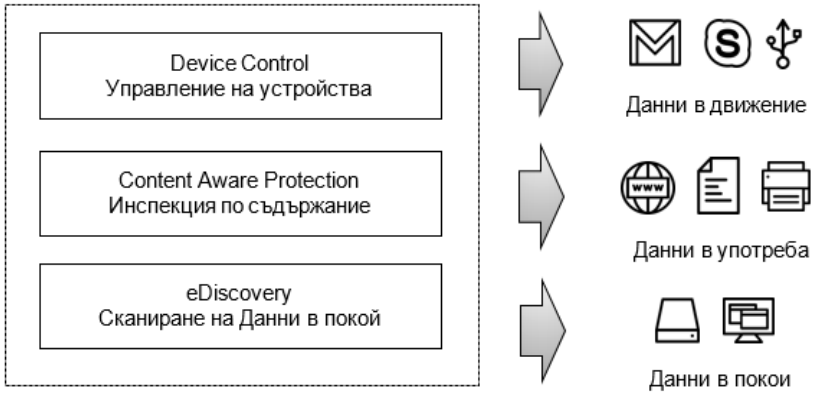
участници в процеса на проектиране и реализация на СИС. Базово изискване към системата е да притежава подходяща архитектура, която да се адаптира към различни политики за информационна сигурност, които поставят съответни изисквания към различни потребители на информация в дадена организация.

Това изискване се удовлетворява напълно от предложения от нас нов метод за уточняване на изискванията към архитектурата на СИС.

На базата на анализ на проблемната област от различни гледни точки и нейното последващо концептуално моделиране (Фиг.8), се конкретизират изискванията към разработваната СИС. Това дава възможност за избор на подходяща платформа за нейната реализация. Първата гледна точка, която се взима в предвид е гледната точка „Обработка на информация“. Тя отразява различните видове данни – данни в покой, данни в употреба и данни в движение. Друга гледна точка е „Технологична гледна точка“, отразяваща способите за защита на данните и съдържаща поддържаните платформи и технологии. Тя е от голямо значение за осигуряване на оперативна съвместимост на СИС, която се изгрзжда като допълнение към вече съществуваща СИС. За избора на платформа за реализация се използва и гледна точка „Информационна сигурност“, отразяваща изискванията на организацията към защитата на данните. Те са описани в политиката за Информационна сигурност. На базата на трите гледни точки и сходните цели на проектираната от нас СИС и системите за предотвратяване изтичането на данни, се избира платформа за реализация от тип СПИД. Използвайки концептуалният мета-модел от Фиг.15, изграден от гледната точка „Обработка на информация“ се извършва анализ на водещи СПИД (Cososys Endpoint Protector 5.0.2.1 [96], Symantec Data Loss Prevention 14.6 [137], McAfee DLP Endpoint 9.3.200 [138], Forcepoint DLP 8.9 [139], DeviceLock 8.2 [95]) и как те изпълняват изискванията на проблемната област.

Като резултат от анализа е избрана най-подходящата за нашите цели конкретна платформа за реализация. СПИД избрана за реализация на СИС е част от нейната архитектура. В нашия случаи, на базата на анализа изборът ни пада върху СПИД Cososys Endpoint Protector 5.0.2.1 [96]. Освен предимствата по отношение на защитата на основните типове данни (данни в покой, данни в употреба и данни в движение), друго сериозно предимство е осигуряването на оперативна съвместимост с останалите средства и подходи за информационна сигурност в организацията. Допълнително предимство на избраната платформа е нейната цена. При реализацията на СИС, задачата на избраната СПИД е единствено осигуряване на защита на данните на организацията в посока отвътре-навън, без да пречи на останалите средства за защита.

4.2 Платформа за реализация СПИД Cososys Endpoint Protector 5.0.2.1



Фигура 31. СПИД „Cososys EndPoint Protector 5.0.2.1“ – Структура

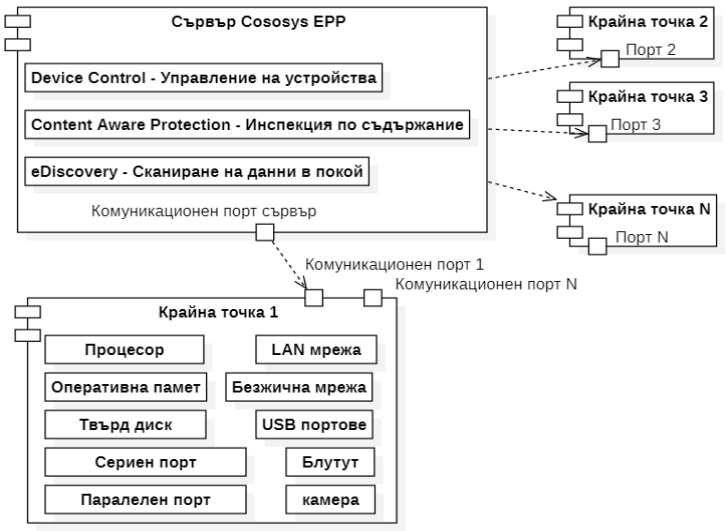
Освен агентно-ориентирани модели с цел симулация, модела на реализация може да бъде създаден чрез използването на съществуващата среда за реализация. За постигането на тази цел избираме съществуваща платформа за изграждане на СПИД Cososys EPP 5.0.2.1 [96]. За създаването на модела е използван подхода на обектно-ориентираното моделиране. В резултат е създаден обектно-ориентиран модел на реализация, които да съответства на разработения ОО проектен модел. Избраната платформа за реализация Cososys EPP 5.0.2.1, се състои от хардуерен сървър и софтуерни модули Device Control, Content Aware Protection и eDiscovery. Хардуерния сървър осигурява централизираното управление на СПИД, а отделните модули осуряват различна функционалност (Фигура 31).

4.3 Обектно-ориентиран модел на реализация на системи за информационна сигурност

За създаването на ОО модел на реализация отново използваме нструментариума на езика UML. Чрез него създаваме следните диаграми:

- Пакетна диаграма,
- Компонентна диаграма,
- Диаграма на внедряване.

Фигура 32. UML Пакетна диаграма на СПИД Cososys EPP 5.0.2.1

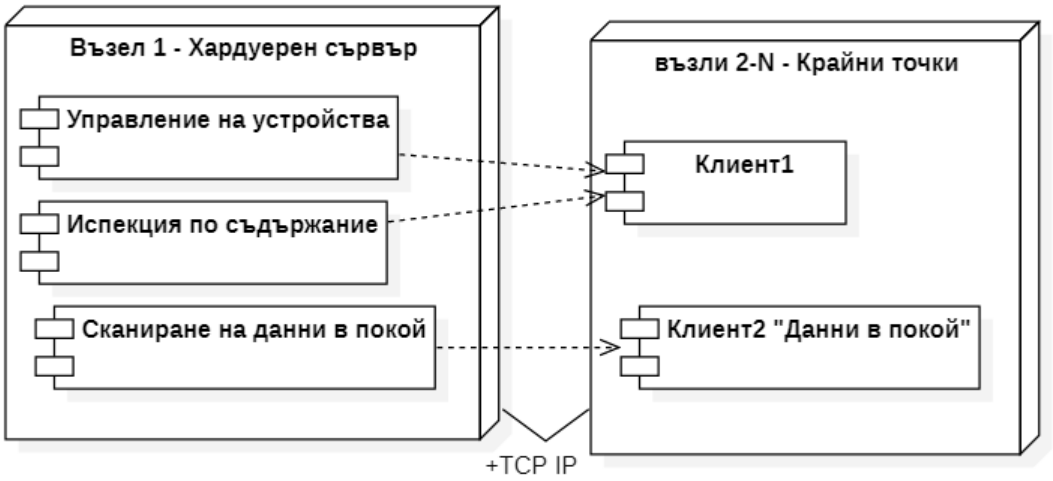


Фигура 33. UML Компонентна диаграма на Cososys EPP 5.0.2.1

Пакетната диаграма от модела на реализация (Фигура 32) е съставена от следните основни пакети: “Device Control – Управление на устройства“, „Content Aware Protection – Инспекция по съдържание“, „eDiscovery – Сканиране на Данни в покой“ и „Доклади и анализи“, отговарящи на основните модули на СПИД Cososys EPP 5.0.2.1.

