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

ДИСЕРТАЦИЯ

за придобиване на образователна 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.

Съдържание

Списък на фигурите

Списък на таблиците

Списък на термините

Accounting	Отчетност	Документиране на ресурсите, изразходвани от потребителя за достъп до данни или системи.
Attack	Атака	Опит да се получи неоторизиран достъп до информационен актив.
Authentication	Удостоверяване	Процес на потвърждение на самоличността на субект.
Authenticity	Автентичност	Доказателство че дадена единица е това, за което претендира.
Authorization	Упълномощаване	Осигуряване на достъп до данни или системи в организацията на съответния потребител след успешното му удостоверяване.
Availability	Наличност	Свойство за достъпност и използваемост при поискване от оторизирана единица.
Breach	Нарушение	Инцидент, водещ до потенциална експозиция или разкриване на данни към неоторизирана страна.
Confidentiality	Поверителност	Свойство на информацията да не бъде достъпна или да не се разкрива пред физически лица без разрешение.
Data	Данни	Съвкупност от стойности, определени за базови измерители, производни измерители и/или индикатори
Data Breach	Изтичане на данни	Инцидент, при който е осъществен достъп до чувствителни данни от неоторизирана страна.
Data Loss	Загуба на данни	Унищожаване или повреда на данни в резултат на инцидент, природно бедствие или човешка грешка.
External Threat	Външна заплаха	Атака срещу защитените информационни активи в посока отвън навътре.
Incident	Инцидент	Събитие, компрометиращо Цялостта, Поверителността или Наличността на информационните активи.
Information	Информация	Продукт на взаимодействие на данни и методи за тяхната обработка, необходим за решаване на конкретна задача.

Internal Threat	Вътрешни заплахи	Вътрешно за организацията лице, злоупотребяващо с оторизиран достъп до чувствителна информация.
Identification	Идентификация	Удостоверение на самоличност въз основа на официален документ.
Integrity	Цялостност	Свойство за точност и пълнота.
Knowledge	Знание	Неизяснена и променлива съвкупност от опит, ценности и информация в определен контекст, експертни възгледи и обоснована интуиция, които осигуряват среда и рамка за оценка и придобиване на нов опит и информация.
Signals / Alarms	Сигнали / Аларми	Известяване за настъпване на критично събитие, изискващо специално внимание.
Threat	Заплаха	Възможността източника на заплаха случайно или умишлено да експлоатира конкретна уязвимост
Threat Agent	Агент на заплаха	Агент на заплаха е лице, което причинява, пренася, предава или поддържа заплаха.
Threat Source	Източник на заплаха	Причинител на заплаха за информационна сигурност
Threat Vector	Вектор на заплахата	Определя се от източника на възникване на заплахата и пътя за достигане до целта
Validation	Валидиране	Потвърждаване на достъп до данни, приложение или система след предоставяне на обективно доказателство. че изискванията за достъпа са изпълнени.
Vulnerability	Уязвимост	Наличие на слабости в защитата, от които се възползва източника на заплаха.

Списък на съкращенията

ЗС	Защитна стена	Специализиран софтуер или хардуерно устройство, следящо и филтриращо мрежов трафик.
ЗЗС	Защита от зловреден софтуер	Решения за предпазване от зловреден софтуер.
ЗКТ	Защита на крайните точки	Защита на устройства срещу заплахи, атаки и изтичане на данни.
ИС	Информационна Сигурност	Осигуряване на поверителност, цялостност и наличност на чувствителна информация в цифров или аналогов формат.
КД	Класификация на данни	Маркиране на данни в зависимост от степента на тяхната чувствителност.
ПС	Периметрова сигурност	Набор от мерки за осигуряване на сигурност на данни и ресурси в периметъра на корпоративна ИТ мрежа.
СИС	Система за Информационна Сигурност	Система за опазване на информация, използвана или съхранявана в организация.
СОА	Системи за откриване на аномалии	Системи за наблюдение и анализ на мрежов трафик.
СПП	Системи за предотвратяване на проникване	Системи за елиминиране на заплахи от проникване в защитена мрежа.
СПИКЗ	Системи за предварителна информация за кибер-заплахи	Системи, осигуряващи информация в реално време за текущи и бъдещи кибер-заплахи.
СПИД	Системи за предотвратяване изтичане на данни	Системи за откриване и предотвратяване изтичане на данни извън защитената мрежа на организация.
AAA	Authentication, Authorization, and Accounting	Базов принцип за осигуряване на информационна сигурност - Принцип на тройното А – състоящ се от три компонента - Удостоверяване, Упълномощаване и Отчетност.
BYOD	Bring Your Own Device	Концепция „Донеси Собствено Устройство“
CIA	Confidentiality, Integrity, Availability	Базов принцип за осигуряване на информационна сигурност - Триада „Поверителност, Цялостност, Наличност“

Cyrex	Cyber Research Exercise	Ежегодно международно компютърно подпомагано упражнение за кибер-обучение, на представители на университети, академични и професионални асоциации, индустрия и бизнес.
DSA	Digital Signature Algorithm	Криптографски стандарт за цифрови подписи
DSS	Digital Signature Standard	Федерален стандарт за обработка на информация, определящ набор от алгоритми, които могат да бъдат използвани за генериране на цифрови подписи, установени от NIST, САЩ през 1994.
HMAC	Hashed Message Authentication Code	HMAC е специфичен код в криптографията, за удостоверяване на съобщение, включващ криптографска хеш-функция и секретен криптографски ключ.
IoT	Internet of Things	Интернет на нещата
UML	Unified Modeling Language	Унифициран обектно-ориентиран език за моделиране.

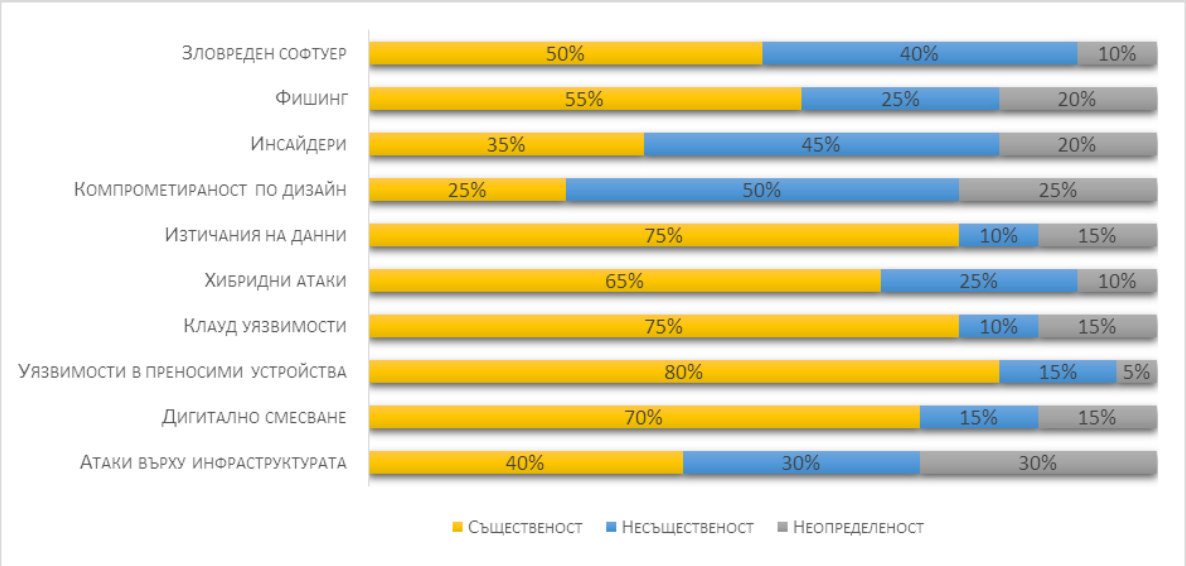
Увод

Актуалност на проблема

Информацията е най-ценния актив, с които разполагат организациите. 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].

Основни заплахи в киберпространството

При еволюционното развитие на технологиите, налагащи нови подходи за комуникация и съхраняване на данни, нови операционни системи, протоколи или просто техни нови версии, се появяват нови уязвимости, водещи до нови заплахи и съответно атаки. За съвременната информационна сигурност е от жизнено значение периодичното проучване, изследване, систематизиране и разработване на нови защитни процедури, техники, механизми и решения.



Фигура 1. Топ 10 заплахи в киберпространството през 2019 година

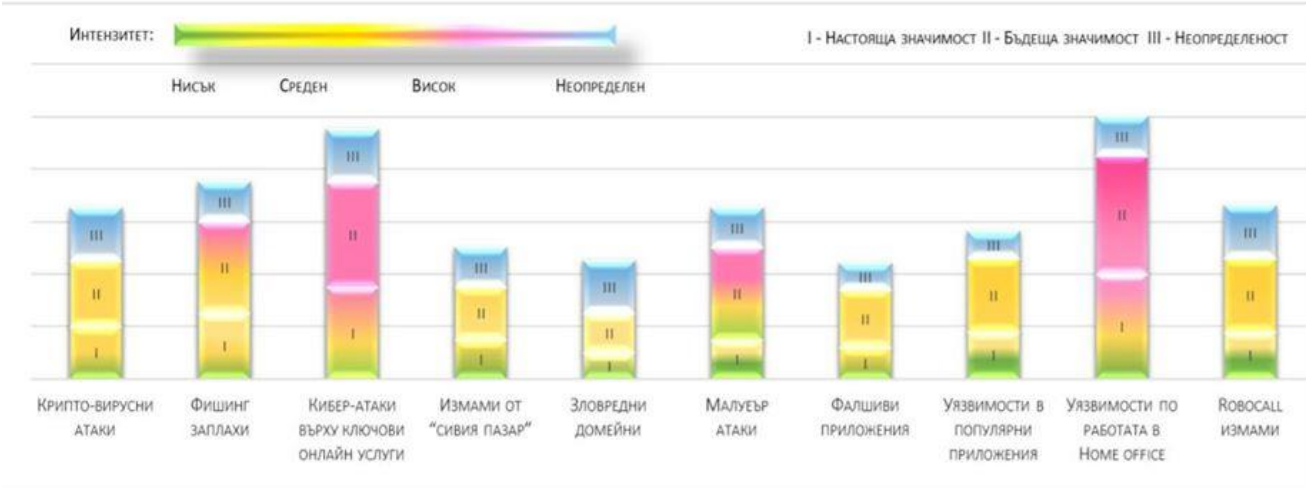
На Фигура 1 е показана обобщената картина на значимост за 10-те направления на изследване на заплахи в киберпространството през 2019 година [27, 32]:

1. Експозиция към трети страни;
2. Управление на софтуерно осъвременяване и кръпки;
3. Уязвимости в облака;
4. Нови разновидности на „Фишинг“ атаки;
5. Атаки тип „Откуп“;
6. Объркване между понятията, определени в стандарти и регулации, и реална защита на информационните активи;

7. Заплахи за мобилната сигурност;
8. Концепцията „Донеси Собствено Устройство“ (BYOD);
9. Интернет на нещата (IoT);
10. Остарял хардуер.

Актуалните заплахи за 2021 година са свързани с КОВИД-19 [32]. Основните резултати от направеният анализ могат да се обобщят около следните десет най-актуални рискове и заплахи от техно-социален тип (Фигура 2):

1. Крипто-вирусни атаки;
2. Фишинг заплахи;
3. Кибер-атаки върху ключови онлайн услуги;
4. Измами от сивия пазар;
5. Зловредни домейни;
6. Атаки на вируси и зловреден софтуер;
7. Фалшиви приложения;
8. Уязвимости в популярни приложения;
9. Уязвимости при дистанционна работа от къщи;
10. Измами тип „Роботизирани обаждания“.



Фигура 2. Обобщена картина на настоящата и бъдеща значимост за 10-те най-актуални рискове и заплахи от техно-социален тип, свързани с КОВИД-19

Веригата “уязвимости”, “заплахи”, и “атаки” 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. Методите за идентифициране и използване на уязвимостите на активите са известни като „Експлоатация“ (Exploits). Това са фактори, които дефинират “Пейзаж на заплахите” (Threat Landscape) [24, 25, 26]. 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 уязвимостите, и съответно до по-голяма успеваемост на атаките. 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 [24, 25, 26]. За да бъдат редуцирани успешните атаки към информационните активи е необходимо да бъде извършен анализ на всички елементи във веригата уязвимости-заплахи - атаки.

Информационната сигурност (ИС) е свързана със осигуряване на безопасността на информационните 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 проникване 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]. Компютърната 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 [3, 4, 124].

Информационната сигурност представлява непрекъснат процес на изравняване на риска с бизнес целите на организацията и минимизиране на остатъчния риск, политики за сигурност, повторно използване на знания, резултати от тестване за сигурност, управление на уязвимостта и противодействие на заплахи, както и прилагане на най-съвременните технологии като Големи масиви от данни (Big Data) [113], Машинно самообучение (Machine Learning) и Изкуствен Интелект(Artificial Intelligence) [22, 35, 50]. Необходимо е организациите да разработят цялостна, основана на оценка на риска стратегия за ИС, за да защитят чувствителната си информация.

Проектирането и последващото внедряване на съвременна система за информационна сигурност 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.

Регулации и законови рамки

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. Всяка организация работи в специфична среда, в която са в сила различни регулации и директиви. Такива например са: Общия регламент относно защита на личните данни (Регламент (ЕС) 2016/679), известен още и като EU GDPR [67], който регламентира защитата на личните данни на граждани на Европейския Съюз и Директива 2016/1148 ЕС относно мерки за високо общо ниво на сигурност на мрежовите и информационни системи в Съюза [77].

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. В аспекта на Системите за Информационна Сигурност (СИС), в областта на интерес са нормативните актове, формиращи основата на държавната политика в областта на информационната сигурност, сигурността в кибер-пространството, дейности по кибер-отбрана и по противодействие на кибер-престъпността [57]. Такива са:

- Наредба за минималните изисквания за мрежова и информационна сигурност , приета на 26.07.2019, чрез МПС N:186 [15],
- Националната стратегия за кибер-сигурност „Кибер устойчива България 2020”, приета от Министерски съвет на Република България на 13 юли 2016 г. [69],
- Актуализирана стратегия за национална сигурност на Република България, приета с Решение на Народното събрание от 14.03.2018 г.[70, 71],
- Закон за управление и функциониране на системата за защита на националната сигурност, в сила от 01.11.2015 г.[72],
- Правилник за дейността, структурата и организацията на Държавна агенция “Електронно управление”, приет с постановление № 274 от 28.10.2016 г.[73],
- Закон за кибер-сигурност, приет от Народното събрание на 31.10.2018 г.[74],
- Закон за защита на класифицираната информация [75].