СПИД Cososys EPP 5.0.2.1 е изградена на базата на „клиент-сървър“ архитектура. Контролираните от системата работни станции се наричат „Крайни точки“. На всяка крайна точка се инсталира клиент, наречен „агент“, които контролира съответните канали за данни като Lan мрежа, безжична мрежа, USB портове, Блутут портове, серийни и паралелни портове (Фигура 33). СПИД контролира и достъпа на всички устройства, използващи каналите и портовете за данни – USB запаметяващи устройства, принтери, камери и т.н. Системата комуникира с крайната точка като и налага за изпълнение приетата политика за сигурност, указваща КОИ може да използва каналите за данни и устройствата, КОГА да ги използва, КАК да ги използва (чрез какви протоколи и приложения), КАКВИ данни може да използва и изпраща.

Чрез диаграмата на внедряване 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. Примерна диаграма на внедряване на СПИД система е показана на Фигура 34. Поради факта че СИС обикновена е сложна система, съставена от голям брой компоненти, диаграмата е опростена и показва няколко хардуерни компоненти като СПИД (DLP) сървър, който е свързан със софтуерните агенти, работещи на потребителските работни станции. Чрез софтуерните агенти, СПИД сървъра наблюдава, контролира и управлява каналите за данни на крайните точки (работни станции и лаптопи) – LAN мрежа, безжична мрежа, Блутут, USB портове, електронна поща, чат комуникации и др. СПИД е в състояние да контролира комуникационните канали, да активира и деактивира потока от данни през тях според контекста и потребителя. Данните могат да бъдат инспектирани по съдържание, като при констатиране на нарушение – неоторизирано изтичане на данни, то може да бъде блокирано и докладвано. Комуникацията между клиентите и сървъра се осъществява чрез TCP/IP протокол.



Фигура 34. UML Диаграма на внедряване на СПИД

4.4. Разширяване на съществуваща СИС с нови случаи на използване за защита на чувствителни данни за организацията

При реализацията на политики за информационна сигурност в организацията, главно внимание се обръща на различните позиции (работни места). Длъжностната характеристика на работното място определя използването на информационната система. Начините на използване на ИС от служителите на организацията дефинират съвкупност от случаи на употреба (use cases). Случаите на употреба, свързани с използване, обработка или комуникация на данни, обект на защита в организацията могат да бъдат описани в СИС, която да следи как съответния служител спазва политиката за сигурност.

Изборът на СПИД като платформа за реализация на СИС дава възможност за гъвкава настройка на системата със съответните изисквания към работните места - с каква информация е допустимо да работи и какви операции са разрешени.

Реализацията на СИС се описва чрез модела на реализация. Той се конструира чрез обектно-ориентирано моделиране от обектно-ориентиран проектен модел на СИС. За целта се използват UML диаграми според представеният от нас метод. Чрез тях се описват конкретни случаи на използване (use cases) чрез които могат да бъдат постигнати и удовлетворени поставените пред СИС цели. Използвайки случаите на използване не е необходимо да се реализира реална, пълномащабна СИС. Достатъчно е описаните случаи да покриват поставените цели за различните работни места в организацията. Чрез сценариите, описани в случаите на използване се осигурява възможност на СИС да се адаптира към нови изисквания на организацията и съответните работни места. Наборът от описани случаи на използване, описващ различни сценарии на взаимодействие на СИС с околната среда и потребителите (Фиг.23) дават възможност на системата да удовлетвори изискванията на различни по своя характер, дейност и големина организации.

Представеният метод, съчетан с използването на гъвкава платформа за реализация като СПИД осигурява възможност за доразвиване на съществуващи СИС чрез нови сценарии за защита на данни, нереализирани досега в организацията. Метода дава възможност за моделиране и реализация на нови аспекти от СИС без да се налага системата да се проектира отначало. Друго основно предимства на метода и използването на СПИД е запазването на оперативната съвместимост с останалите елементи на съществуващата СИС или на отделни подходи и механизами за информационна сигурност, реализирани вече в

организацията.

Такъв е случаят с организация, притежаваща функционираща СИС и предпазваща ефективно нейната инфраструктура чрез различни подходи за информационна сигурност (ПИС) с мрежова комуникация – Фиг.3. След влизането в сила на Общия регламент относно защита на личните данни - Регламент (ЕС) 2016/679 (GDPR), регламентиращ защитата на личните данни на граждани на Европейския Съюз, се налага организацията да се съобрази с него и да въведе мерки за защита на личните данни на клиенти и служители.

За целта са наложителни следните промени в политиката за информационна сигурност

1. Спазване на изискванията на GDPR за опазване на лични данни,
2. Опазване на информацията от изнасяне в посока отвътре-навън.

Тяхната реализация се базира на определянето и опазването на чувствителната за организацията информация. Описват се необходимите сценарии за защита на лични и/или чувствителни данни и се съставят необходимите за изпълнението на сценариите динамични UML диаграми, свързани с описанието на динамичното поведение на системата (Фигура 23). Няколко такива сценария са показани в Таблица 2. След това така описаните сценарии се добавят към съществуващата СИС, чрез избраната СПИД за реализация на защитата в реални условия, съобразявайки се с отделните работни места и спецификата на работата им с данни.

Сценарий 1	
Ключови контроли	Контрол на лични/чувствителни данни чрез политики и правила за IBAN, ЕГН, ID, Credit Card Numbers.
Описание	Контрол на трансфера на лични/чувствителни данни, съдържащи IBAN, ID, Credit Card Numbers чрез външни запаметяващи устройства (USB флаш памети).
Сценарий	Копиране на данни върху външно запаметяващо устройство (USB флаш памет). СИС проверява дали копираните файлове съдържат чувствителни за организацията данни. Ако данните са чувствителни, политиката за сигурност определя дали потребителя има право да копира файловете, съдържащи тези данни. Проверява се дали според политиката за сигурност потребителя има право да използва този външен носител. Например в организацията може да е регламентирано използването само на служебни оторизирани флаш памети или само на криптирани USB носители. В този случаи се дефинира „бял списък“ от разрешени за използване преносими Flash памети. За всеки потребител се определя персонална Flash памет която може да бъде използвана само от него. При нарушаване на политиката за сигурност копирането на файла се забранява и се изготвя доклад за нарушението. Възможно е да се създаде резервно копие на файла (документа) за по-нататъшно разследване.
Проектни модели описващи Сценарий 1	Виж Приложение 1 1. Диаграма на случай на използване (Use Case Diagram) – Фигура 1.1

(UML диаграми)	2. Диаграма на взаимодействие или Диаграма на активност – Фигура 1.2 3. Диаграми на състояние – Фигура 1.3.1 и 1.3.2
Сценарий 2	
Ключови контроли	Принудително криптиране на данни, пренасяни чрез USB флаш памети.
Описание	Криптиране на лични/чувствителни данни, съдържащи IBAN, ID, Credit Card Numbers при пренасяне на данни чрез външни запаметяващи устройства (USB флаш памети).
Сценарий	При копиране на файлове върху външно запаметяващо устройство (USB флаш памет).се проверява дали политиката за сигурност разрешава тази операция от този потребител, с тези данни. След това се проверява дали външното запаметяващо устройство е хардуерно криптирано. Ако то е хардуерно криптирано, операцията се разрешава и се прави резервно копие, ако политиката за сигурност го изисква. Ако устройството не е хардуерно криптирано се активира вграденият в СПИД модул за софтуерно криптиране и файловете се криптират принудително. След това операцията за копиране се разрешава, като се копира криптиран файл. Чрез този сценарии се гарантира че при загуба или кражба на външното запаметяващо устройство (USB флаш памет) GDPR е спазен.
Проектни модели описващи Сценарий 2 (UML диаграми)	Виж Приложение 1 1. Диаграма на случай на използване (Use Case Diagram) – Фигура 2.1 2. Диаграма на взаимодействие или Диаграма на активност – Фигура 2.2 3. Диаграми на състояние – Фигура 2.3
Сценарий 3	
Ключови контроли	Контрол на лични/чувствителни данни чрез политики и правила за IBAN, ЕГН, ID, Credit Card Numbers.
Описание	Контрол на трансфера на лични и чувствителни данни, съдържащи IBAN, ID, Credit Card Numbers чрез електронна поща (email).
Сценарий	Изпращане на данни чрез електронна поща (email). СИС проверява дали изпращаната електронна поща съдържа чувствителни за организацията данни. Ако данните са чувствителни, политиката за сигурност определя дали потребителя има право да изпраща пощата, съдържаща тези данни. Проверява се дали според политиката за сигурност потребителя има право да изпраща електронна поща до адресата. Например в организацията може да е регламентирано изпращането на електронна поща до оп-

	ределени адреси от определени потребители. В този случаи се дефинира „бял списък“ от разрешени адреси на електронна поща. При нарушаване на политиката за сигурност изпращането на електронното писмо се забранява и се изготвя доклад за нарушението. Възможно е да се създаде резервно копие на файла (документа) за по-нататъшно разследване.
Проектни модели описващи Сценарий 3 (UML диаграми)	Виж Приложение 1 1. Диаграма на случай на използване (Use Case Diagram) – Фигура 3.1 2. Диаграма на взаимодействие или Диаграма на активност – Фигура 3.2 3. Диаграми на състояние – Фигура 3.3

Таблица 2. Сценарии на нови случаи на употреба на съществуваща СИС

4.4.1 Резултати от проведени изпитания на реализирано разширяване на съществуваща СИС с нови случаи на използване за защита на чувствителни данни

Цел на изпитанията

Изпитание на предложените сценарии за разширяване възможностите на съществуваща СИС за предотвратяване изтичане на информация в държавни и частни структури.

Обхват на проучването

До момента проучването обхваща 7 организации – 5 държавни и 2 частни.
Размер на субектите: Мащабни добре структурирани държавни и частни субекти.

Методология

Проведени са срещи с представители на проявили интерес държавни и частни субекти, на които е обсъдена нуждата от разширяване възможностите на системите за информационна сигурност. Дискутирани са различни инструменти за защита на чувствителна информация, в зависимост от спецификата на дейността, нормативните изисквания и размера на субекта. След проведените срещи се стига до извода, че най-голяма е нуждата от внедряването на решения от типа СПИД.

В два от субектите са направени подробни тестове и Доказване на концепцията (POC - Proof Of Concept) на решения от тип СПИД. За провеждане на тестовете и POC са съгласувани и одобрени тестови сценарии, представени със случаи на използване (use cases) за защита на чувствителна информация, съответстваща на нормативните уредби и вътрешни правила на субекта. Наблюдавани са и съвместимостта с наличните към момента инструменти и решения за ИТ сигурност, използвани в организациите.

Нормативна база

Закон за киберсигурност в Р.България [57, 74], Наредба за минималните изисквания за мрежова и информационна сигурност [15], EU GDPR [68], ISO 27001 и 27002 [8, 78, 79] и други спицифични наредби за субектите.

Описание на проведените изпитания

За осъществяване на специфичните за средата тестове, одобрените правила и сценарии са основани на извадки от ключови контроли, използващи функционалността на приложеното решение от тип СПИД.

Резултати и заключения от изпитанията

Използвайки предложеният от нас метод за проектиране на СИС, се разширяват

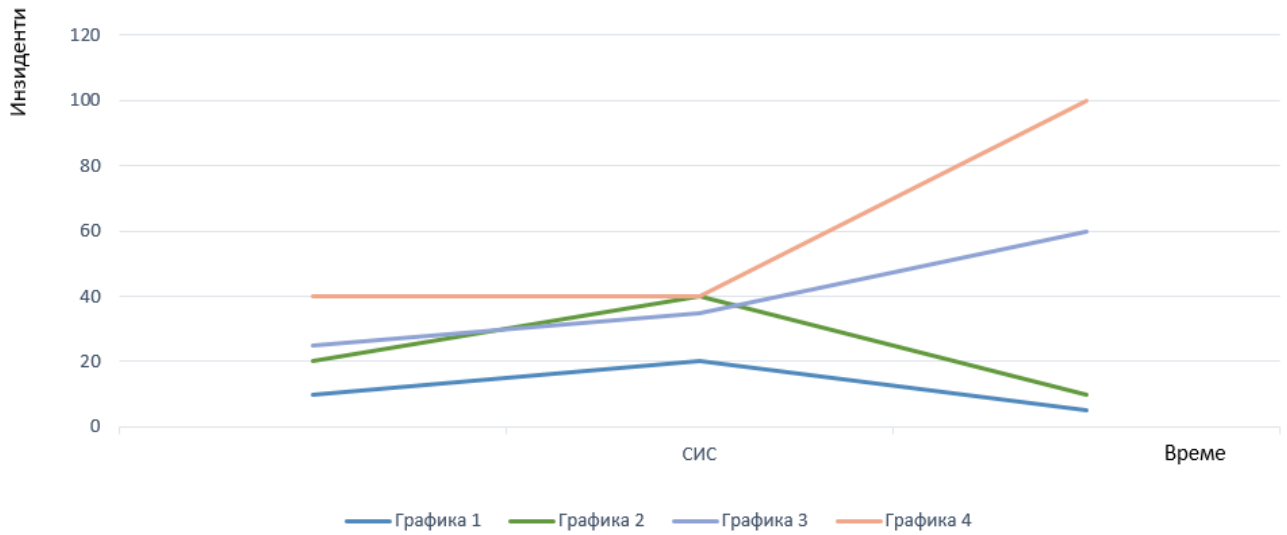
възможностите на съществуващите системи за информационна сигурност. Детайлното описание на случаите на употреба за защита на чувствителни за организацията данни чрез проектните модели с помощта на UML диаграми още на етап проектиране осигуряват възможност на СИС точно да изпълнява поставените цели, свързани с политиките за вътрешна сигурност, правните разпоредни и директивите за поверителност. Реализирането на СИС с платформа СПИД осигурява интиутивно създаване на политики, описващи случаите на употреба чрез предложените сценарии.

Функционално разширената СИС е ефикасен инструмент за предотвратяване и разследване на инциденти, свързани с изтичане на чувствителна информация.

Проектния модел дава ясна представа за процесите, свързани с обработка и трансфер на информация в организацията.

В резултат на проведените изпитания на доразвитие на съществуваща СИС чрез нови случаи на употреба за защита на чувствителни за организацията данни (Таблица 11), е установено следното:

1. Намаляване на инцидентите, свързани с изтичане на чувствителна информация (Графика 1 от Фиг. 35).
2. Ограничаване на информационните канали по които е възможно изтичането чувствителна информация (Графика 2 от Фиг. 35)
3. Повишаване видимостта на чувствителната информация от тип Данни в покои (Графика 3 от Фиг. 35)
4. Подобряване на съответствието с политиките за вътрешна сигурност, правните разпоредби и директивите за поверителност (Графика 4 от Фиг. 35)
5. Правилата за защита на чувствителни данни, изготвени по сценариите на случаите на употреба се изпълняват стриктно и безотказно от Функционално разширената СИС.



Фигура 35. Обобщени резултати от изпитания на доразвитието на съществуваща СИС

4.5 Трансформиране на ОО проектен модел в агентно-базиран модел на реализация

Внедряването на система с реални компоненти изисква значителни средства,

време, сериозни усилия и човешки капитал за нейното тестване и събиране на реални данни. Поради тази причина се налага да симулираме действието на проектираната система в избраната агентно-базирана симулационна среда. Това изисква да се трансформира създадения ОО проектен модел на системата във агентно-базиран модел на реализацията, чието действие трябва да се симулира.