От особено значение за приемането на единна политика за сигурност в организациите е Наредбата за минималните изисквания за мрежова и информационна сигурност. Чрез нея се дефинират изисквания за минималните мерки за мрежова и информационна сигурност; препоръчителни мерки за мрежова и информационна сигурност, правила за извършване на проверките за съответствие, редът за водене, съхраняване и достъп до регистъра на съществените услуги по чл. 6 от Закона за Кибер- сигурност, както и. образци на уведомленията при инциденти. Наредбата има задължителен характер.

Влияние върху формирането на политиката за сигурност имат и различни приложими стандарти като:

- БДС EN ISO/IEC 27001:2017 „Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията“ [76, 78, 79];
- БДС EN ISO/IEC 27002:2017 “Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията” [119];
- БДС EN ISO/IEC 27003:2020 “Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Указания” [120];
- БДС EN ISO/IEC 27004:2017 "Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Наблюдение, измерване, анализ и оценяване" [121];
- COBIT на ISACA (Information Systems Audit and Control Association) [80,81];
- “800 series" на NIST (The National Institute of Standards and Technology) [82];

Съществуват и специални регулации за специфични сектори и индустрии:

- Gramm-Leach-Bliley Act (GLBA) [83] – финансов сектор;
- Sarbanes-Oxley Act (SOX) [84,85] – публични компании в САЩ;
- Health Insurance Portability and Accountability Act (HIPAA) [86] – здравен сектор;
- Payment Card Industry (PCI) Data Security Standard (DSS) [87] – оператори на кредитни карти.

В практиката намират приложение и специализирани стандарти като IEEE 1471 [88] и IEEE 42010 [89], описващи архитектури на системи чрез методите на концептуалното моделиране, обект на настоящата дисертация.

Особено внимание трябва да се обърне на обработваните от организацията данни – често те подлежат на допълнителни регулации, не обхващащи останалата дейност на организацията. Например за организация, базирана в Япония EU GDPR не обхваща локалните лични данни, които тя обработва, освен ако те 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.

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 типа 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, които са в съответствие с различните етапи на разработване на СИС, показани на Фигура 5:

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.

Структура на дисертацията

Дисертацията се състои 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 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.

Глава 1

Базови принципи и метод за разработване на система за информационна сигурност

1.1. Базови принципи за осигуряване на информационна сигурност

Съществуват три базови принципа за осигуряване на информационна сигурност, известни като: Триада „Поверителност, Цялостност, Наличност“ (CIA Triad), принципа на тройното А (AAA) и принцип на най-слабото звено [10]. Едновременно с това се използват и няколко базови защитни модели, като периметрова защита, известна като „Модел на близалката“ (Lollipop model), многослоен модел, известен като „Луков модел“ (Onion model) и др.[2, 21].

Принципите се описват по следния начин:

1. „Триада „Поверителност, Цялостност, Наличност“ (ПЦН Триада)

Този принцип се фокусира върху три основни понятия: Поверителност (Confidentiality), Цялостност (Integrity) и Наличност (Availability), осигуряващи основните цели на мрежовата и информационната сигурност, а именно запазване на конфиденциалността, интегритета (цялостност и наличност) и достъпността на информацията през целия й жизнен цикъл (създаване, обработване, съхранение, пренасяне и унищожение) в и чрез информационните и комуникационни системи. Концепцията за ПЦН триадата е ориентирана към данните, ресурсите и се фокусира в най-важните аспекти на защитата на информацията. Принципът не претендира за всеобхватност и към него успешно може да бъдат добавени и допълнителни понятия, като Отчетност (Accountability) и Осигуряване (Assurance) или Надеждност (Reliability) [2, 4, 5, 16, 21]:

- Поверителност;
- Цялостност;
- Наличност;
- Отчетност;
- Осигуряване,
- Надеждност и др.

Поверителност – обозначава конфиденциалността на данни и системи, предотвратяването на разкриването или на достъпа до информация на неоторизирани лица, т.е. лица, нямащи съответното разрешение. В организации, боравещи с големи количества информация, данните могат да бъдат класифицирани с различни нива на сигурност, спрямо действащата нормативна база и вътрешни критерии. Осигуряването на поверителност изисква всички лица, имащи достъп до чувствителна информация, да разбират свързаните с това рискове и да носят съответна отговорност при боравенето с тази информация.

Цялостност – дефинира осигуряването на увереността, че информацията в организацията не е променяна, добавяна или изтривана без съответното разрешение. Общите мерки за защита на целостта включват криптиране на данни в покои и хеширане на данни в движение, права на файлове, контрол на версиите за предотвратяване на случайни промени или изтриване.

Наличност – чрез това понятие се дефинира гарантирането на наличността и достъпността на данни и активи, винаги когато те са необходими. За целта се използват различни технологии, осигуряващи: устойчивост на откази (fault tolerance),

балансиране на натоварването, излишък на хардуерни и софтуерни компоненти - резервни механизми (failover), системи за автоматичен отказ (automatic failover), както и различни процедури, като например план за възстановяване след бедствия и аварии..

Отчетност – отразява изискването за уникална идентификация и отчетност на даден актив. Чрез него се осигурява възпиране, изолация, откриване и предотвратяване на проникване, както и възстановяване след вреда или юридически действия.

Осигуряване – създава увереност, че основните цели на сигурността са адекватно изпълнени чрез конкретна реализация, осигуряваща основна функционалност, както и защита срещу неволни грешки от страна на потребители или софтуер, и устойчивост на умишлено влияние.

Надеждност – определя колко дълго услугата може да работи без никакво прекъсване.

2. *„Принцип на тройното А“ (AAA - Authentication, Authorization, and Accounting)*

Този принцип се състои от три компонента – Удостоверяване (Authentication), Упълномощаване (Authorization) и Отчетност (Accounting) [2, 21].

Удостоверяване – Това е процес, при който самоличността на даден субект е потвърдена чрез предоставяне на доказателство, че притежава конкретна цифрова или лична идентичност, например идентификатор и съответните идентификационни данни. Примери за идентификационни данни са пароли, еднократни токени, цифрови сертификати или цифрови подписи.

Упълномощаване – Този процес възниква в контекста на удостоверяване. След като потребителят е удостоверен, той може да бъде упълномощен за достъп до данни или системи в организацията.

Отчетност – Този компонент измерва ресурсите, които потребителят изразходва при достъп до данни или системи, например времето на достъп до системата, количеството данни, които потребителят е изпратил и/или получил по време на сесия и др. Отчетността се извършва чрез регистриране на статистическа информация по време на сесията за достъп. Тази информация може да се използва за контрол на достъпа до ресурси на организацията, таксуване, анализ на тенденциите, използване на ресурси и капацитет и планиране на дейности.

3. *„Принцип на най-слабото звено“ (Principle of the weakest link)*

Според този принцип, атакуващият се насочва към най-слабото звено в защитата. Ако то не може да бъде преодоляно се насочва към следващото по трудност звено и така до успешен резултат. Съответно най-слабата връзка ще привличат най-голям брой атаки. За целта е необходимо всички контроли за сигурност да се допълват взаимно и всеки да бъде толкова силен, колкото и другите. Този принцип се нарича още Еквивалентна сигурност (Equivalent security) или Преходна сигурност (Transitive security).

За изпълнение на гореописаните принципи, има два подхода за защита на данните и активите на организацията, които използват различни защитни модели:

1. *Периметрова защита*

Периметровата защита известна още като „модел на близалката“ се отнася до изграждането на защитен периметър около активите и гласуване на доверие на всички, които имат достъп до тях. Недостатък на модела е, че когато атакуващият преодолее външната защита, получава пълен достъп до защитаваните активи.

2. *Многослоен модел*

При многослойния модел (Фигура 4), известен още като „луков модел“ на сигурност се използват различни видове контроли за сигурност и нива на контрол, формирайки

многопластов подход за защита, осигуряващ отбрана на активите или данните в дълбочина. Налага се атакуващият да преодолява отделните слоеве на защита, за да получи достъп до защитените активи. Колкото повече са различните слоеве, толкова по-трудна ще бъде задачата му. Предимство на модела е не само по-комплексната защита, а и редуциране на риска от компрометиране на цялостната защита при отпадане на даден контрол на сигурност или слой.

1.2 Подходи за управление на информационна сигурност

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“ [48]. И двата вида са жизнено важни за ежедневната дейност на организацията и за нейното съществуване като цяло. Първостепенна задача на ИС в организацията е да защити чувствителните данни в двата вида комуникация. Подходът на ИС трябва да е съобразен и да покрива всички варианти – цялостен подход [45].

Съществуващите подходи за управление на ИС могат да се разделят на две големи групи: Подходи за информационна защита при Мрежови комуникации и подходи за защита на данни при Йерархична организационна комуникация (Фигура 3):

1. Подходи за управление на ИС при мрежови комуникации:
    - Защитна стена (Firewalls);
    - Системи за откриване на аномалии (IDS);
    - Системи за предотвратяване на проникване (IPS);
    - Защита от зловреден софтуер (Antivirus, Anti Malware);
    - Защита на крайните точки (Endpoint Protection);
    - Периметрова сигурност (Perimeter Security);
    - Системи за предварителна информация за кибер-заплахи (Cyber-threat intelligence)

Защитна стена /ЗС/

Защитната стена представлява специализиран софтуер или хардуерно устройство, следящи мрежовия трафик и притежаващо способности да го филтрира по зададени критерии, с цел предотвратяване на неоторизиран достъп до компютърни мрежи. Защитната стена е първата линия на защита между вътрешната мрежа и ненадеждни външни мрежи като Интернет [2]

Системи за откриване на аномалии /СОА/

Системите за откриване на аномалии наблюдават и анализират мрежовия трафик, търсейки аномалии и съвпадение на предварително заложени шаблони, като по този начин намират зловредни приложения или проникване в мрежата. При съвпадение подават задача към следващите системи за сигурност да елиминират заплахата [2, 3].

Системи за предотвратяване на проникване /СПП/

Системи за предотвратяване на проникване работят съвместно със СОА. След получаване на сигнал за налична заплаха те използват предварително заложени шаблони от действия за елиминиране на заплахата [2, 3, 4].

Защита от зловреден софтуер /ЗЗС/

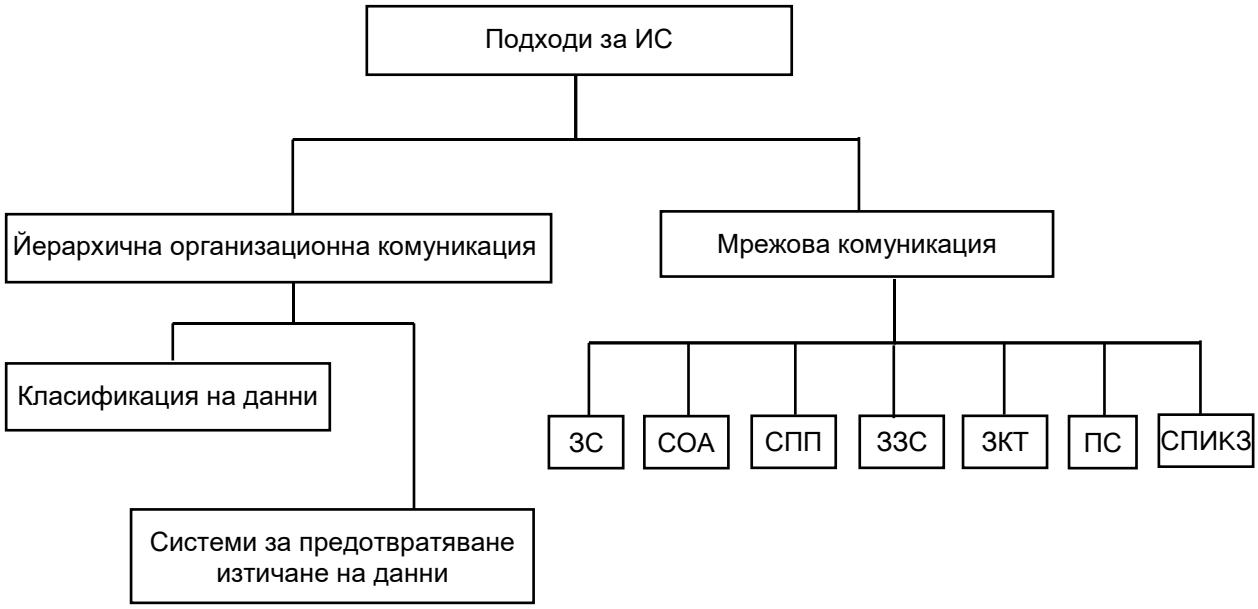
Това обикновено са софтуерни системи, сканиращи приложенията и файловете, които потребителите използват във всекидневната си дейност за зловреден софтуер – вируси, троянски коне и др., като при откриване ги елиминират [2, 3, 4].

Защита на крайните точки /ЗКТ/

Крайна точка се нарича всяко устройство, което може да обработва данни. Освен традиционните работни станции, лаптопи и сървъри тук са включени и мобилни устройства - таблети и смартфони, IoT устройства - смарт часовници, и спортни гривни и др. ЗКТ адресира осигуряване и защита на крайните точки срещу всякакви атаки и заплахи, както и изтичане на данни поради човешки грешки [3, 4]. Някои от мерките за ЗКТ включват разделяне на корпоративни и лични данни и приложения и криптиране.

Периметрова сигурност /ПС/

Периметровата сигурност е нова концепция за осигуряване на данни и ресурси в периметъра на корпоративната ИТ мрежа чрез различни системи и подходи за информационна сигурност. Най-добрите практики за периметрова сигурност включват разпознаване на заплахи, откриване и анализ на модели заплахи и атаки [4, 52].



Фигура 3. Подходи за ИС в зависимост от вида комуникация

Системи за предварителна информация за кибер-заплахи /СПИКЗ/

Системите за предварителна информация за кибер-заплахи осигуряват информация в реално време, за текущи и бъдещи кибер-заплахи, насочени към организацията. СПИКЗ събират сурови данни за възникващи или съществуващи заплахи и заплахи от редица източници – т.нар. „сензори“. След това тези данни се анализират, за да се формира цялостна картина относно текущите заплахи към организацията, извън нейния защитен периметър. Тази информация може да бъде използвана за подготовка, предотвратяване и идентифициране на кибер-заплахи към активите и данните на организацията [2, 3].

2. Подходи за управление на ИС при Йерархична комуникация в организация:
    - Класификация на данни (Data Classification);
    - Системи за предотвратяване на изтичане на данни (DLP).

Класификация на данни /КД/

Чрез класифициране на данни организациите могат да идентифицират по-точно данните, които трябва да бъдат защитени. Класификацията се извършва предварително с оглед на нейното значение за организацията и ролята на потребителя й в организацията. След това данните се маркират според предварителната чрез

визуални маркери - етикети и метаданни, който могат да бъдат използвани както самостоятелно, така и от останалите решения за ИТ сигурност като системите за предотвратяване изтичане на данни СПИД. Чрез маркирането значително се намалява риска от изтичането на чувствителни данни в организацията [52, 53].

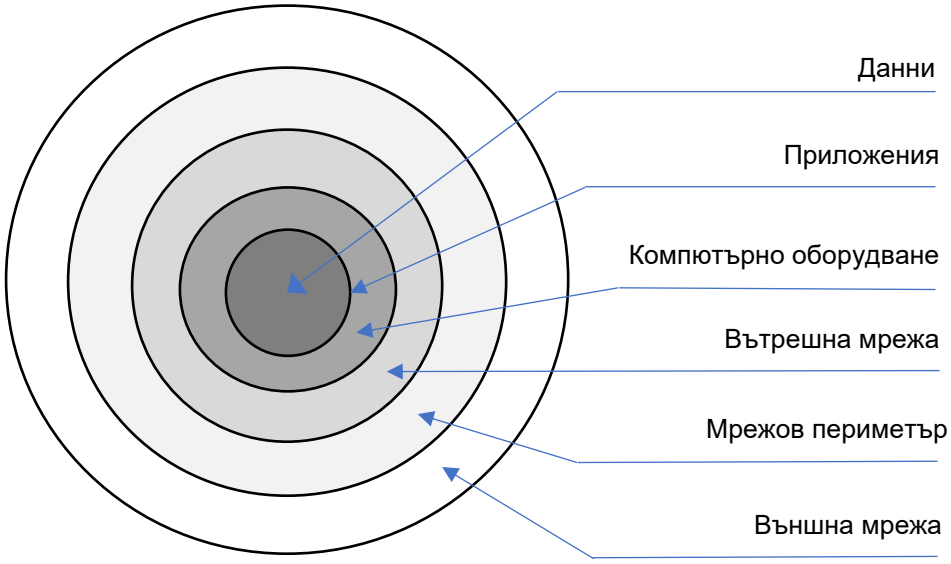
Системи за предотвратяване изтичане на данни /СПИД / [4, 5].

Системите за предотвратяване изтичане на данни представляват набор от технологии, предназначени за откриване и предотвратяване на опити за изнасяне или изтичане на чувствителни данни извън защитената мрежа на организацията. Такива данни могат да бъдат класифицирани документи, патентна информация, търговски тайни, лични данни (ЕГН, осигурителни номера, номера на кредитни карти, банкови сметки).и други [2, 4].

Подходите за управление на ИС определят начина по които се реализират целите в една СИС. Под система се разбира организирана колекция на части (или подсистеми), които са силно интегрирани за постигане на обща цел. Системата има входове, като входящите сигнали / данни преминават през определени процеси / трансформации за получаване на точно определени резултати на изхода, които заедно постигат желаната цел. Целта на СИС е обезопасяване на съществуваща информация.

1.3 Области на приложение на различните подходи за информационна сигурност

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 илюстрация може да бъде използван многослойния модел на защита (Фигура 4), състоящ се от няколко слоя:



Фигура 4. Многослоен модел на защита

Външна мрежа – Обединяващо понятие за всички външни за организацията мрежи. Такава е например Интернет. Характерно за външните мрежи е, че са незащитени.

Мрежов периметър – Граничната зона между външната мрежи и защитената вътрешна мрежа.

Вътрешна мрежа – Защитената вътрешна мрежа, в която организацията извършва своята всекидневна дейност.

Компютърно оборудване – Обединяващо понятие за сървърите, работните станции, таблети, смартфони и ИТ услуги, свързани в мрежа и използвани в организацията.

Приложения – Софтуерните приложения, инсталирани върху компютърното оборудване и използвани във всекидневната дейност на организацията.

Данни – Всички данни, използвани, обработвани и генерирани в организацията. Тук се включват и данните, собственост на организацията, но използвани от трети страни – доставчици, партньори и др.

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)

Демилитаризирана зона /ДЗ/ – Част от ИТ системите, използвани в организацията, като пощенски (e-mail) или web сървъри се нуждаят от достъп до външна незащитена мрежа като Интернет. Сегментираната част от мрежата, даваща достъп до външни мрежи и същевременно защитаваща вътрешната мрежа чрез изолиране се нарича ДЗ.

Виртуална частна мрежа /ВЧМ/ – Криптирана връзка между две точки, наричана още „тунел“. При пренасянето на информация чрез ВЧМ е невъзможно тя да бъде прихваната или подменена.

Създаване на дневници /СнД/ – Система за създаване на дневници (логове), регистрираща всяка извършена операция и записваща я в определен формат.

Одит - Дейности като инспекция или проверка, на процес или система за качество, за да се гарантира спазването на изискванията. Одитът може да се прилага за цяла организация или може да е специфичен за функция, процес или производствен процес.

Тестове за проникване /ТП/ – известни са още като „етично хакерство“. Те представляват комплекс от упълномощени симулирани кибер-атаки върху компютърни системи, сървъри и мрежи на организацията, за извършване на оценка на сигурността и издаване на препоръки за подобряването ѝ.

Анализ на уязвимости /АУ/ - Процес на анализ на уязвимости, даващ основа и отправна точка за оценка на различни мерки за намаляване на уязвимостите.

Сървър – посредник /СП/ – сървър, действащ като посредник при заявки от клиенти, търсещи даден ресурс от сървъри, които предоставят нужните ресурси, маскирайки истинския произход на заявката.

Пакетна филтрация /ПФ/ - Филтрирането на пакети е процесът на управление на потока от пакети въз основа на атрибути като IP адреси на източника, IP адреси на местоназначение, тип, дължина и номер на порт.

Статична пакетна филтрация /СПФ/ - Статично филтриране на пакети чрез конфигуриране на избрани портове като постоянно отворени или постоянно затворени.

Динамична пакетна филтрация /ДПФ/ - Динамичното филтриране на пакети осигурява подобрена защита, като позволява на избраните портове да бъдат отворени в началото на легитимна сесия и след това затворени в края на сесията, за да се осигури портът срещу опити за неоторизиран достъп.

Хеширане на пароли /ХП/ - Това е математическа операция, извършвана върху даден низ, която е лесна за изпълнение, но много трудна за обратно възстановяване. Хешовете не са предназначени да бъдат декодирани, а само да осигурят еднопосочно кодиране. При ХП се създава хеш на въведената парола, а самата парола не се съхранява в явен вид. При въвеждането на парола от потребителя се създава нов хеш,

които се сравнява с вече запазения и при съвпадение имаме вярна парола. Така при пробив паролите не могат да изтекат.

Филтриране по съдържание – Предотвратява на достъпа до определени компоненти, които могат да бъдат опасни за сигурността, ако са достъпни. Най-често това са изпълними файлове, електронни писма или уебсайтове.

Валидация на данни /ВД/ – Процес на проверка на целостта и валидността на данните, които се въвеждат. Чрез него се осигурява безпроблемна работа на дадена система и се избягва наличието на уязвимости, свързани с недокументирани формати на данните.

Криптиране - Процес на кодиране на информация по такъв начин, че само лицето притежаващо ключа, чрез които е кодирана, може да я декодира.

Контрол на достъп / КоДо/ – Комплекс от мерки за сигурност, чрез които се регулира достъпа до ресурси в изчислителна среда според предварително дефинирани правила за достъп на различните потребители.

Архивиране на данни / АД/ – Процес на създаване и съхранение на резервно копие на данни, така че да е възможен процеса на възстановяване на оригинала след събитие, водещо до загуба на данни.

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

При разработване на ефективни системи за информационна сигурност е необходимо доброто познаване на редица научни и научно приложни области като:

- Информационна и Кибер-сигурност;
- Проектиране на системи;
- Анализ на данни;
- Големи масиви от данни
- Машинно самообучение;
- Изкуствен Интелект;
- Софтуерно инженерство;
- Системен анализ.

Информационна и Кибер-сигурност;

Информационната сигурност осигурява Поверителност, Цялостност и Наличност на информация, която може да бъде дефинирана като "чувствителна“ за организацията, независимо дали е в цифров формат или аналогова форма. Цифровата информация обикновено се манипулира от микропроцесори (персонални компютри, сървъри), съхранява се върху магнитни, оптични или дискови носители (магнитни ленти, DVD, твърди дискове и флаш-памети) и се предават по електронни канали (локална мрежа, Интернет). Информацията може да е и в аналогов формат, например в печатна форма. Информационната сигурност има за цел да защити информацията, която предоставя стойност на хората и организацията.

Кибер-сигурността е състояние на кибер-пространството, определяно от нивото на конфиденциалност, интегритет, достъпност, удостоверяване и отказоустойчивост на информационните ресурси, системи и услуги. Кибер-сигурността се основава на ефективно изграждане и поддръжка на активни и превантивни мерки[55, 56, 57, 60, 134].

Проектиране на системи

При проектиране на системи има два основни подхода: „отдолу-нагоре“ и “отгоре-надолу”. За проектиране на СИС ние използваме втория подход, които осигурява

единна политика за информационна сигурност, процедури и процеси, чрез които да се постигнат очакваните резултати. Този подход отчита изискванията на всички заинтересовани страни.

Анализ на данни. Анализа на данни е процес на събиране, анализиране и трансформиране на данни за откриване на полезна информация, скрита в тях, за да се стигне до заключения и решаване на проблеми.

Големи масиви от данни

Областта на големите масиви от данни се свързва с адресиране на проблеми за събиране, съхранение и анализ на големи количества сложни данни или набор от данни, процесите на изследване, трансформиране и моделиране, както и съответните инструменти [46, 113].

Машинно самообучение (МСО)

Машинното самообучение разглежда използването на алгоритми за трансформиране на емпирични данни в използваеми математически модели. То се основава на обработка на набори от данни и опити за откриване на причинно-следствени променливи. Чрез МСО е възможно идентифицирането на основни модели на поведение на дадена система. Едно от основните приложения в информационната сигурност е откриване на аномално поведение в системата, причинено от външни атаки, както и прогнозиране на бъдещи такива [57, 60].

Изкуствен Интелект (ИИ)

Изкуственият интелект е клон на компютърните науки, който се занимава с автоматизиране на интелигентно поведение и изграждането на интелигентни машини, способни да изпълняват задачи, които обикновено изискват човешки интелект [47, 63]. Една от целите на ИИ е, при общуване на човек с неизвестен субект, да не може да се различи дали субекта е друг човек или компютър. Ако остане с впечатлението, че е общувал с човек, но всъщност това е бил компютър, то тогава компютърът проявява изкуствен интелект [62]. Стремежът е репликиране или симулиране на човешкият разум в машина. ИИ е интердисциплинарна наука с множество подходи, част от които са машинното самообучение, задълбоченото обучение (Deep Learning), Големите масиви от данни и др..Раздел от ИИ са мулти-агентните системи [51].

Софтуерно инженерство

Софтуерното инженерство е системен подход към анализ, проектиране, оценка, внедряване, тестване, поддръжка и ре-инженеринг на софтуер. В този подход се дефинират модели за жизнения цикъл на софтуера, и се използват методологии за определяне и оценка на различните фази на модела на жизнения цикъл [63]. На Фигура 5 е показан цикъл на разработване на софтуерни системи, които успешно може да се приложи към проектирането на СИС. Saltzer и Schroeder [61] описват основен набор от принципи на защита на информация в компютърни системи, които осигуряват добра основа за проектиране на СИС [61].

Системен анализ

Целта на системния анализ е да се определи проблема, решаван от системата, какво трябва да бъде проектирано и реализирано, защо е необходимо, да се направи оценка на стойността и да се определят съответните приоритети на процеса на разработване, за да се удовлетворят изискванията към системата [57, 58, 59]. Той е във връзка с процеса на разработване на системи, описан на Фигура 5 и се състои от няколко основни компонента и връзки между тях, които се разглеждат в контекста на разработване на СИС:

- Проблемна област - дефинира областта в която се решава проблема на СИС;

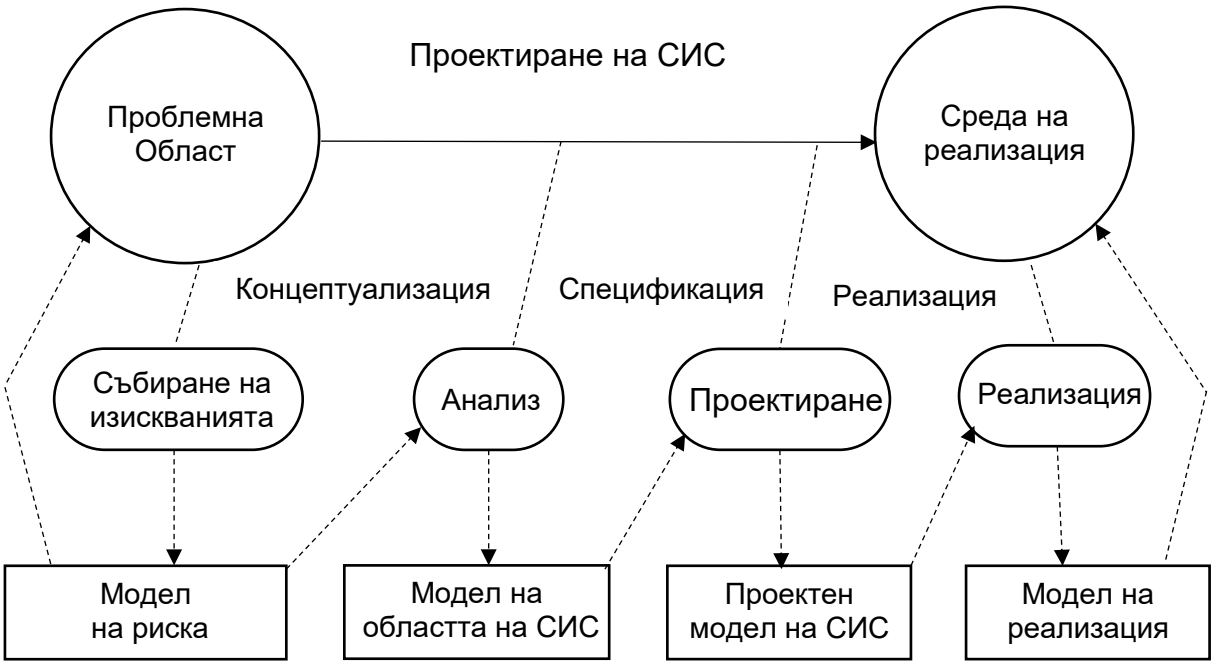
- Проблем - реализация на определен начин на функциониране на СИС, която трябва да заработи в дадена среда;
- Среда на реализация - представлява условията при които се реализира СИС;
- Етапи - Това са етапите през които трябва да премине разработването на СИС;
- Създаване на модели на СИС на различни етапи от разработването;
- 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:

- 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 на 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.