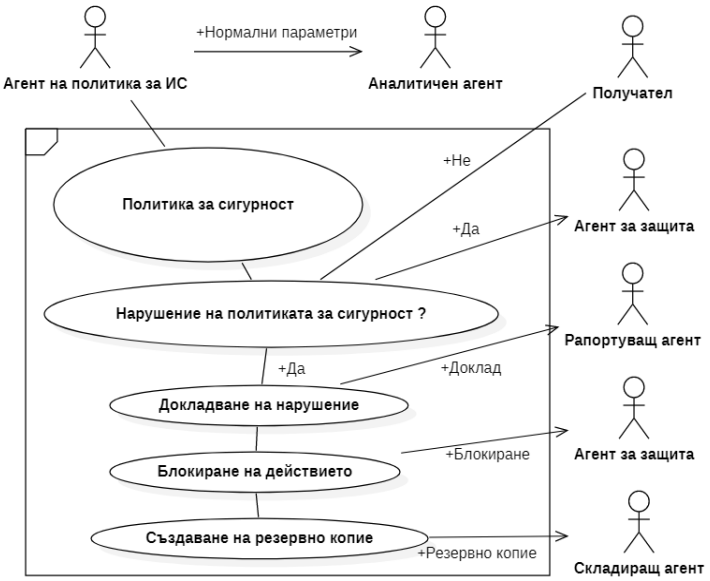
В агентно-базираните системи, агентът събира и обработва информация за околната среда, в която действа, и въздейства върху нея на базата на взети от него решения и про-активна дейност. При СИС допускаме, че отделни агенти изпълняващи самостоятелни задачи по защита на даден актив или информация са част от системата. За да се постигнат целите на СИС, тя трябва да осигури дейността на няколко основни вида агенти, изпълняващи определена роля и извършващи интеракции между тях: *„Агент по нарушенията“, „Агент за Защита“, „Агент на политика за ИС“, „Агент за наблюдение“, „Рапортуващ агент“,„Комуникационен Агент“,„Обработващ агент“, „Складиращ агент“,„Агент за реализация на услуги“.*

Трансформацията от обектно-ориентирания проектен модел на СИС в агентно-базиран модел на реализация се основава на клас-диаграмата от Фигура 21. Видимо е че клас "Контрол" съдържа в себе обекти, които имат потенциал да се превърнат в про-активни агенти, взимащи самостоятелни решения. Този клас взаимодейства с останалите класове (Защита, Данни и Управление), които оформят околната среда на класа агенти, която осигурява необходимата им за работа информация за вземане на решения. Освен това агентите въздействат на тази околна среда с цел постигане на конкретни резултати за които СИС е създадена и получава от тях информация, на чиято база взима решенията. Можем да приемем че тези класове формират околната среда, с която класа "Контрол" взаимодейства. Можем да дефинираме клас "Околна среда", съставен от трите класа Защита, Данни и Управление. Тогава класа "Контрол" става Агент "Контрол", взаимодействащ с новия клас "Околна среда" (Фигура 36). На тази база приемаме, че класът "Контрол" се трансформира в клас “Агент“, които представя съвкупност от агенти, всеки от които има определена цел.

Фигура 36. Класове „Агент“ и „Околна среда“

В съответствие с отделните цели и нуждата от определени роли, класът „Агент“ обхваща: „Агент по нарушенията“, „Агент за Защита“, „Агент на политика за ИС“, „Агент за наблюдение“, „Рапортуващ агент“, „Комуникационен агент“, „Обработващ

агент“, „Складиращ агент“ и „Агент за реализация на услуги“ (Фигура 36).



Фигура 38. Диаграма на случай на използване при „Агент на политика за ИС“

Фигура 39. Диаграма на случай на използване при „Агент за защита“

За да се опише ролята на всеки агент чрез използване на ОО език UML се използва диаграма „случай на използване“, която описва взаимодействието на даден агент с околната среда, която в нашия случай се разглежда като ОО система. За всеки един от изброените агенти се създава такава диаграма, която описва сценария по които той действа. За да покажем как става това се представя диаграмата „случай на използване“, на околната среда от агентите „Агент на политика за ИС“ и „Агент за защита“. По аналогичен начин са описани и останалите агенти, с което се създава агентно-базиран модел на реализация на СИС. Този модел се използва при симулиране дейността на проектираната система. На Фигура 37 е показана диаграма на случай на използване за „Агент на политика за ИС“, а на Фигура 38 - диаграма на случай на използване за „Агент за Защита“.

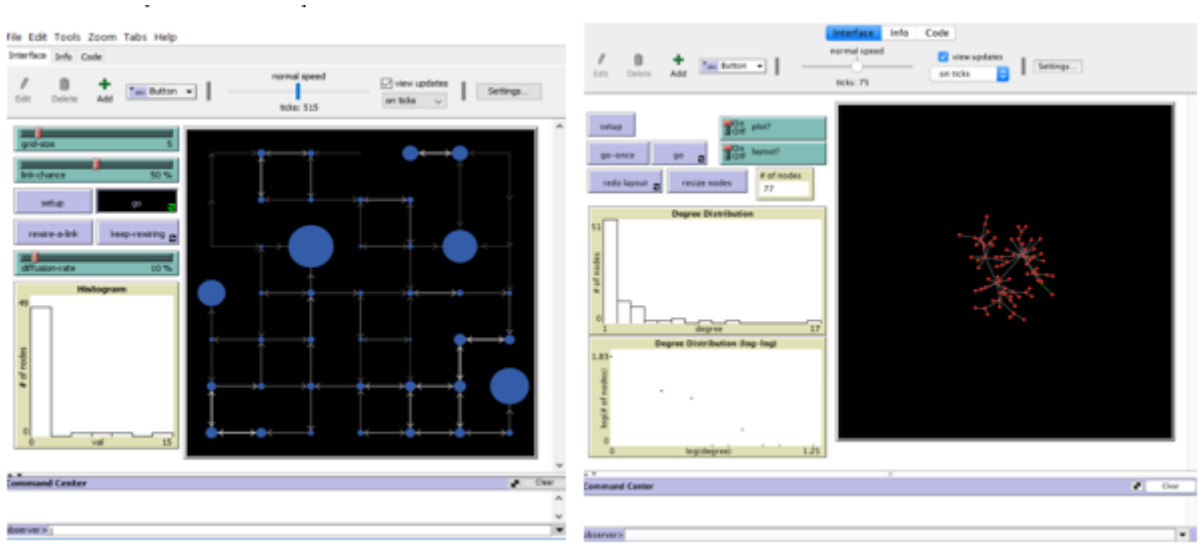
4.6 Симулиране на системи за информационна сигурност и анализ на генерираните тестови данни

Реализацията на симулацията на архитектурния модел на СИС извършваме 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 [102].

Експерименти в средата NetLogo

NetLogo (Фигура 39) е мулти-агентна крос-платформена симулационна среда за симулиране на сложни системи във времето [47, 118]. 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 Фигура 14 е създаден агентно-ориентиран модел в средата NetLogo (v.6.0.4).

Резултатите от симулациите на този модел са показани на Фигура 40. Като цяло са изследвани взаимодействията между отделните блокове: “Агент за Защита ”, “Комуникационен Агент”, “Агент по нарушенията”, “Агент на политика за ИС”, “Рапортуващ агент”, “Складиращ агент”, “Агент за наблюдение”, “Агент за реализация на услуги” и “ Обработващ агент”. 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.



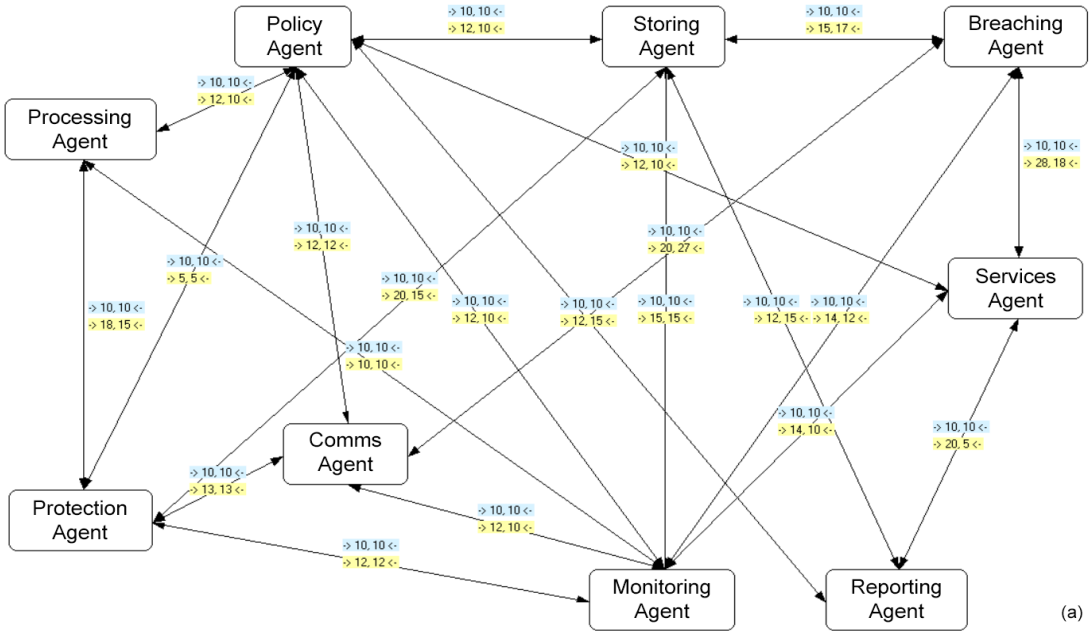
Фигура 40. Екранни снимки от симулация в среда на NetLogo

Експерименти в средата I-SCIP-SA

С цел по-голяма близост до реалността, позволяваща смесено изследване на предложените архитектурни решения на СИС е разработен мулти-агентен модел [28] от тип „система-от-системи“ [126] в средата I-SCIP-SA (Intelligent Scenario Computer Interface Program for System Analysis) [105]. При това е приложен опита от [106] и организацията от модела, предложен в [103] и реализиран в [107], аналогични на изследванията в средата NetLogo. Целта е 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 с активното участие и на човешкия фактор. Машинно, резултатите са представени посредством организацията „обект-връзка“ [108] 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 между-агентна комуникация, така и за визуализация на външни (записани или получавани в реално време) данни (Фигура 40). Между-агентните 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 между-агентните 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.



Фигура 41. Мулти-агентен модел на СПИД за проактивно изследване изтичане на данни в корпоративна среда

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, например [109, 110, 111], като тук се използва “3D Диаграма на чувствителността” – “3D ДЧ” (Фигура 41), 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]).

Фигура 41. Мулти-агентен модел на СПИД с допълнителни класификационни начални оценки на агентите в 3D ДЧ

Предложеното решение предоставя възможност за проактивно участие на човешкия фактор в процеса на вземане на решения, гарантирайки цялостно разглеждане и оценка на ролите на СПИД (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” [112], в зависимост от избраните симулационни сценарии. Получените резултати от анализа на мулти-агентния модел на СПИД 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, пост-анализа 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.

Генериране и анализ на тестови данни

Изпълнението на тази задача е 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.

В настоящата глава подробно е описано проактивно стохастично решение за смесена валидация върху предложения системен модел.

Верифицирането на резултатите от стохастичните симулации е проведена емпирично, с използване на интерактивна симулация в трансформирана реалност, организирана в рамките на ученията CYREX 2018, 2019 и 2020 [109, 117, 122, 123].

4.5 Заключение

В глава 4 са описани подходи за създаване на модел на реализация на СИС чрез предлаганата от нас методология за разработване на СИС.

На базата на проектен обектно-ориентиран модел е изграден ОО модел на реализация, съобразен със съществуваща среда за реализация. След извършване на анализ на проблемната област и на базата на изграден концептуален модел, резултат от този анализ, са уточнени изискванията към архитектурата на разработваната СИС. Направен е анализ на съществуващи платформи за реализация СПИД и е избрана най-подходящата в съответствие с модела на анализа.

Моделът на реализация описва съществуваща платформа за реализация на СИС от тип СПИД „Cososys EndPoint Protector 5.0.2.1“. За целта се използват съществуващите UML диаграми: „Пакетна диаграма“, „Компонентна диаграма“ и „Диаграма на внедряване“.

Представеният метод дава възможност за моделиране и реализация на нови аспекти от СИС без да се налага системата да се проектира отначало. За целта е достатъчно да се доразвие съществуваща СИС чрез включване на нови случаи на употреба за защита на чувствителни данни за организацията. В главата е представен пример с конкретни сценарии на нови случаи на употреба (use cases), както и проведени изпитания на реализираното разширение на системата.

За да се симулира работата на проектираната СИС е изграден агентно-базиран модел на реализация. За целта е създаден симулационен модел на разработваната СИС, който може да се реализира в мулти-агентна крос-платформена симулационна среда за симулиране на сложни системи във времето. Представен е подход за трансформиране от обектно-ориентиран модел в агентно-базиран модел.

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.

Генерирането и анализа на тестови данни е организирано на две стъпки:

- Стохастична валидация на очакванията за изтичания на данни, посредством експертни допускания и машинно генерирани ad-hoc селекции за изтичания на данни;
- 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.

Предложените практическа валидация и верификация на избрана комерсиално достъпна СПИД платформа за реализация 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.

Чрез агентно-ориентирания подход може да се покаже динамиката на системата, която с другите модели не може да бъде представена. Агентно-ориентирания модел ни дава цялостна картина, която нито концептуалния, нито обектно-ориентирания модел може да даде. Симулацията на СИС дава възможност да бъде изследвана динамиката на системата при различни сценарии. Сценариите са описани и предс-тавени чрез диаграми на случаи на използване в ОО модел и след това симулирани чрез агентния подход. Симулацията може да покаже поведението на системата при промяна на околната среда. Такава е например промяна на законодателство или нормативна база, даващо определени приоритети, влиянието на вътрешни или външни за организацията лица, поява на нов тип заплахи или нестандартни начини за изтичане на данни. Резултатите от симулацията помагат да се предвидят както традиционните, така и по-рядко срещани заплахи и да се оптимизира използването на ПИС.

Глава 4 описва изпълнението на задачи 5 и 6, дефинирани в "Цел и задачи на дисертацията":

- Развитие на съществуващи СИС на базата на проектиране и реализация на нови случаи на употреба, отнасящи се до чувствителни данни.
- Определяне на подход за трансформиране на проектния модел на СИС в модел на реализация;
- Симулация на СИС на базата на модела на реализация. Генериране и анализ на тестови данни.

В резултат от изпълнената научноизследователската дейност се постигат следните научно-приложни приноси:

1. Предложен е UML модел на реализация на СИС в организация, използваща СПИД платформа за реализация „Cososys Endpoint Protector 5.0.2.1“
2. Сравнителен анализ на съществуващи СПИД платформа за реализация на базата на изискванията, описани в модела на анализа.
3. Проектиране, реализация и тестване на разширение на съществуващи СИС с поддържането на нови случай на употреба.
4. Реализиран е симулационен модел на СИС на базата на обектно-ориентирано описание на архитектурата му чрез използване на агентно-базирано представяне в средите NetLogo и I-SCIP-SA; Симулационно изследване на архитектурата на СИС чрез извършване на стохастична валидация и интерактивна верификация.