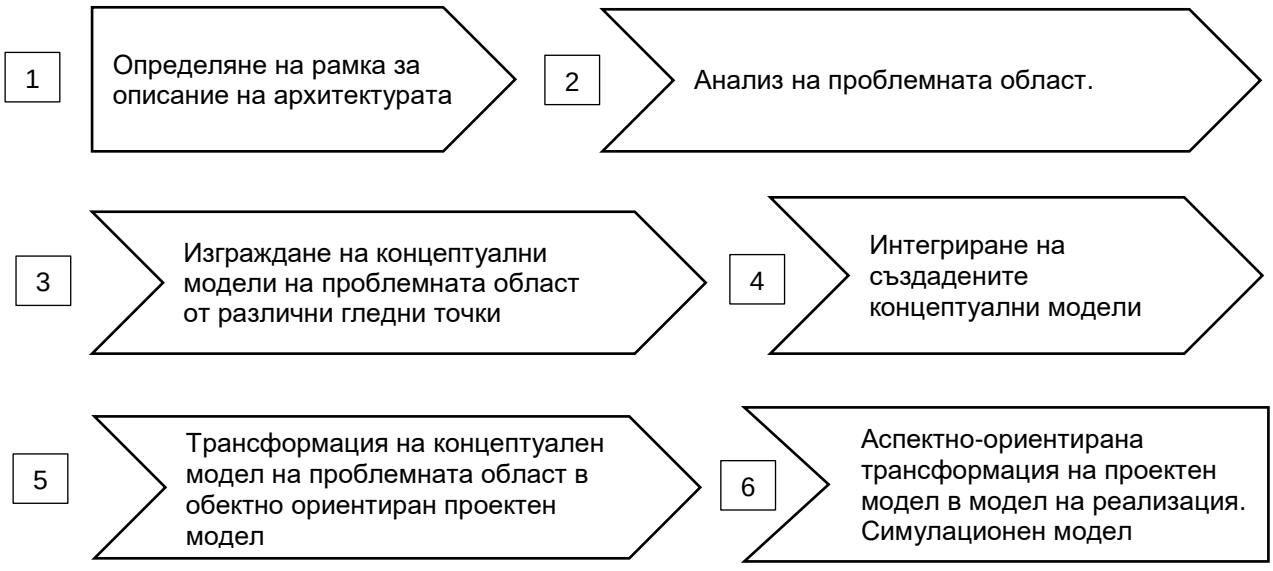
2. Анализ на проблемната област на СИС, за определяне на изискванията към системата от различни гледни точки. На базата на този анализ се формират изискванията към СИС.

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.

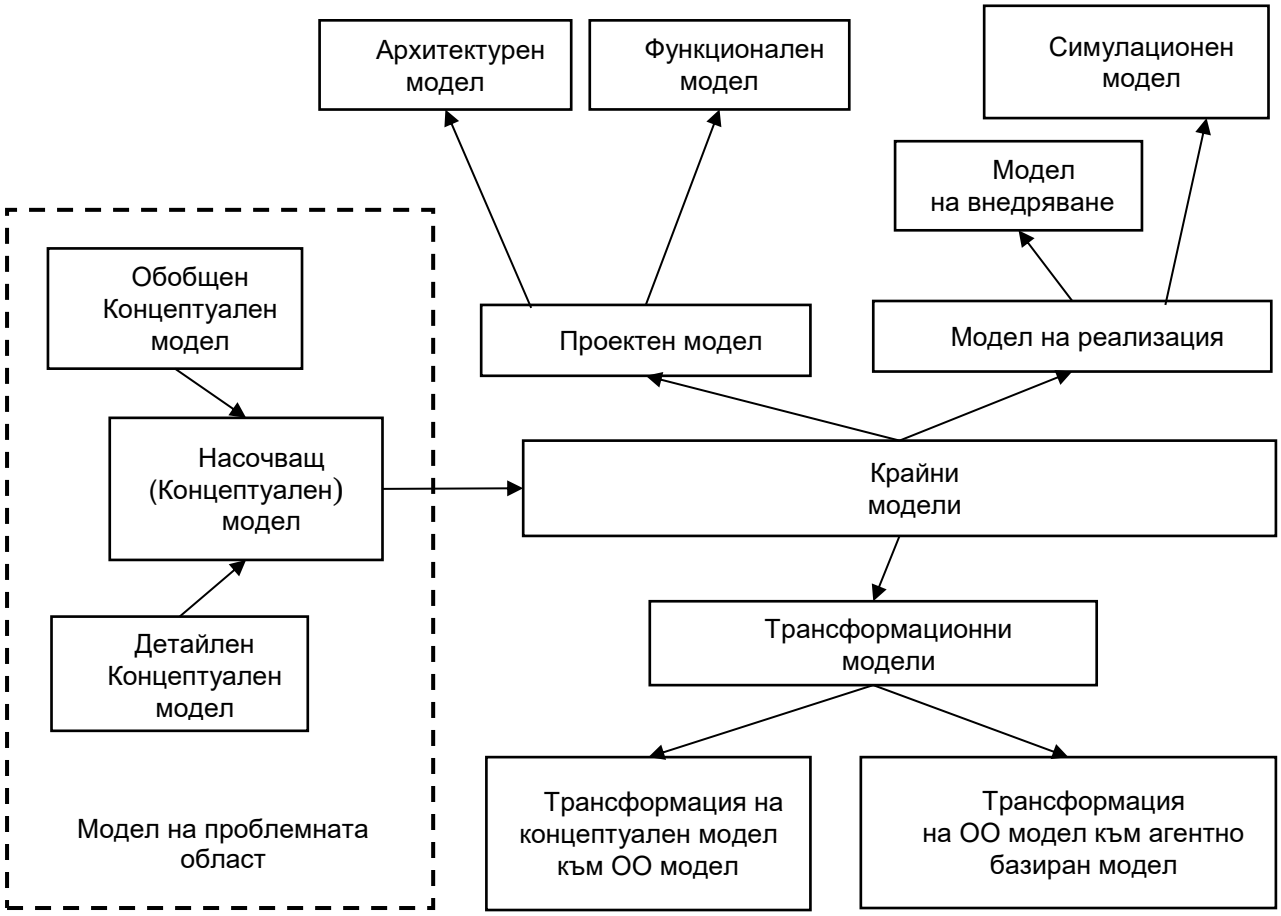
5. Трансформация на концептуален модел на проблемната област в обектно ориентиран проектен модел.

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



Фигура 6. Метод за разработване на СИС

Моделите, които се конструират при прилагане на метода са показани на Фигура 7 [135,136]. На базата на анализ на проблемната област е конструиран 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 7. Модели за разработване на СИС

На неговата база, след съответна трансформация са създадени 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 платформи, представляващи среда 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, са представени трансформациите между моделите - "Трансформация на концептуален модел към ОО модел" и "Трансформация на ОО модел към агентно базиран модел".

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].

Стандарт IEEE 1471 представлява препоръчителни практики относно създаване, анализ и поддържане на архитектури на софтуерно интензивни системи и тяхното архитектурно описание. Той предлага концептуална рамка за архитектурно описание и се дефинира съдържанието на архитектурно описание.

Стандарт ISO/IEC/IEEE 42010:2011 адресира създаване, анализ и поддържане на архитектури на системи чрез архитектурни описания. Създава се концептуален модел и се уточнява съдържанието на описанието на архитектурата. Въвежда се рамка за описание на архитектурата, която включва гледни точки, езици за описание и общи практики за описание на архитектурата на системата.

Тези стандарти въвеждат понятия, свързани с начина на описание на архитектурата на една система [67]:

Околна среда (Environment). Системата е разположена в околна среда. Тя определя съвкупността от влияния и въздействия върху системата през целия й жизнен цикъл, включително технологични, бизнес, оперативни, организационни, политически, икономически, правни, регулаторни, екологични и социални. Средата на системата може да съдържа други системи.

Изглед (View). Всеки изглед обхваща една или повече области на интерес на различните заинтересовани страни към системата. Той представя системата като свързан набор от проблеми в съответствие с правила и конвенции, дефинирани в гледната точка.

Гледна точка (Viewpoint). Гледната точка се определя като спецификация на правила за изграждане и използване на различни изгледи. Това може да бъде модел или шаблон за създаване на различни изгледи чрез установяване на цели и техники за тяхното проектиране и анализ [66].

Заинтересована страна (Stakeholder) - физическо лице, група, организация или комбинация от тях, имащи интерес към функционирането на дадена система.

Област на интерес (Concern) – интересът към системата на дадена заинтересована страна от дадена гледна точка. Тя се отнася до съвкупността от влияния и въздействия върху системата през целия й жизнен цикъл.

Архитектура на системата (System Architecture) - основни понятия или свойства на системата в нейната околна среда, изразени чрез нейните елементи, взаимоотношения и принципите на нейното проектиране и развитие. Архитектурата на една система представлява съществената за нея, разглеждано във връзка с нейната околна среда. Няма строга характеристика на това, което е съществено за системата. Тази характеристика може да се отнася до един, няколко или всички от изброеното:

- Системни компоненти;
- Подредба или взаимна връзка на системните компоненти;
- Принципи за организация и проектиране на системата;
- Принципи, регулиращи развитието на системата през нейния жизнен цикъл.

Архитектурно описание (Architectural description). То се определя като набор от средства или продукти, служещи за документиране на архитектурата на системата. Архитектурното описание се съставя от един или няколко изгледа и е част от проектния модел. Докато архитектурата на системата е концептуална, то начина на описание на тази архитектура е напълно конкретно.

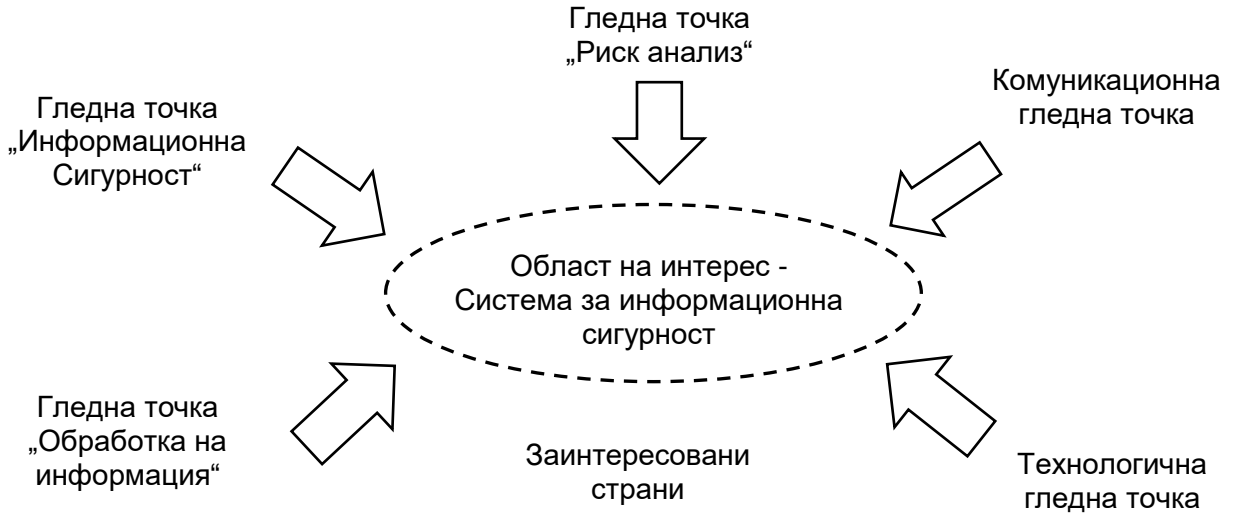
Рамка на създаване на архитектурно описание (Architectural framework) - конвенции, принципи и практики за описание на архитектури, създадени в конкретна област на приложение и общност от заинтересовани страни.

Архитектурен изглед (Architectural View) - набор от средства или продукти, изразяващи архитектурата на системата от гледната точка на специфични проблеми, решавани от системата.

Архитектурна гледна точка (Architectural Viewpoint) - набор от средства или продукти, установяващи принципите за изграждане, интерпретиране и използване на архитектурни изгледи на специфични проблеми, решавани от системата.

Вид на модела (Model kind) - Конвенции за моделиране, включващи диаграми на потоците от данни, диаграми на класове, организационни диаграми и модели на преходи на състоянието.

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.



Фигура 8. Област на интерес на СИС

Разработването на комплексни системи задължително 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 разработването 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 разработване на системи за информационна сигурност в организации. 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 поддържаните платформи и технологии, както и различни подходи при информационните и комуникационни технологии като обектно-ориентиран подход и агентен подход,
- 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.

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

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

2.1.1 Основни понятия в информационната сигурност

На Фигура 9 е представен фундамента на областта на информационната сигурност, описан чрез нейните основни понятия.

„Събитие“ (Event) –Значителна съществена промяна на състоянието. Евентуално може да бъде нормална промяна на състоянието, различна от отрицателна промяна, или отказ на хардуера [2].

„Сигнали (Signals) / Аларми (Alarms)“ - започват като събития, които са достатъчно критични, за да изискат внимание [2].

„Инцидент“ (Incident) - Събитие, компрометиращо Целостта, Поверителността или Наличността на информационните активи.

„Нарушение“ (Breach) - Инцидент, който води не само до потенциална експозиция, а до потвърдено разкриване на данни към неоторизирана страна [5, 6].

„Уязвимост“ (Vulnerability) е слабост в проектирането, изпълнението, експлоатацията, вътрешните правила и процедури или вътрешните контроли на съответния актив, или система, която се използва от източник на заплаха за постигане на определени цели - пробив в сигурността или нарушение на процедурите за сигурност[1, 6, 12, 29].

„Заплаха“ (Threat) е възможността източника на заплаха случайно или умишлено да експлоатира конкретна уязвимост, което да доведе до пробив в сигурността, унищожаване на данни, прекъсване на услуги или нарушение на процедурите за сигурност [1, 3, 7, 16].

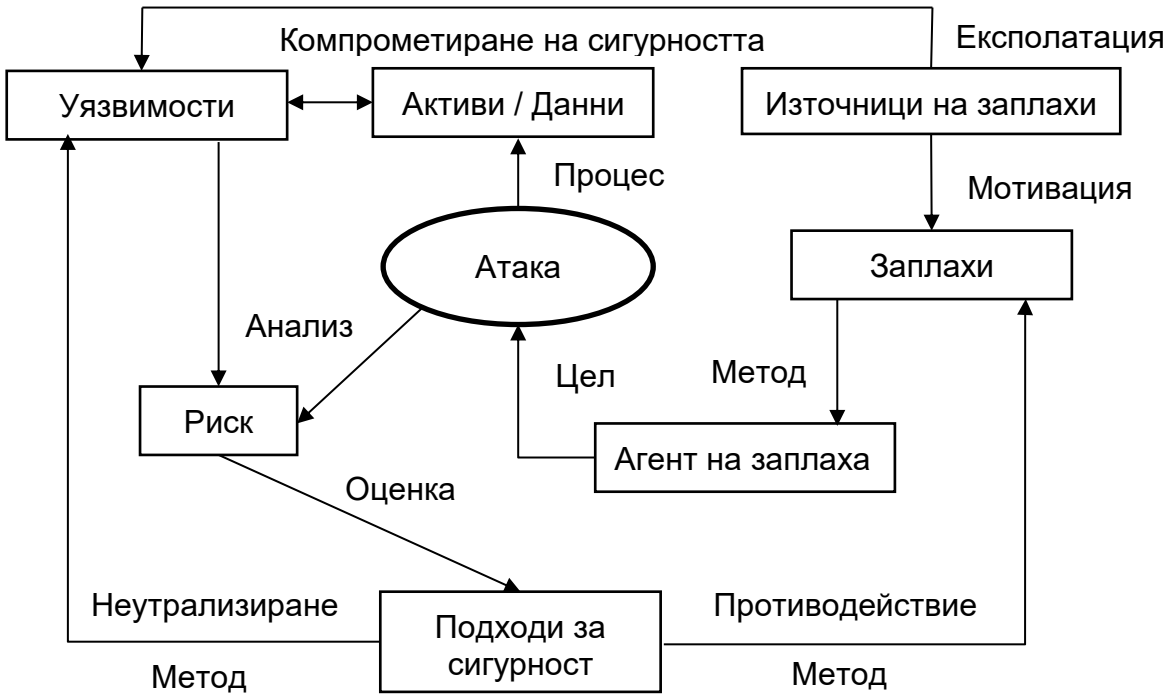
„Агент на заплаха“ (Threat Agent) – Агент на заплаха е всяко лице, което действа или има силата да действа, да причинява, пренася, предава или поддържа заплаха [25].

„Източник на заплаха“ (Threat Source) - Причинител на заплаха за информационна сигурност [25].

„Атака“ (Attack) – Всеки опит да се разкрие, промени, открадне, унищожи, да се получи неоторизиран достъп до или неоторизирано да се използва информационен актив, чрез целенасочено действие, при което се експлоатира конкретна уязвимост от източника на заплахата и се осъществява нарушение в сигурността, водещо до инцидент, свързан със сигурността [6, 7].

„Изтичане на данни“ (Data Breach) - е инцидент, свързан със сигурността, при който чувствителни, лични или поверителни данни са достъпени, копирани или трансферирани от неоторизирана страна. Изтичането на данни е заплаха с висок риск и води до сериозни загуби от финансов, технологичен или репутационен характер за пострадалата страна. То може да бъде причинено от целенасочени атаки, човешки грешки, уязвимости на приложенията или даже от лоши практики за информационна сигурност.

Загуба на данни“ (Data Loss) - Липсващи или повредени данни, в резултат на природни бедствия (наводнения, земетресения), човешки грешки като случайно изтриване на файлове или събития като повреда на твърдия диск, прекъсване на захранване,



Фигура 9. Уязвимости, заплахи и атаки

инфектиране със зловреден софтуер и други. За избягване на загубата на данни се използват различни методи като периодично архивиране на данни, дислокация (разполагане на архивите на различни локации, включително в облака) или други.

2.1.2 Уязвимости. Заплахи. Източници и агенти на заплахата

„Уязвимости“

Уязвимостите са слабости, от които се възползва източника на заплаха, за да проведе успешна атака и да навреди на информационните активи (Фиг. 9) [29]. Уязвимостта може да е конкретна операционна система; приложение, което потребителите използват; физическо място, на което се намира офис сградата или центъра за данни; обслужващи системи, - климатични и вентилационни инсталации; системи за безопасност – алармена или противопожарна система; липса на резервни генератори или източници на захранване и много други фактори като слабости в проектирането, човешки фактор, системна среда, неефективни политики за сигурност. Може да се създаде списък с тези фактори, например на уязвимостите, свързани със системната среда – “системни уязвимости”, които биха могли да бъдат използвани от потенциалните източници на заплаха [16]. Фрагмент от подобен списък е показан в Таблица 2. Колкото по-пълен е списъка и колкото повече фактори сме взели предвид толкова по-ефикасна ще бъде и защитата на активите и ресурсите.

Уязвимост	Източник на заплахата	Възможен резултат
Системни идентификатори (потребителски имена и пароли, валидни цифрови сертификати) на напуснали или уволнени служители не са премахнати, а	Напуснали / уволнени служители	Възможен е пълен несанкциониран достъп до ресурсите на организацията.

правата за достъп (оторизацията) не са променени.		
Защитната стена позволява входяща сесия с активен акаунт за гости.	Неоторизирани потребители (хакери, бивши служители, кибер-престъпници, терористи).	Вход в системата чрез активен акаунт за гости и получаване на достъп до системните файлове на сървърите.
Макар че са известни конкретни уязвимости в сигурността на дадена система, тя не е актуализирана.	Неоторизирани потребители (хакери, бивши служители, кибер-престъпници, терористи).	Получаване на неоторизиран достъп до системата и до чувствителна информация, на базата на известни системни уязвимости.
В център за данни се използват водни пръскачки като част от противопожарната инсталация, но не са монтирани защитни платна (брезенти) за защита на хардуера и оборудването от водата.	Пожар, Унищожаване на оборудването от водните струи, Небрежни служители.	Водни пръскачки могат да бъдат включени дистанционно от хакери.

Таблица 2. Уязвимости и източници на заплаха

„Заплахи“

При заплаха има възможност източникът на заплаха случайно или умишлено да експлоатира конкретна уязвимост, което да доведе до пробив в сигурността и застрашаване на информационни активи. Заплахите, свързани с информационната сигурност са специфични и зависят от особеностите на средата, източника и агента на заплаха. За пример може да се посочи вирус, проектиран за Windows среда, които няма да има никакъв ефект в Linux или MacOS среда. Заплахите са свързани с конкретни уязвимости, чрез които може да се осъществи атаката върху информационни активи. Ако определена уязвимост е неутрализирана, например чрез актуализиране на операционната система посредством последните осъвременявания на сигурност, адресиращи известните до момента уязвимости, източниците на заплахите нямат среда, която да експлоатират и съответно да извършат успешна атака. Така заплахите се елиминират или редуцират още в началната фаза [29].

Заплахите могат да варират според своя характер, посока, източник и резултат. За ефективно противодействие трябва да се вземат в предвид редица фактори [1,11]:

- Източници и агенти на заплахата и тяхната мотивация;
- Вектор на заплахата;
- Цели на заплахата;
- Тип на атаката;
- Характер на заплахата;
- Въздействие на заплахата.

Оценката на заплахите е важна част от анализа на риска. Чрез идентификация на заплахите, се намалява вероятността от пренебрегване на важни активи, които в противен случай могат да останат незащитени.

„Източници“, „Агенти на заплахата“. Мотивация.

Агент за заплаха е всяко лице, група, организация или процес, което действа или има силата да действа, причинява, пренася, предава или поддържа заплаха. Агентите на заплаха използват една или повече уязвимости за да постигнат целта си: атака с потенциал да причини вреда – изтичане или увреждане на данни или системи, поемане на контрол и експлоатиране на определени информационни канали или активи, блокиране на нормалната функционалност и др.[1, 11, 16, 29]

Мотивацията и ресурсите за извършване на атаки дефинират хората като потенциално опасни източници на заплаха. В Таблица 3 са представени често срещани източници и агенти на заплаха, тяхната мотивация и методите (действията) на заплахите.

Някои от типичните агенти на заплахи в киберпространството са:

Хакери и Хактивисти. Хактивизмът е нова тенденция при агентите на заплахата. За разлика от хакерите, търсещи финансова изгода или целящи компрометиране или унищожаване на ИТ ресурсите на организацията, хактивистите са политически или социално мотивирани лица, които използват компютърни системи, за да протестират и насърчаване на тяхната кауза. Тяхна цел обикновена са публични уебсайтове, разузнавателни агенции и военни институции.

Кибер-престъпници. Тези агенти на заплаха са високо квалифицирани и враждебни по природа. Тяхната мотивация е финансова Те може да са организирани на местно, национално или дори международно ниво.

Терористи. Тяхната мотивация може да бъде политическа или религиозна. Предпочитаните цели на кибер-терористите са предимно обекти от критичната инфраструктура (транспорт, енергийна система, телекомуникации и др., които да предизвикват сериозно въздействие върху обществото и правителствата).

Агент на заплахата	Мотивация	Методи на заплахата	Вид на организацията
•Хакери; •Хактивисти	•Предизвикателство; •Егоизъм; •Отмъщение.	•Хакинг; •Социален инженеринг; •Проникване в системата; •Неоторизиран достъп.	•Търговска; •Производствена; •Научна; •Административна; •Публична;
Кибер-престъп-ници	•Унищожаване на информация; •Нелегално Разкриване на информация; •Печалба; •Неоторизирана промяна на информация с цел заблуда.	•Компютърно престъпление; •Кражба на самоличност; •Прихващане на данни; • Измама; •Злоупотреба с информация; •Проникване в системата.	•Търговска; •Производствена; •Административна; •Публична.
Терористи	• Изнудване; •Унищожаване на активи; • Експлоатация; • Отмъщение.	•Бомба / Тероризъм; •Информационна война; •Системна атака (DDoS); •Проникване в системата; •Фалшифициране	•Търговска; •Производствена; •Научна; •Административна; •Публична.

		на системата (System tampering).	
Корпорации	•Осигуряване на предимство; •Икономически шпионаж.	•Кражба на информация •Вмешателство •Социален инженеринг •Проникване в системата •Неоторизиран достъп до чувствителна информация.	•Търговска; •Производствена; •Научна.
Недобро-съвестни служители	•Любопитство; •Егоизъм; •Шпионаж; •Печалба; •Отмъщение; •Неумишлено; •Пропуски (напр. въвеждане на данни, грешка в кода).	•Нападение над служител; •Изнудване; •Компютърна злоупотреба; •Измами и кражба; •Фалшифициране на данни; •Прихващане на данни; •Зловреден код (вирус, троянски кон); •Продажба на данни; •Системни грешки; •Проникване; •Саботаж; •Неправомерен достъп.	•Търговска; •Производствена; •Административна; •Публична.

Таблица 3. Източници, мотивация и методи на заплахи в организации

Корпорации. Това са корпорации, организации или предприятия, които възприемат или участват в кибер-атаки. Тяхната мотивация е да изграждане на конкурентно предимство, придобиване на чувствителна информация, ноу-хау, финансова информация и др. Този тип агенти на заплаха притежават значителни ресурси от технологично и човешко естество, особено в своята област на експертиза.

Недобросъвестни служители . Това са служители на организацията, имащи достъп до нейните ресурси и злоупотребяващи с тях. Мотивацията им е различна - небрежност, недоволство, злонамереност, финансова облага и др. Този вид агенти са особено ефективни, поради факта че традиционната защита обикновено е насочена за атаки отвън-навътре, а служителите вече се намират в защитената среда, т.е. те са преодолели част от защитите. За ефективна защита от този вид агенти на заплаха се използват нови и съвременни методи, реализирани чрез платформи за реализация от типа СПИД, както и идентифициране на рисковите потребители и вземане на мерки за ограничаване на техния достъп до критична информация или системи.

Правителства. Тези агенти на заплаха разполагат със значителни потенциал. Тяхната мотивация може да бъде икономическа или гео-политическа - доминиране в определени сектори, осигуряване на стратегическо предимство, прокарване на собствени интереси и др.

Подробна информация за агентите на заплаха може да бъде открита в специализирани списъци и библиотеки като Intel Threat Library, VERIS Threat Agent Categories, FAIR Threat Communities, OWASP Threat Agent Groups и NIST Threat Sources [25].

Организациите, обект на кибер-заплахи могат да бъдат от различен размер и с различен профил – търговска, производствена, научна, административна или публична, всяка от които има специфики и различна степен на защита и уязвимост. Различните организации боравят с различни данни и имат различни разбирания за

чувствителността на тези данни. По-подробно темата е разгледана в т. 2.5 Обработка на информация

2.1.3 Вектори, цели и характер на заплахата

Векторът на заплахата се определя от източника на възникване на заплахата и пътя за достигане до целта и - например външна атака от хакер към корпоративна мрежа, електронно писмо със зловреден код, изпратено до конкретен служител. За улесняване идентифицирането на потенциални вектори на заплаха можем да съставим списък с различни типове заплахи, източникът им и тяхната цел (Таблица 4).

Поради комплексния характер на съвременните заплахи, както и резултатите от тяхното действие, са възможни различни и дори произволни комбинации от заплахи, източници и цели от Таблица 3, описващи реални или хипотетични, но напълно възможни заплахи и тяхната посока. За да се противодейства успешно на заплахите или да се минимизира резултата от тяхното действие, е особено важно да се направи анализ, отчитащ всички възможни елементи и тяхното въздействие. Само тогава може да се предвидят и използват ефективно подходящите контра-мерки. Анализът на заплахите дава и точна картина към ръководството на организацията за необходимостта от заделяне на ресурси (финансови и човешки), както и за създаване и поддържане на ефикасна политика за информационна сигурност. Тази информация е необходима и за постигане на съвместимост с важни за работата на организацията законови рамки, регулации и стандарти.

Според вектора заплахите могат да се класифицират на външни и вътрешни.

Заплаха	Източник	Цел
Кражба	Служител	Интелектуална собственост
Експозиция	Консултант	Лични данни (PII)
Загуба	Доставчик	Търговска тайна
Неоторизирана промяна	Системен интегратор	Здравна информация (PHI)
Частично изтриване	Риселър	Номера на кредитни карти
Пълно изтриване	Доставчик на услуги	Финансова информация
Непозволено добавяне	Доставчик	Номера на социални
Измама	Хигиенен персонал	осигуровки
Шпионаж	Инсайдър	Документ
Подправяне на	Външна поддръжка	Данни
самоличност	Терорист	Компютър
Отказ на услуга	Интернет атака	Мрежа
Неизправност	Софтуерен бъг	Операционна система
Грешка	Malware	Приложения
Злоупотреба	Инцидент	Гласова комуникация
Прекъсване	Естествени причини	Поверителност
Нараняване	Време	Здраве и безопасност
Физическа опасност		Продуктивност

Таблица 4. Типове заплахи

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 хакерските атаки, DoS атаките [25].

„Червеи“ (Worms) и „Троянски коне“ (Trojans)

Червеят представлява злонамерен изпълним код, имащ способността да се репликира и разпространява чрез използване на системните уязвимости на тяхната цел. *Троянският кон е* злонамерен изпълним код, които скрито се инжектира в потребителските системи и осигурява неофициален и несанкциониран достъп до тях чрез т.нар. *задна врата – трояски коне с отдалечен достъп (RATs)* или такива които имат за цел кражба на потребителски и идентификационни данни. Тези две заплахи са класически злонамерен софтуер и са широко разпространени в киберпространството. Примери за такива заплахи са Conficker, Win32/Autorun, Trojan.AutorunINF.Gen, Win32.Worm.Downadup и Exploit.CplLnk [21, 23, 25].