Библиография

1. Suryateja P.S., “Threats and Vulnerabilities of Cloud Computing: A Review”, International Journal of Computer Sciences and Engineering, Volume 6, Issue 3, published 30.03.2018
2. Rhodes-Ousley M., “Information Security the Complete Reference”, 2nd Edition, The McGraw-Hill, 2013
3. Diogenes Y., Ozkaya E., “Cybersecurity - Attack and Defence Strategies”, Packt Publishing Ltd., 2018
4. Pfleeger C. P.,.Pfleeger S.L, Margulies J., “Security in Computing”, 4th Edition, Prentice Hall, 2015
5. Ciampa M., “Security+ Guide to Network Security Fundamentals”, 4th Edition, Course Technology, Cengage Learning, 2015

6. CISSP Study Guide, https://www.sciencedirect.com/book/9781597499613/cissp-study-guide, last accessed 2021/08/11
7. The European Network and Information Security Agency (ENISA) (2012b), https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape/at_download/fullReport, last accessed 2021/08/11
8. Landoll D., Information Security Policies, Procedures and Standards - A Practitioner's Reference, CRC Press, Taylor & Francis Group, 2016, ISBN 978-1-4822-4591-2
9. Гайдарски И., Кутинчев П., Откриване на вътрешни заплахи и предотвратяване изтичането на чувствителна информация от организацията, Научна конференция "Необходима достатъчност за осигуряване на въздушния суверенитет на България и ролята на човешкия фактор", Военна Академия "Г.С.Раковски", 11.10.2018, София, България, ISBN 978-619-7478
10. Whitman M, Mattord H., Principles of Information Security, Fourth Edition
Course Technology, Cengage Learning, 2012
11. Gragido W., Pirc J.. Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats. Syngress, 2011.
12. Keung Y., "Information Security Controls", Adv Robot Autom 2013, Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Hong Kong
13. Bhaskar SM, Ahson SI (2008) Information Security: A practical Approach, Oxford: Alpha Science International Ltd.
14. Schweitzer JA, Managing Information Security: Administrative, Electronics, and Legal measures to Protect Business Information. Boston: Butterworths. 1990
15. Наредба за минималните изисквания за мрежова и информационна сигурност, https://www.mtitc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf, last accessed 2021/08/11
16. Guide for Conducting Risk Assessments. NIST Special Publication 800-30 rev.1, NIST, September 2012, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, last accessed 2021/08/11
17. Guidelines on assessing DSP and OES compliance to the NISD security Requirements, ENISA, November 2018, https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements,last accessed 2021/08/11
18. Standards, Guidelines, Tools and Techniques, ISACA, May 2016, https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/standards-guidelines-tools-and-techniques , last accessed 2021/08/11
19. Шаньгин В.Ф. "Защита информации в компьютерниьх системах и сетях", ДМК Пресс 2012, ISBN 978-5-94074-637-9
20. Hayden L., "IT Security Metrics: A Practical Framework for measuring Security & Protecting Data, 2010 by The McGraw-Hill, ISBN: 978-0-07-171341-2
21. Alhassan M, Adjei-Quaye A., Information Security in an Organization, International Journal of Computer (IJC), Global Society of Scientific Research and Researchers 2017, ISSN 2307-4523
22. Dimitrov W, Syarova S., Analysis of the functionalities of a Shared ICS Security Operations Center, International Conference "Big Data, Knowledge and Control Systems Engineering" 6th IEEE International Conference BdKCSE'2019, 21-22 November 2019, Sofia, Bulgaria
23. Accenture Security 2019 Cyber Threatscape Report, 2019
https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf, last accessed 2021/08/11

24. Insider Threat Report, Verizon 2019, _https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf, last accessed 2021/08/11
25. ENISA Threat Landscape - Responding to the Evolving Threat Environment European Network and Information Security Agency (ENISA), 2012, https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape/at_download/fullReport, last accessed 2021/08/11
26. ENISA Threat Landscape Report 2020 - 15 Top Cyberthreats and Trends, European Network and Information Security Agency (ENISA), 2019, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020, last accessed 2021/08/11
27. Минчев З., Кутинчев П., Гайдарски И.. Топ 10 заплахи за киберпространство през 2019. IT4Sec Reports, Institute of ICT, Bulgarian Academy of Sciences, 2019, ISSN:1314-5614, DOI:10.11610/it4sec.0133, 133-1-133-12 Национално академично издателство
28. Bollinger J., Enright B., Valites M., Crafting the InfoSec Playbook, O'Reilly Media, Inc., 2015, ISBN: 978-1-491-94940-5
29. Andress J., The basics of information security : understanding the fundamentals of InfoSec in theory and practice, Elsevier Inc. 2011
30. Taylor-Duncan L., Come in, We're Open – Keeping Your Company's IT Data Safe From Threats, Techni-Core productions, 2014
31. SysSec Red Book - Roadmap in the area of Systems Security, SysSec consortium, http://www.red-book.eu/, last accessed 2021/08/11
32. Минчев З., Гайдарски И., Кибер рискове, заплахи и мерки за защита, свързани с COVID-19, CSDM Views, Number 37, 2020, ISSN 1314-5622
33. Gaydarski I.,Discovery and Protection from Internal Threats in Critical Infrastructure's objects., Proceedings of BISEC 2019, Belgrade Metropolitan University, Belgrade Metropolitan University, приета за печат: 2019
34. Yassein M., Hmeidi I., Mohammad Al-Rousan Y., Arrabi D., Black Hole Attack Security Issues, Challenges & Solution In Manet, Conference: International Conference on Computer Science, Engineering and Information Technology (CSEIT-2018) Dubai, UAE, DOI: 10.5121/csit.2018.81815
35. Chandler J., Security in Cyberspace: Combatting Distributed Denial of Service Attacks, University of Ottawa, January 2003
36. Understanding Denial-of-Service Attacks, Cybersecurity & Infrastructure Security Agency, USA, https://www.us-cert.gov/ncas/tips/ST04-015, last accessed 2021/08/11
37. WASC Threat Classification v2.0, Web Application Security Consortium, 2010, http://projects.webappsec.org/f/WASC-TC-v2_0.pdf?ld=1 , last accessed 2021/08/11
38. LizaMoon Mass SQL-Injection Attack Infected at least 500k Websites, https://isc.sans.edu/forums/diary/LizaMoon+Mass+SQLInjection+Attack+Infected+at+least+500k+Websites/10642, last accessed 2021/08/11
39. Botnets: Measurement, Detection, Disinfection and Defence, European Network and Information Security Agency (ENISA), March 2011, https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence, last accessed 2021/08/11
40. DDoS Malware, Verisign 2013, https://www.informationweek.com/pdf_whitepapers/approved/1370027144_VRSNDDoSMalware.pdf , last accessed 2021/08/11
41. Nazario J., BlackEnergy DDoS Bot Analysis.. Arbor Networks, 2007, http://pds15.egloos.com/pds/201001/01/66/BlackEnergy_DDoS_Bot_Analysis.pdf, last accessed 2021/08/11

42. Tracking GhostNet: Investigating a Cyber Espionage Network. Information Warfare Monitor, March 2009, https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, last accessed 2021/08/11
43. Shadows in the Cloud: An investigation into cyber espionage 2.0. Information Warfare Monitor and Shadowserver Foundation, 2010, https://citizenlab.ca/wp-content/uploads/2017/05/shadows-in-the-cloud.pdf, , last accessed 2021/08/11
44. Keizer, G., Is Stuxnet the 'best' malware ever?, Computerworld, September 2010. http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever, last accessed 2021/08/11
45. Gaydarski I., Kutinchev P., Holistic Approach to Data protection - identifying the weak points in the organization.. Proceedings of BdKCSE'2017 (7 December, 2017 Sofia), САИ, 2018, ISSN:2367-6450, 125-135
46. Gaydarski I, Minchev Z.. Challenges to Data Protection in Corporate Environment, Chapter 8, In Minchev Z., (Ed) Book "Future Digital Society Resilience in the Informational Age", Sofia, Institute of ICT, Bulgarian Academy of Sciences, SoftTrade, December, 2018, ISBN 978-954-334-221-1, 82-100
47. Parsons, S., Gymtrasiewicz, P. and Wooldridge, M. (Eds). Game Theory and Decision Theory in Agent-Based Systems (Multiagent Systems, Artificial Societies, and Simulated Organizations), Springer, 2002.
48. Wahlstrom B. "Perspectives of Human Communication", Wm.C.Brown Publishers, 1992, ISBN 0-697-10704-3
49. Nwana, H. and Ndumu, D. An Introduction to Agent Technology, Software Agents and Soft Computing: Towards Enhancing Machine Intelligence, Concepts and Applications, Lecture Notes in Computer Science 1198, Springer, 3-26,1997.
50. Russel, S., Norving, P. Artificial Intelligence: A Modern Approach, Prentice Hall, New Jersey, 1995.
51. Wooldridge M, An Introduction To Multiagent Systems, John Wiley & Sons 2002, ISBN: 047149691X
52. Buecker A., Andreas P., Paisley S., Understanding IT Perimeter Security, Redpaper, IBM, November 2009, https://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf, last accessed 2021/08/11
52. Santana G.,Cruz D., Modelling a network security systems using multi-agents systems engineering, Systems, Man and Cybernetics, 2003. IEEE International Conference, Vol.5, November 2003, DOI: 10.1109/ICSMC.2003.1245655
53. Guidelines for Data Classification, Carnegie Mellon University, https://www.cmu.edu/iso/governance/guidelines/data-classification.html,
last accessed 2021/08/11
54. Ahmed S., Karsiti M., Multiagent Systems ,In-Teh Croatia, 2009, ISBN 978-3-902613-51-6
55. Закон за киберсигурност, приет на 31 октомври 2018, 7 ноември 2018, https://www.mlsp.government.bg/uploads/3/zakonodatelstvo/za-kibersigurnost.pdf, last accessed 2021/08/11
56. Национална стратегия за киберсигурност „Кибер устойчива България 2020", Юли 2016, http://www.strategy.bg/StrategicDocuments/View.aspx?Id=1120, , last accessed 2021/08/11
57. Полимирова Д, Шаламанов В., Стоянов Н, Тагарев Т., Янакиев Я., Шарков Г., Папазов Я., Ризов В., Иванова К., Киберсигурност и възможности за приложение на иновативни технологии в работата на държавната администрация в България, Институт за публична администрация, 2019, ISBN 978-619-7262-14-8 https://www.ipa.government.bg/sites/default/files/01_ipa_study_v10.0._final_ed.pdf, last accessed 2021/08/11

58. Olivé A., Conceptual Modeling of Information Systems, January 2007, Springer DOI: 10.1007/978-3-540-39390-0
59. Mallikaarachchi V., Data Modeling for System Analysis, INFORMATION SYSTEMS ANALYSIS - IS 6840, University of Missouri, St. Louis, 2010 http://www.umsl.edu/~sauterv/analysis/Fall2010Papers/varuni/, last accessed 2021/08/11
60. Edgar T., Manz D., Research Methods for Cyber Security, Elsevier Inc. 2017, ISBN: 9780128053492
61. Saltzer J., Schroeder M., "The protection of information in computer systems," in Proceedings of the IEEE, vol. 63, no. 9, pp. 1278-1308, September 1975
62. Turing A., Computing Machinery and Intelligence, Mind, Volume LIX, Issue 236, October 1950, Pages 433–460, https://doi.org/10.1093/mind/LIX.236.433,
63. Laplante P., What Every Engineer Should Know about Software Engineerin, Boca Raton, CRC, 2007. ISBN 9780849372285
64. Cyber Kill Chain, Lockheed Martin https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html , last accessed 2021/08/11
65. Hutchins, E. M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research Volume 1. 2011, pp. 80-106.
66. Finkelsetin A, Kramer J., Nuseibeh B., Finkelstein L., Goedicke M., Viewpoints - A Framework for Integrating Multiple Perspectives in System Developmen, International Journal of Software Engineering and Knowledge Engineering 02(01), November 2011
67. Hilliard R.,Emery D., Maier M., ANSI/IEEE 1471 and Systems Engineering, Systems Engineering 7(3):257 - 270, June 2004, DOI: 10.1002/sys.20008
68. Общ регламент относно защита на личните данни (Регламент (ЕС) 2016/679), https://cpdp.bg/?p=element&aid=991 , last accessed 2021/08/11
69. Националната стратегия за киберсигурност „Киберустойчива България 2020", приета от Министерски съвет на Република България на 13 юли 2016 г., http://www.cyberbg.eu/, last accessed 2021/08/11
70. Актуализирана стратегия за национална сигурност на Република България, приета с Решение на Народното събрание от 14 март 2018 г, https://www.mod.bg/bg/doc/cooperation/20181005_Akt_strateg_NS_RB.pdf, last accessed 2021/08/11
71. Стратегията за национална сигурност на Република България, https://me.government.bg/bg/themes/bulgaria-s-national-security-strategy-904-0.html, last accessed 2021/08/11

72. Закон за управление и функциониране на системата за защита на националната сигурност, Ноември 2015, https://www.parliament.bg/bg/laws/ID/15270, last accessed 2021/08/11
73. Правилник за дейността, структурата и организацията на Държавна агенция "Електронно управление", приет с постановление № 274 от 28 октомври 2016, https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=108729, last accessed 2021/08/11
74. Закон за киберсигурност, приет от Народното събрание на 31 октомври 2018 г, https://parliament.bg/bg/laws/ID/78098, last accessed 2021/08/11
75. Закон за защита на класифицираната информация, 26.02.2019г. https://www.damtn.government.bg/wp-content/uploads/2019/06/zakon-za-klasifitsiranata-informacia.pdf, last accessed 2021/08/11
76. БДС EN ISO/IEC 27001:2017 „Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията", https://www.bds-bg.org/bg/project/show/bds:proj:102367, last accessed 2021/08/11

77. Директива 2016/1148 ЕС относно мерки за високо общо ниво на сигурност на мрежовите и информационни системи в Съюза, https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32016L1148, last accessed 2021/08/11
78. J. Hintzbergen, K. Hintzbergen, A. Smulders, and H. Baars, “Foundations of Information Security Based on ISO27001 and ISO27002,” 3rd Edition, Van Haren Publishing, 2015.
79. ISO 27001 Official Page, https://www.iso.org/isoiec-27001-information-security.html, last accessed 2021/08/11
80. COBIT Security Baseline: An Information Survival Kit, 2nd Edition, IT Governance Institute, 2007.
81. COBIT resources, http://www.isaca.org/COBIT/Pages/default.aspx, last accessed 2021/08/11
82. NIST Special Publications (800 Series), https://csrc.nist.gov/publications/sp800, last accessed 2021/08/11
83. Gramm-Leach-Bliley Act (GLBA) Resources, www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act, last accessed 2021/08/11
84. S. Anand, Sarbanes-Oxley Guide for Finance and Information Technology Professionals, 2nd, Wiley, Edition, 2006
85. Sarbanes-Oxley Act, https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#sox2002, last accessed 2021/08/11
86. R. Herold and K. Beaver, “The Practical Guide to HIPAA Privacy and Security Compliance,” 2nd Edition, CRC Press, 2014
87. PCI Security Standards, https://www.pcisecuritystandards.org/pci_security/ , last accessed 2021/08/11.
88. IEEE 1471, IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, https://standards.ieee.org/standard/1471-2000.html, last accessed 2021/08/11
89. ISO/IEC/IEEE 42010:2011 – Systems and Software Engineering – Architecture Description, https://www.iso.org/standard/50508.html, last accessed 2021/08/11
90. Наков С., Колев В., Принципи на програмирането със C#, Издателство Фабер, Велико Търново 2018, ISBN: 978-619-00-0778-4
91. Горанов П., Тодорова Е., Георгиева Д., Концептуален модел на обектно-ориентирана библиотека от механични компоненти, Българско списание за инженерно проектиране, брой 35, януари 2018г, ISSN 1313-7530
92. Митрев Р., Компютърно моделиране и симулация, Пропелер, София, 2016г
93. A. Solvberg, Data and What They Refer to, Conceptual Modeling, Lecture Notes in Computer Science, vol 1565. Springer, Berlin, Heidelberg, 1999. https://doi.org/10.1007/3-540-48854-5_17
94. L. Vigotsky, Thought and Language, The M.I.T. Press, USA, 1962
95. DeviceLock Web Page, https://www.acronis.com/en-us/products/devicelock, last accessed 2021/08/11
96. CoSoSys Endpoint Protector Web Page, https://www.endpointprotector.com/, last accessed 2021/08/11
97. The Unified Modeling Language (UML) Web Page, https://www.uml-diagrams.org accessed 2021/08/11
98. 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.
99. Gaydarski, I., Minchev, Z., Andreev, R.. Model Driven Architectural Design of Information Security System. Advances in Intelligent Systems and Computing, Madureira A., Abraham A., Gandhi N., Silva C., Antunes M. (eds) Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018).,