„Бот-Мрежи“ (Botnet)

Бот-мрежите са клъстери от свързани компрометирани компютърни системи, намиращи се под контрола на нападателя. Тези системи са заразени със зловреден софтуер и се наричат ботове или „зомбита“. Бот-мрежите представляват плацдарм за многократно използване от които се атакуват целите. Те се управляват от главен бот (Master bot), който разпределя задачите между различните групи или индивидуални ботове [39]. Бот-мрежите могат да бъдат използвани за спам, кражба на информация, DDoS атаки, заразяване на други системи и разпространяване на зловреден код (Malware) [25, 36]. Примерни Бот-мрежи са комерсиалния „ZeuS crimeware toolkit“ [38], Darkness [40], BlackEnergy [41], GhostNet [42], Shadow Network [43] и Stuxnet [44].

„Атаки за отказ на услуга“ - DoS и DDoS атаки

При атаки за отказ на услуга (*DoS*) имаме опит даден ресурс или услуга, предоставени на потребителите да бъдат направени недостъпни за тях. Цел на тези заплахи са бази данни, интернет информационни сайтове, онлайн платформи за търговия, портали и онлайн услуги. При варианта Distributed denial-of-service (DDoS) атаката се извършва от повече от един източник, обикновено Бот-мрежи, съставени от десетки, стотици и дори хиляди ботове, работещи върху компрометирани машини. По команда ботовете заливат целевата жертва с трафик или информация, докато услугата спре да работи и стане недостъпна. Това става чрез изчерпване на пропускателната способност на канала или чрез изчерпване на изчислителните ресурси на сървъра [21, 23, 25, 26, 35]. Примери за такъв вид заплахи са Smurf Attack, SYN Flood и Teardrop [36].

„Заплаха тип Drive-by Exploits“

В основата на този тип външна заплаха е инжектирането на злонамерен код в HTML кода на уеб сайтове, с които се експлоатират уязвимости в уеб браузърите. Целта на тези заплахи са уеб браузъри, плъгини за тях и операционната система на потребителския компютър. Заразяването става автоматично при посещението на заразения сайт, дори без никакво взаимодействие с потребителя [25].

Такъв тип заплаха е например Black Hole [34]

„Инжектиране на код“ (*Code Injection Attacks)*

Тази категория заплахи включва техники за атака срещу уеб приложения като SQL Injection (SQLi), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Remote File Inclusion (RFI) и др. Цел на атакуващите чрез този метод е кражба на идентификационни и чувствителни данни, чувствителни данни, придобиване на контрол върху сървъри чрез използването на уязвимости на уеб приложения [25, 37].

Примери за такъв тип заплахи са кампании като LizaMoon [38].

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. Поради своя характер, вътрешните заплахи на практика са непредсказуеми и представляват сериозно предизвикателство за традиционните мерки за ИТ сигурност [9]. Съществуват множество причини за инциденти, свързани с вътрешни заплахи:

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

Вътрешните заплахи могат да се разделят на няколко основни групи според техния източник:

“Човешка заплаха”

Във всекидневната си работа служителите могат да проявят небрежност, водеща до инцидент със сигурността, да станат обект на хакерска атака или напълно умишлено да причиняват вреди. Те се превръщат в сериозна вътрешна заплаха ако имат достъп до чувствителна информация или достъп до критични за сигурността на организацията системи. Затова е важно да се класифицират различните типове потребители профилирани според риска, които те носят за организацията. Могат да бъдат различени следните категории от служители:

- Външни доставчици - Външни за компанията доставчици, имащи достъп до нейните ресурси;
- Привилегировани потребители – потребители с пълен достъп до ресурсите на организацията, например системни администратори;
- Обикновени потребители с достъп до чувствителни данни.

Обикновените потребители представляват по-голям риск за сигурността на организацията от привилегированите, поради по-големия им брой (обикновено 20-30:1), водещ до сумарно по-висок риск за сигурността. Друга причина е липсата на знания и умения за предпазване от инциденти [9].

Активност на потребителите

Многообразната всекидневна активност е най-разпространеният вектор на вътрешната заплаха. Поради огромния брой на действията и операциите, извършвани от служителите в нормалния работен процес, е изключително трудно да се установят неоторизираните или рискови дейности. От първостепенна важност е организацията да бъде снабдена с инструментариум, отчитащ и блокиращ тези дейности с цел намаляване на риска от изтичане на чувствителна информация чрез вътрешни или външни атаки [9].

Бизнес-приложения

Заради достъпа си до чувствителни данни, бизнес-приложенията, използвани от служителите на всекидневна база са сериозен източник на рискове. Освен специализираните приложения, във всекидневната работа е наложително използването на помощни приложения - облачни услуги, споделяне на десктоп с цел обучение (webinars), трансфер на файлове, peer-to-peer споделяне на файлове (торенти) и много други. Те са директен източник на висок риск за организацията [9].

2.1.4 Атаки и противодействие

“Атака” имаме когато източникът на заплаха извършва целенасочено действие, при което се експлоатира конкретна уязвимост, за компрометиране на сигурността на даден актив чрез разкриване, промяна, кражба, унищожаване, получаване на неоторизиран достъп или неоторизираното му използване. Атаката е процес, последователност от изпълними действия (Фигура 9). За да може да се неутрализира е необходимо да се извърши анализ на условията и компонентите от които зависи тя - изследване на заплахи, източници на заплахи, уязвимости на активите в различни работни среди [16, 30]. За ефективно противодействие на атаките е нужно да се знае принципа на действие на различните типове атаки, риска, които атаката представлява за активите, и подходящите подходи за сигурност, които можем да използваме като контрамярка за защита [26, 29, 30, 31].

Различните типове атаки се категоризират в следните категории:

- Прихващане (Interception);
- Прекъсване (Interruption);
- Модификация (Modification);
- Фалшификация (Fabrication).

Всяка категория може да засегне едно или повече от понятията на „ПЦН Триадата“, както е показано на Фигура 10. Границата между тях е размита, поради комплексността на атаките и различните конкретни проявления. В зависимост от контрамерките атаките биват видоизменяни в различните си версии, което обуславя известна условност в тяхната категоризация [29].

Фигура 10. Типове атаки

„Прихващане“. Този тип атаки позволяват на неоторизирани потребители достъп до данни или други активи и са по същество атаки срещу Поверителността. Прихващането може да бъде под формата на неразрешено преглеждане или копиране на файлове, подслушване на телефонни разговори или четене на електронна поща и може да се извършва срещу “Данни в покой” или “Данни в движение”. Този тип атаки могат да бъдат много трудни за откриване.

„Прекъсване“. Тези атаки водят до временна или постоянна невъзможност за използване или недостъпност на данни или други активи. Те засягат както Наличност,

така и Цялостност като елементи на „ПЦН“ Триадата. За пример може да се даде DoS атака към пощенски сървър – това е атака към Наличността. В случай на атака, свързана с манипулация на база данни имаме атака срещу Цялостността заради възможната загуба или повреда на данни. Тази атака може да бъде категоризирана и като Модификация ако резултатът е промяна на данните.

„Модификация“. Чрез тези атаки се извършва подправяне на данни или други активи. Те са насочени както срещу категорията Цялостност, така и срещу категорията Наличност. Пример за този тип атака е неоторизиран достъп до файл и промяна на данните, които той съдържа – имаме атака срещу Цялостност на данните. Ако засегнатия файл е конфигурационен за системата, ще бъде променен начина по които работи системата и съответните услуги, например Web сървър, ще бъде засегната и неговата Наличност. Ако с промяната на файла се промени и начина по които системата обслужва примерно криптирани връзки, ще имаме засягане и на Поверителност.

„Фалшификация“. Атаките от този тип включват неоторизирано генериране на данни, процеси, комуникация или други дейности чрез дадена система. Тези атаки засягат преди всичко Цялостност, но може да се считат и за атаки срещу Наличност. Като пример за подобна атака може да се даде генериране на фалшива информация в база данни, изпращане на фалшифицирана електронна поща от името на оторизирания потребител, която обикновено се използва като метод за разпространение на зловреден софтуер и атаки от тип Spear-fishing. Атака от този тип може да бъде и атака към Наличност, ако атакуващия успее да генерира достатъчно процеси, консумиращи системни ресурси, като мрежов или Уеб трафик и направи така, че услугите обработващи трафика да претоварят системата, то като резултат тя ще блокира и ще стане недостъпна за легитимните потребители.

Атаките могат да се проведат на различни нива, използвайки слабости и уязвимости на множество протоколи, среди и приложения. В Таблица 5 са посочени примери за различни атаки, проведени в различните слоеве на OSI модела в мрежова комуникация [34]. В зависимост от метода на атака, атаките могат да използват слабостите на няколко различни слоеве едновременно, усложнявайки тяхното неутрализиране.

Както посочихме при моделите за защита, един от най-ефикасните модели е Многослойния, известен и като Луков модел. При него се използват различни видове подходи за сигурност и нива на контрол, формирайки многопластов подход за защита. В Таблица 5 са представени различни подходи за сигурност, които обхващат слоевете от OSI мрежовия модел. Чрез комбинирането им се създава комплексна защита, способна да противодейства на многослойни атаки [29].

OSI Мрежови Слоеве	Атаки	Методи на защита
Многослойни атаки	Отказване на услуга (DoS) , Представяне за друг (Impersonation), Човек-в-средата (Man in the middle)	Генериране на дневници от системните събития, (System Logging) и от различните услуги и сървъри (Web, proxy logs)
Приложен слой	Отхвърляне (Repudiation), Повреждане на данни	Генериране на дневници (Log files) от сървъри и приложения.

Транспортен слой	Прихващане на сесия (Session Hijacking), вариации на DoS атаки (SYN Flooding)	Системи за откриване на аномалии
Мрежов слой	Червеева дупка (Worm hole), Черна дупка (Black hole), Наводняване (Flooding), Разкриване на местоположение (Location Disclosure)	Безжични системи за откриване на аномалии, Филтриране по портове (Switch Port Filtering)
Канален слой	Анализ и мониторинг на трафик, MAC Disruption, WEP слабости	Филтриране и контрол по портове (Switch Port Control and Filtering)
Физически слой	Заглушаване (Jamming), Прихващане, Подслушване (Eavesdropping)	Филтриране и контрол по портове (Switch Port Control and Filtering)

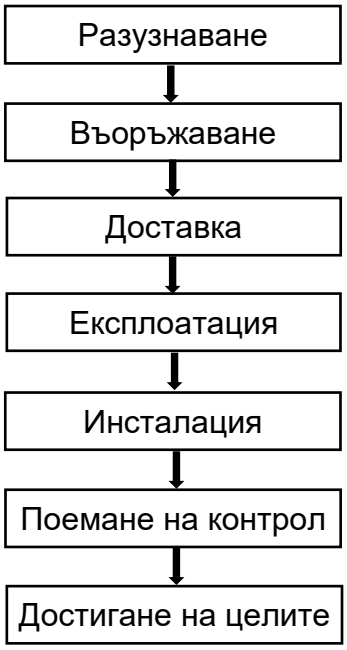
Таблица 5. Атаки и методи на защита в OSI модела

За илюстрация на принципа на действие на атаките успешно може да бъде използван Модела за извършване на кибер-атаки, предложен от американската компания Lockheed Martin (Фигура 11) [28, 64, 65]. Предложената от тях абстрактна рамка описва последователностите от изпълними действия, представляващи основните етапи на атаката и методите за нейното неутрализиране. Защитата може да адаптира предложената рамка и да я изменя според конкретните среда, условия и атаки. Моделът за извършване на кибер-атаки се състои от седем етапа:

- Разузнаване (Reconnaissance);
- Въоръжаване (Weaponization);
- Доставка (Delivery);
- Експлоатация (Exploitation);
- Инсталация (Installation);
- Поемане на контрол (Command and control);
- Достигане на целите (Actions on objectives).

Етапът на Разузнаването включва събиране на полезна информация за целта на атаката – IP адреси, операционни системи, конфигурации, имейли, имена и др. Вторият етап „Въоръжаване“ включва подготовката на зловреден товар, експлоатиращ дадена уязвимост и доставен до целта през следващия етап на Доставка. Зловредният товар може да бъде доставен например чрез подвеждаща електронна поща или чрез методите на социалното инженерство. След като е доставен, при етап „Експлоатация“ се използват уязвимости, позволяващи изпълнението на зловредния код. По време на етапа „Инсталация“ той бива инсталиран върху системите на целта. Следващият етап е поемането на отдалечен достъп до целта. Последния етап е Достигане на целите, където злонамерените лица имат контрол и могат да осъществят поставените цели.

Други ресурси, представляващи бази знания и рамки за описание на кибер-атаки, широко залегнали в практиката са MITRE ATT&CK® [127] и NIST Cybersecurity Framework [128].



Фигура 11. Модел за извършване на кибер-атаки

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 (Таблица 6) [2, 12, 13]:

- Превантивни – Блокират заплахите преди те да се възползват от дадена уязвимост;
- Разкриващи – Разкриват и предупреждават за атаки в реално време, в момента на случването им;
- Възпиращи - Възпрепятстват външните атаки и нарушенията на приетите политики за информационна сигурност;
- Коректривни – Възстановяват целостта (интегритета) на данните или други засегнати активи;
- Възстановителни – Възстановяват достъпността на атакуваните и нарушени услуги;
- Компенсативни – Компенсират последствията от успешните атаки към дадени контроли за сигурност чрез един или повече от останалите незасегнати контроли. Използват се при многопластова стратегия за сигурност

Категории ПИС	Действие	Примери
Превантивни	Блокиране, Избягване	Ключалки, Сейфове, Охрана, ЗС , СПП, Контрол на достъп, ПС, обучения по

		сигурност, Криптиране, Политика за пароли, Тестове за проникване в системата
Разкриващи	Разкриване, Предупреждаване	Камери за наблюдение, СОА, SIEM, Патрули, Капани (Honeypots), СПИКЗ.
Възпиращи	Възпрепятстване	Огради, Политики за сигурност, Мултифакторно удостоверяване, СПП
Корективни	Възстановяване	Административни мерки, Архив, Дублиране на дисково пространство с RAID технологии, Мерки за управление на инциденти,
Възстановителни	Възстановяване	Архив, Репликация на данни, План за възстановяване след бедствия
Компенсативни	Компенсиране	Ръчни и автоматични процеси за възстановяване, процедури от приет План за възстановяване след бедствия

Таблица 6. Категории ПИС

ПИС могат да имат различна физическа реализация - Таблица 7 [2,12,13,14]:

- ПИС за физическа сигурност - присъстващи физически в реалния свят;
- Административни ПИС – определят се и се прилагат от ръководството на база на действащото законодателство, регламенти, стандарти и добри практики;
- Технологични ПИС - извършват се от изчислителни машини;
- Оперативни ПИС - извършват се от хора;
- Виртуални ПИС – задействат се динамично, при възникване на определени обстоятелства.

ПИС за физическа сигурност са средства и устройства за контрол на физическия достъп до чувствителна информация и за защита на информацията [2]. Тези елементи на сигурност са необходими, за да се гарантира че неоторизираните лица нямат достъп

ПИС	База	Примери
ПИС за Физическа сигурност	Реален свят	Ключалки, Сейфове, Алармени системи, Портали, Врати, Огради, Предупредителни табели и др.
Административни ПИС	Действащо законодателство, регламенти, стандарти и добри практики	Политика за ИС, политика за защита на данните, приети правила за достъп, глоби и административни наказания и др.
Технологични ПИС	Изчислителни и комуникационни устройства, софтуерни системи	Видеокамери, ЗС, СОА/СПП , Контрол на достъп, SIEM, Архивиране, СПИД, ЗЗС и др.
Оперативни ПИС	Човешки фактор	Охрана, служители ИТ сигурност, служители преминали Security Awareness обучения и др.

Виртуални ПИС	Помощни инструменти, работещи с други ПИС	Списъци за контрол на достъп, Списъци с IP адреси, Политика за пароли, 2FA авторизация, Географско разположение

Таблица 7. Начини на реализация на ПИС

до определени физически пространства (район, зона, сграда, лаборатория, офис или стая), където присъствието им се смята за потенциална заплаха [14]. Примери за ПИС за Физическа сигурност са всички системи за физическа защита (портали, врати и огради), системи за контрол на достъп, системи за физическо наблюдение и алармиране при проникване.

Административни ПИС – Определят се и се прилагат на база на действащото в страната законодателство, регулации по индустрии, регламенти, стандарти и добри практики в дадената област [14]. Такива са EU GDPR [68], Наредба за минималните изисквания за мрежова и информационна сигурност [15], стандарти като ISO 27001 и ISO 27002 [8, 78, 79], Национални стратегии [56], Закон за Кибер сигурността в Р. България [57, 74] и др.

Технологични ПИС - Всяко изчислително, запаметяващо или архивиращо устройство и свързаните с тях комуникационни съоръжения се считат за чувствителни активи и съответно да бъдат защитени. Това става чрез съответните технологични ПИС:видеокамери, антивирусни решения, СОА, СПП, ЗЗС, ЗКТ,ПС и СПИКЗ (Фигура 3).

Оперативни ПИС – Тук се включва човешкия фактор в ПИС. Такива са физическата охрана, служители информационна сигурност, служители преминали обучение по информационна сигурност, служители по сигурността и др.

Виртуални ПИС – Те представляват помощни инструменти, работещи с други ПИС и прецизиращи техния обхват. Те могат да бъдат както пасивни инструменти (различни видове списъци), така и динамични системи, задействащи се динамично, при възникване на определени събития или обстоятелства, например Geofencing защитата, ограничаваща достъпа до определени ресурси или данни в зависимост от географското местоположение, на базата на географски координати и др.

2.2 Риск анализ

Според дефиниция по ISO 27005, рискът е вероятността даден източник на заплаха да експлоатира определена уязвимост (Фигура 7), в резултат на което да причини вреда на организацията [25]. Дефиницията на риска се базира на следните елементи:

- Активи, съществуващите уязвимости и нивото на защита, реализирано чрез подходите за защита;
- Заплаха, състояща се от агент на заплаха, който използва вектор на атака за компрометиране на активи. Ефективността на атака, изразена чрез вероятност за успех) зависи от възможностите на агента на заплахата и нейния характер;
- Въздействие, което отчита стойността на активите за организацията в конкретна среда, и последиците, когато поверителността, цялостността и наличността на активите е компрометиран чрез заплахата.

Дефиницията на риска чрез посочените компоненти - актив, заплаха и въздействие, отговаря на повечето съществуващи дефиниции, добре практики и стандарти: OWASP [129], CAPEC [130], ISO 15408 [131], ISO 31000 [132], WEF [133].

В информационната сигурност 100% защита е невъзможна, заради необходимостта да се ангажират хора, време и капитал, които винаги са ограничен ресурс. Затова най-

добрия подход е да се разгледа всеки ценен актив или данни в контекста на свързания с него риск от загуба и неговата стойност, за да се прецени цената на неговата защита и дали защитата му е оправдана за организацията. Това е и основната цел на риск анализа. Оттук произлиза още една от основните цели при разработването на СИС – да се редуцира риска от загуба на информация или активи.

Управление на риска. Това е общия процес на идентифициране, контрол и смекчаване на рискове, свързани с информационни системи. Управлението на риска включва оценка на риска, анализ на разходите и ползите, избор, внедряване, тестване и оценка на сигурността на защитните мерки. Процесът на управление на риска осъществява цялостен преглед на сигурността на системата, отчитайки както ефективността, така и ефикасността на подходите за сигурност, така и ограниченията породени от приетата политика за сигурност, действащите разпоредби и регулации [16]. Управлението на риска е процесът, който позволява на ИТ мениджърите да балансират оперативните разходи и наличните ресурси за постигане на заложените цели на системите за информационна сигурност. Управлението на риска обхваща няколко отделни процеса:

- Оценка на риска,
- Потискане на риска,
- Периодичен процес на оценка.

Оценка на риска. Процесът на идентифициране на рисковете за сигурността на системата и определяне на вероятността за възникване, последващо въздействие и допълнителни предпазни мерки, които биха смекчили това въздействие. Оценката на риска е свързана с шанса заплахата успешно да използва дадена уязвимост и последиците, ако това се случи. В практиката намират приложение няколко метода за оценка на риска:

- Качествен. Този метод използва матрица за анализ на риска и присвоява стойност на риска като нисък, среден или висок;
- Количествен. Този метод е използва различни количествени показатели и метрики за количествено определяне на риска;
- Хибриден. Съчетание от горните методи.

Част от оценката на риска са процесите на идентифициране на заплахи и уязвимости и оценка на активите:

Идентифициране на заплахи и уязвимости. Заплахите и уязвимостите са свързани. Заплаха е възможна когато е налице съответна уязвимост. При това заплахите могат да бъдат както известни, така и неизвестни. Идентифицирането на известни заплахи и прогнозирането на неизвестни заплахи е предпоставка за намаляване на риска, свързан и информационните активи.

Оценка на активите.

В активите, освен материални единици като сгради, комуникационни мрежи, сървъри и работни станции, се включват и нематериални - данни, интелектуална собственост и ноу-хау. Оценката на активите се извършва чрез няколко подхода:

- Разходен подход. Колко би струвало подмяната на актива?
- Приходен подход. Какъв е прихода на активът през жизнения му цикъл?
- Пазарен подход. Колко струва подобен актив?
- Количествен подход. Директна оценка в парична стойност.
- Качествен подход. Оценка на риск чрез точкова система, оценяваща дадени качества на актива.

Потискане на риска. Потискането на риска, е процес, отнасящ се до приоритизиране, прилагане и поддържане на подходящите мерки за намаляване на риска, препоръчани от процеса на оценка на риска.

Периодичен процес на оценка. Чрез процеса на оценка на програмата за управление на риска се определя дали оставащият риск е на приемливо ниво и дали следва да се приложат допълнителни подходи за сигурност, за да се намали или премахне остатъчният риск, преди да се акредитира системата. Този процес се изпълнява периодична на определени интервали.

При проектирането на СИС, на базата на риск анализ се определя точно какви активи трябва да защити системата, като се имат в предвид изискванията на различните заинтересовани страни, действащата нормативна и финансова база, регулаторни режими и т.н. На базата на риск анализа се определят и защитните мерки, формиращи подходите за информационна сигурност използваме за постигане на целите на СИС. Те от своя страна ще определят и изискванията към системата при нейното проектиране.

В нашия случай ще разгледаме подходите за защита в посока отвътре-навън за предотвратяване изтичането на информация в резултат на пробив, кражба или инцидент.

2.3 Видове комуникации

От гледна точка на подходите за осъществяване на комуникация тя се разглежда като:

- *„Йерархична организационна комуникация“* - комуникация в рамките на дадена организация основана на йерархичната структура на организацията;
- *„Мрежова комуникация“* - комуникация, осигуряваща равнопоставеност между участниците в нея [48].

В зависимост от спецификата на двата вида комуникация се използват различни подходи за информационна сигурност (Фигура 3). 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 човешкия фактор, всяка организация обхваща сравнително голяма група от хора, функционираща на пълен работен ден с ясно дефинирана структура, отговорности и установени взаимоотношения между служителите. С еволюцията на организациите като социални структури, комуникацията в тях се променя от просто изпращане и получаване на съобщения към обработка и интерпретация на съобщенията и информацията, съдържаща се в тях, вътре и навън от организацията.

С окрупняването на организациите се поражда нуждата от промяна в тяхната структура. Тя се видоизменя от плоска към строга вертикална йерархична, дефинираща различни нива на управление, роли и отговорности за служителите. Такава структура е необходима за да се координират ефективно основните дейности на организацията. Ролите в организацията са набор от ясно разписани права и отговорности, описани в длъжностната характеристика на съответната позиция. Тези длъжностни характеристики отразяват нуждите на организацията и не отразяват личностни качества на заемащите тази позиция служители. Така съответната позиция не зависи от конкретни личности и позволява гъвкавост при смяна на служителите.

Съвременната организация оперира като мащабна интегрирана система, в която всички операции са взаимозависими. Оттук идва и необходимостта от стандартизирани

комуникационни процедури и тяхното формализиране. Увеличава се и комплексността на комуникациите, развиват се формалните пътища по които минава основната комуникация, въвеждат се и нови форми на комуникация, като меморандуми, официални изявления, различни видове доклади и други. В организацията се създават както общи така и специализирани съобщения със специфични получатели и съдържание. Различават се формална и неформална комуникация:

- *Формалната комуникация* следва както йерархичната структура на организацията, така и хоризонталната комуникация между служителите. Този вид комуникация 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. Този вид комуникация 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 системи за информационна сигурност

Тази гледна точка може включва различни технологични подходи за разработването на една система за информационна сигурност. За целите на дисертацията съм се спрял върху Обектно-ориентиран подход, Агентен подход и Мулти-агентни системи.

2.4.1 Обектно-ориентиран подход

Обектно-ориентираният подход (ООП) позволява един проблем да бъде разбит на съставните му компоненти. Всеки компонент се превръща в самостоятелен обект, който съдържа свои собствени данни, методи за обработка, както и определени действия. ООП съдържа следните основни елементи:

- *Обект* - Елементарна единица в ООП, включваща в себе си както описващите обекта данни, така и средствата за обработка на тези данни.
- *Клас* - Обобщено описание на набор обекти, притежаващи някои еднакви методи и структури от данни.
- *Подклас* - По-подробно описание, отнасящо се към някакво специализирано подмножество на набор от обекти, от описания клас. Понякога подклас наричат също производни или дъщерни класове

ООП се характеризира със следните свойства:

Капсулиране. Това е механизмът, който свързва заедно данните и методите за обработка, като ги запазва невредими от външна намеса и злоупотреба. Така формираният обект може да се разглежда като “черна кутия”, без да се интересуваме какво точно е съдържанието му.

Наследяване - процес, при който един обект може да придобие свойствата на друг обект. Към наследените свойства обекта може да добави свои собствени свойства, които да бъдат наследени от друг обект. Наследяването дава възможност за създаване на йерархия на обектите.

Полиморфизъм. Свойство, позволяващо едно и също име да бъде използвано за две или повече сходни, но технически различни цели. В ООП полиморфизмът дава възможност с едно име да се зададе общ клас от действия. В рамките на един такъв общ клас специфичното действие, което трябва да се приложи, се определя от типа на данните и от мястото на всеки обект в йерархията.

Обектно-ориентираното моделиране (ООМ) е процес при които с методите на ООП се създава модел. Използват се тези обекти и техните характеристики, които са свързани с решаването на конкретния проблем, като останалите се игнорират. Моделът е опростена абстрактна версия на оригиналната реалност, позволяваща ни да решим проблема или задачата, използвайки ООП – обекти, класове и методи [90]. Следните концепции са от съществено значение за създаване на адекватен и полезен модел [91, 92]:

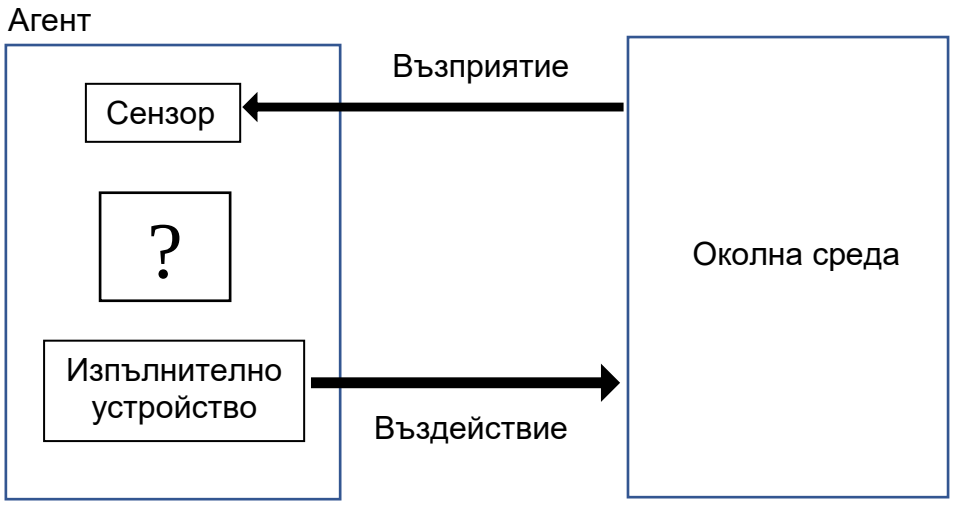
- *Абстракция* – разглеждане само на важните за изследването качества на обекта и пренебрегване на несъществените;
- *Идеализация* – създаване на идеален обект, на който са предадени допълнителни характеристики, които не може да се реализират, но спомагат за придобиване на познания за обекта;
- *Дедукция* – преминаване от общото към частното, от общи закони и положения към единични частни изводи;
- *Аналогия* – информацията за един обект се свързва с друг въз основа на сходството между тях.

2.4.2 Агентен подход. Мулти-агентни системи.

Според Russel и Norving [50] агент е всяка съвкупност, възприемаща околната среда чрез сензори, обработваща информацията за нея и въздействаща върху околната среда чрез изпълнителни механизми (Фигура 12).