492, Springer, 2019, ISBN:978-3-030-17064-6, ISSN:2194-5357, DOI:10.1007/978-3-030-17065-3_35, 349-359.
100. Gaidarski, I. K., Minchev, Z. B., Andreev, R. D.. Model Driven Approach for Designing of Information Security System. Journal of Information Assurance and Security, 13, MIR Labs, 2019, ISSN:1554-1010, 149-158,
101. Gaydarski, I., Minchev, Z., Conceptual Modeling of Information Security System and Its Validation Through DLP Systems. Proceedings of BISEC 2017, Belgrade Metropolitan University, 2017, ISBN:978-86-89755-14-5, DOI: 10.13140/ RG.2.2.32836.53123, 36-40
102. Gaydarski, I., Minchev, Z.. Virtual Enterprise Data Protection: Framework Implementation with Practical Validation. Proceedings of BISEC 2018, October 20, Belgrade, Serbia, Belgrade Metropolitan University, 2019, ISBN:978-86-89755-17-6,
103. Gaydarski, I., Minchev, Z., Andreev, R.. Model Driven Architectural Design of Information Security System. Advances in Intelligent Systems and Computing, Madureira A., Abraham A.,Gandhi N., Silva C., Antunes M. (eds) Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018)., 492, Springer, 2019, ISBN:978-3-030-17064-6, ISSN:2194-5357, DOI:10.1007/978-3-030-17065-3_35, 349-359.
104. Гайдарски И., Минчев З., „Моделиране, анализ, експериментална валидация и верификация на системи за информационна сигурност в корпоративна среда“, IT4SEC Reports, No. 132, 2019, стр. 1-29, ISSN 1314-5614
105. Minchev Z., “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, DOI: 10.13140/RG.2.1.1865.4481
106. Boyanov L., Minchev Z., “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.
107. Gaydarski I., Minchev Z.. Challenges to Data Protection in Corporate Environment, Chapter 8, In Z. Minchev, (Ed) Book “Future Digital Society Resilience in the Informational Age”, Sofia, Institute of ICT, Bulgarian Academy of Sciences, SoftTrade, December, 2018, ISBN 978-954-334-221-1, 82-100
108. Chen P., “The Entity-Relationship Model-Toward a Unified View of Data,” ACM Transactions on Database Systems 1, 1976, pp. 9-36.
109. Minchev Z., “Data Relativities in the Transcending Digital Future,” In Proc. of BISEC 2018, Belgrade, Serbia, October 20, 2018 (in press)
110. Minchev Z., Dukov G., Cyber Intelligence Decision Support in the Era of Big Data, In ESGI 113 Problems & Final Reports Book, Chapter 6, Fastumprint, 2015, pp. 85-92.
111. Minchev Z., “Security Challenges to Digital Ecosystems Dynamic Transformation,” In Proc. of BISEC 2017, Belgrade, Serbia, October 18, 2017, pp. 6-10.
112. Sycara K., “Multiagent Systems,” AI Magazine, 19, No. 2, 1998, pp. 79-92.
113. Gaydarski, I., Kutinchev,P.. Using Big Data for Data Leak Prevention. proceedings of The International Conference “Big Data, Knowledge and Control Systems Engineering” (BdKCSE’2019)), IEEE Digital Library, 2020, ISSN:2367-645, DOI:10.1109/BdKCSE48644.2019.9010596
114. Data Breach Investigations Report 2021, Verizon, 2021,: https://www.verizon.com/business/resources/reports/dbir/, last accessed 2021/08/11
115. Forrester J., “World Dynamics,” Cambridge, Massachusetts, Wright-Allen Press, 1971.

116. Meadows D., Randers J., Meadows D., Limits to Growth: The 30-Year Update, Chelsea Green Publishing Company, 2004.
117. CYREX 2018 Web Page: http://securedfuture21.org/cyrex_2018/cyrex_2018.html , last accessed 2021/08/11
118. Jain L., Lim C., Knowledge Processing and Decision Making in Agent-Based Systems, Springer-Verlag Berlin Heidelberg 2009, ISBN 13:978-3-540-88049-3
119. БДС EN ISO/IEC 27002:2017 “Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията”, https://www.bds-bg.org/bg/project/show/bds:proj:102368, last accessed 2021/08/11
120. БДС EN ISO/IEC 27003:2020 “Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Указания”, https://www.bds-bg.org/bg/project/show/bds:proj:114396, last accessed 2021/08/11
121. БДС ISO/IEC 27004:2017 "Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Наблюдение, измерване, анализ и оценяване", https://www.bds-bg.org/bg/project/show/bds:proj:102534, last accessed 2021/08/11
122. CYREX 2019 Web Page, http://securedfuture21.org/cyrex_2019/cyrex_2019.html, last accessed 2021/08/11
123. CYREX 2020 Web Page, http://securedfuture21.org/cyrex_2020/cyrex_2020.html, last accessed 2021/08/11
124. Gaidarski I., Minchev Z. (2021) Insider Threats to IT Security of Critical Infrastructures. In: Tagarev T., Atanassov K.T., Kharchenko V., Kacprzyk J. (eds) Digital Transformation, Cyber Security and Resilience of Modern Societies. Studies in Big Data, vol 84. Springer, Cham. https://doi.org/10.1007/978-3-030-65722-2_24
125. Schrecker S.,Soroush H., Molina J., Industrial Internet of Things Volume G4: Security Framework Paperback, Industrial Internet Consortium, September 19, 2016
126. Vester F., “The Art of Interconnected Thinking – Ideas and Tools for Dealing with Complexity,” München, MCB – Verlag, 2007.
127. MITRE ATT&CK® Framework, https://attack.mitre.org/, last accessed 2021/08/11
128. NIST Cybersecurity Framework, https://www.nist.gov/cyberframework, last accessed 2021/08/11
129. Open Web Application Security Project, https://www.owasp.org/, last accessed 2021/08/11
130. Common Attack pattern Enumeration and Classification, http://capec.mitre.org/ , last accessed 2021/08/11
131. ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, https://www.iso.org/standard/50341.html, last accessed 2021/08/11
132. ISO 31000:2009 Risk management — Principles and guidelines, https://www.iso.org/standard/43170.html, last accessed 2021/08/11
133. Risk and Responsibility in a Hyperconnected World - Pathways to Global Cyber Resilience
http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf, last accessed 2021/08/11
134. Tagarev T., Polimirova D., Main Considerations in Elaborating Organizational Information Security Policies, Proceedings of the 20th International Conference on Computer Systems and Technologies CompSysTech '19, June 2019, DOI: 10.1145/3345252.3345302
135. Hilliard R.,Malavolta I., Muccini H., Pelliccione P., On the Composition and Reuse of Viewpoints across Architecture Frameworks, Joint Working IEEE/IFIP Conference on

Software Architecture and European Conference on Software Architecture 2012, ISBN:978-1-4673-2809-8, DOI: 10.1109/WICSA-ECSA.212.21
136. Bezivin J., Jouault F., Valduriez P., “On the Need for Megamodels,” in Proceedings of the OOPSLA/GPCE: Best Practices for Model-Driven Software Development workshop, 2004.
137 Symantec Data Loss Prevention Web Page, https://www.broadcom.com/products/cyber-security/information-protection/data-loss-prevention/, last accessed 2021/12/14
138 McAfee DLP Endpoint Web page, https://www.mcafee.com/enterprise/en-us/products/dlp-endpoint.html, last accessed 2021/12/14
139 Forcepoint DLP Web Page, https://www.forcepoint.com/product/dlp-data-loss-prevention/, last accessed 2021/12/14