При аналогия с човек, възприятието на околната среда се извършва от неговите сетивни органи, а въздействието - чрез неговите крайници или глас. Ако разгледаме агентите като синтетичен продукт, органите за възприятие могат да бъдат различни видове сензори (звукови, оптични, тактилни), а изпълнителните устройства, чрез които се въздейства върху околната среда могат да бъдат различни задвижващи и манипулационни устройства или източници на звук или образи. Агентите могат да бъдат и чисто виртуални или софтуерни, представляващи компютърни програми притежаващи способност за самоусъвършенстване и саморазпространение [48, 49, 51, 52, 54]. В този случай те не притежават ясно разграничими сензори и изпълнителни устройства, а говорим по-скоро за входни и изходни данни, чрез които се оказва въздействие върху други програми.

Терминът „Възприятие“ се използва като обобщено понятие на входната информация която агента получава от околната среда във всеки един момент. „Последователност от възприятия“ на агента наричаме пълната история на всичко което агентът някога е възприел от околната среда чрез своите сензори. Изборът на въздействие на агента във всеки един момент зависи единствено и само от „последователността от възприятия“ до момента, но не и от нещо, което не е възприел. Математически погледнато, поведението на агента се описва от функцията на агента, която преобразува дадена „последователност от възприятия“ в някакви действия върху околната среда. Тя може да бъде описана чрез алгоритъм и реализирана от програмата на агента. В случая, докато функцията на агента е абстрактно математическо описание, програмата на агента има конкретна реализация в някаква физическа система чрез програмен език. Така можем да определим агента и като компютърна система, която се намира в някаква околна среда и която е способна на автономни действия в тази среда, за да изпълни своите цели по задание [95]. Средата в която действа даден агент може да включва различни обекти, които да бъдат разглеждани или като други агенти, извършващи интеракция с останалите агенти – мулти-агентни системи или като обекти, които са неспособни на автономна интеракция.



Фигура 12. Агент

Мулти-агентните системи (МАС), са един от модерните методи на Изкуствения Интелект. МАС могат да бъдат дефинирани по следния начин - дадена система се разделя на множество самостоятелни обекти, всеки от които може да решава само определен локален проблем, тъй като не разполага с изчерпателни познания за глобалния проблем. В този случай целите на системата се изпълняват от множество самостоятелни обекти, които наричаме агенти [52]. Такива са например:

- Агент по нарушенията,
- Агент за защита,
- Агент на политика за ИС,
- Агент за наблюдение,
- Рапортуващ агент,
- Складиращ агент,
- Комуникационен Агент;
- Обработващ агент;
- Агент за реализация на услуги.

Чрез комбинация от агенти, на практика може да бъде моделирано и симулирано действието на произволна СИС, както и на произволен подход за сигурност, например платформи от тип СПИД.

2.5 Обработка на информация

Различните организации, в зависимост от спецификата на своята дейност генерират, използват или обработват данни, които са многообразни по вид, съдържание и структура. Всяка организация индивидуално 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. Ако систематизираме съдържанието на типичните документи, използвани в ежедневните дейности на една организация, сред тях можем да открои основни типове чувствителни данни/документи (Таблица 8).

Корпоративни данни	Транзакции	Данни за клиенти	Лични данни
Ценови листи, Списъци с клиенти; Нов дизайн на продукт; Сорс код; Формули; Технологични документи; Все още неодобрени патенти; Интелектуална собственост; Планове за развитие; Непублични финансови документи; Правни документи; Лични данни на служители.	Банкови разплащания; Поръчки; Данни за доставчици; Обеми на продажби; Потенциални печалби; Очаквани продажби; Търговски отстъпки.	Списъци с клиенти; Информация за покупки; Потребителски предпочитания; Продуктови профили на клиенти; Статут на плащания; История на контактите; Финансови баланси; История на покупки и транзакции; Условия на плащания; Търговски договори.	Имена; Рождени дати и места на раждане; Адреси местоживеене; IP адреси; Биометрични данни; Генетична информация; Номера на кредитни карти; Национални Идентификационни номера (ЕГН,номера на паспорти, номера на социални осигуровки); Номера на шофьорски книжки; Регистрационни номера.

Таблица 8. Основни типове чувствителни данни

Различните организации могат да дефинират и използват различни типове чувствителни данни в зависимост от своите нужди, законодателната рамка, действащите регулаторни режими – например GDPR, приети политики за сигурност, нужни сертификации, специфични данни при участие в определени проекти или обединения от няколко организации и т.н. От съществено значение е валидните чувствителни данни да са ясно дефинирани, да бъде дефинирано и разписано кой може да борави с тези данни, какви са задълженията и отговорностите на служителите в зависимост от тяхната роля в организацията. За да бъде възможна защитата на данните е важно да се знае как тези данни се съхраняват, как са структурирани и в какво състояние се намират.

Данните могат да бъдат съхранявани в структурирани и неструктурирани хранилища:

- *Структурирани хранилища на данни*. Данните са организирани в структурирани *в* структурирани хранилища, като например релационни бази данни, които се поддържат и контролират от организацията;
- *Неструктурирани хранилища на данни.* Данните се съхраняват в неструктурирани хранилища като мрежови дялове или директно върху работните станции. В този случай те се управляват от крайните потребители.

Структурираните данни съответстват на предварително дефиниран строг модел и са ограничени от него. Моделът може да дефинира бизнес процес, който контролира потока на информация, схема на организация на данните, система от маркировки и други. Типичен пример за структурирани данни са базите данни. При тях данните са организирани на основа на т.нар. схема на базата данни, определяща правилата за

съхранение, индексация и достъп до данните. От гледна точка на информационната сигурност базите данни имат следните предимства:

1. Базите данни са защитени. Обикновено сървърите се намират в защитени центрове за данни, сериозни механизми за мрежова защита, архивиране и други.

2. Самите данни са структурирани по начин, който обикновено позволява лесна класификация и достъп до данните.

Неструктурираните данни не отговарят на строг модел. Те могат да бъдат от всякакъв формат, да се съхраняват навсякъде и да се движат във всякакви мрежи. Неструктурираните данни са много по-трудни за управление и защита. За да бъдат ефективно защитени чувствителните данни от този вид е необходима тяхната трансформация в структурирани данни и/или използването на специализирани инструменти като Системи за предотвратяване изтичане на данни, решения за маркиране на чувствителни данни и други.

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.

Данни в покой. Това са данни, съхранявани в ИТ инфраструктурата на организацията - сървъри, бази данни, споделени файлове, интранет сайтове, работни станции, лаптопи, мобилни устройства, преносими хранилища, архивни ленти и сменяеми носители. Данните в покой може да бъдат съхраняват на външни носители на информация или чрез външни разширения на ИТ инфраструктурата – в облак.

Данни в движение - данни, които са в процес на прехвърляне. Те могат да бъдат пренасяни през вътрешната мрежа, навътре или извън организацията, чрез различни комуникационни услуги – WWW, E-mail, FTP или sFTP, мрежов печат, VPN канали, телефония, факс и др

Данни в употреба. Това са данни, които са достъпни или се използват от системите и приложенията в определен момент от времето. За пример могат да бъдат дадени данни, намиращи се във временната памет на персонален компютър, отворен с офис пакет отчет или изпълняваща се заявка на работна станция, имейл, който е изготвен, но не е изпратен, файл, който се копира на USB устройство и данни, които се копират от един документ на друг.

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 зависимост от своя обхват и цели, СИС могат да бъдат както специализирани, защитаващи конкретни компоненти на информационната среда така и комплексни, защитаващи информационните активи на организацията като цяло от изтичане, пробив, кражба или злоупотреба. Обикновено СИС от втория вид комбинират различни подходи за информационна сигурност за постигане на цялостна защита на информацията, принадлежаща на организацията. Изборът на ПИС, използвани в СИС зависят от вида на комуникацията в организацията. При равнопоставеност между участниците в комуникацията (Мрежова комуникация), типичните подходи за сигурност, използвани при тях са: ЗС, СОА, СПП, ЗЗС, ЗКТ, ПС, СПИКЗ. При Йерархична организационна комуникация използваните ПИС са значително по-комплексни, заради характера на информацията предавана между различните нива и изискванията за нейната защита като Класификация на данни и Системи за предотвратяване изтичане на данни (Фигура 3).

СИС може да се различават по посоката на векторите на атаките от които те защитават компонентите на информационната среда [45, 46]. Традиционната посока е отвън-навътре, при която СИС защитава организацията от атаки отвън – хакерски атаки, фишинг атаки и др. Целта е неутрализиране на тези атаки, така че атакуващата страна да не може да получи достъп до вътрешната мрежа и съответните информационни ресурси и активи. Такава защита са например ЗС, контролиращи каналите, осигуряващи мрежовият трафик. По-съвременен метод е защита от изтичане на информацията отвътре-навън. При тях се обръща специално внимание на т.нар. “инсайдъри” – вътрешни за организацията лица с достъп до чувствителна информация или ресурси. Типични подходи за ИС, използвани в тях са СПИД като DeviceLock [95] и CoSoSys Endpoint Protector [96]. Ако злонамереното лице да е получило достъп до чувствителна информация чрез тези ПИС е невъзможно тя да бъде изнесена извън организацията или системата. Разбира се ПИС могат да бъдат комбинирани с цел по-сигурна защита на информационните активи на организацията.

Досегашният опит показва че ПИС в рамките на дадена организация обикновено са инцидентно организирани или се отнасят до спазване на определени (единични) законодателни регулации, необходими за нейната нормална работа. Макар стандартите и регулациите да претендират, че включват в себе си най-важните аспекти на ИС, те са по-скоро набор от добри практики. Редки са случаите, когато към ИС се подхожда методично и се спазват всички изисквания на стандартите. По този начин обикновено в практиката се подхожда „на парче“ за решаване на определени задачи от ИС, свързани с инциденти (изтичане на информация, атака към инфраструктурата, загуба на информация и др.) или с решаване на нововъзникнало предизвикателство – например новоприети регулации като Общия регламент относно защита на личните данни (Регламент (ЕС) 2016/679 [67] или наредби като Наредбата за минималните изисквания за мрежова и информационна сигурност [15].

В настоящата дисертация аз се концентрирам в проектирането на Системата за Информационна Сигурност 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. Такива са служителите на

организацията, външни изпълнители с разрешен достъп и доставчици на различни услуги.

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.

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 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

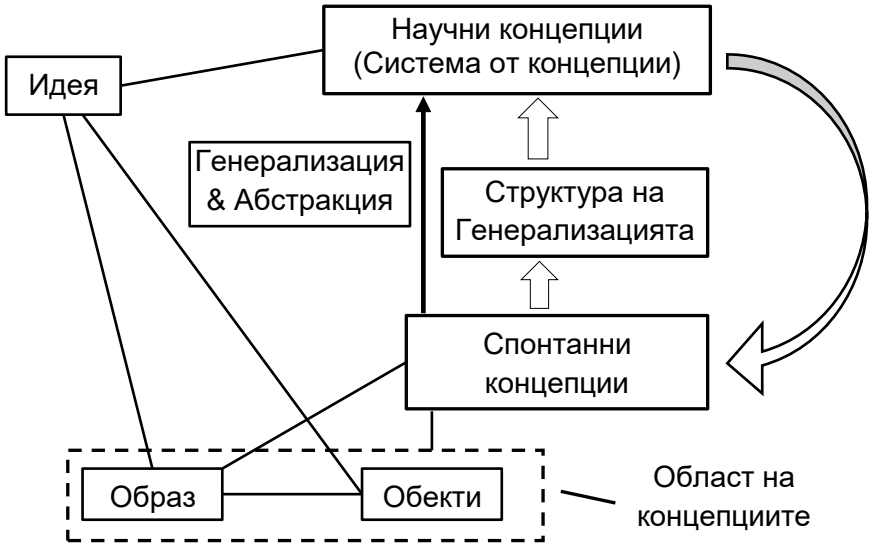
Unified Modeling Language (UML), предоставящ инструменти за описание, анализиране, моделиране и документиране на архитектурата и функционалността на СИС [97, 98].

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].

Контекст на концептуалното моделиране

Според древните гърци формирането на концепциите е свързано с понятието за мисъл, която се базира на някой от следните четири компонента: идея, образ, материал (обекти) и концепции (Фигура 13). Концепциите се свързват с обектите или съответстващите им образи, които са в нашия фокус и определят областта на концепциите [93]. Руският учен Вигодски се концентрира върху психологическите аспекти на развитието на концепциите. Той обозначава две групи концепции, които се отнасят до различни нива на тяхното формиране - спонтанни концепции и научни концепции [94]. Неговите изследвания върху развитието на научните концепции, наречени от него „истински концепции“ изясняват най-основните и съществени общи закони на формирането на понятията.

Спонтанната концепция се характеризира с липса на съзнателно осъзнаване. Вниманието винаги е насочено към обекта, който спонтанната концепция представлява, а не към акта на мисълта за този обект. Концепцията става нещо различно, щом се разглежда в система от концепции. Естеството на спонтанната концепция се променя веднага щом се извади от изолираната си форма, в която тя осигурява по-проста и по-непосредствена връзка с обекта и се поставя в генерализирана система от концепции. Наличието на концептуална система е важно за естеството и структурата на всяка отделна концепция. Ако от дадена концепция възникне по-висша концепция, трябва да има няколко подчинени концепции, които да я включват. Отношенията на тези подчинени концепции към дадената концепция трябва да се определят от система, създадена от висшата концепция. По този начин



Фигура 13. Рамка за формиране на понятия

генерализацията на понятието води до неговото локализиране в определена система от взаимоотношения, които са естествените и важни връзки между концепциите. По този начин едновременно генерализацията е предпоставка за съзнателното осъзнаване и систематизирането на концепциите.

Съзнателното осъзнаване и наличието на система са синоними, когато се изграждат концепции, точно както спонтанността, липсата на съзнателно осъзнаване и отсъствието на система са три различни думи за определяне на естеството на първоначалното развитие на концепцията. Ако съзнателното осъзнаване означава генерализация, очевидно е, че генерализацията от своя страна не означава нищо друго освен формирането на висша концепция в система от обобщения, която включва дадената концепция като частен случай. Всяка структура на генерализация има характерна степен на единство, характерна степен на абстрактност или конкретност. За всеки етап от генерализацията има съответстваща система от взаимоотношения и неопределености. Общи и специфични концепции са подредени в генетична серия в съответствие с тази система. По този начин при развитието на концепцията движението от общото към конкретното или от конкретното към общото е различно за всеки етап от развитието на значението в зависимост от структурата на генерализацията, доминираща в този етап.

Научната концепция предполага различно отношение към обекта. Тя не е свързана директно със съответния обект. Тази връзка се опосредства чрез съществуващи концепции, които сами по себе си имат вътрешна йерархична система на взаимовръзки. Зависимостта на научните концепции от спонтанните концепции и тяхното влияние върху тях произтича от уникалната връзка, която съществува между научната концепция и нейния обект. *Следователно, в своята връзка с обекта, научната концепция включва връзка с друга концепция*, тоест включва най-основния елемент на концептуална система. Тази съществуваща система е предпоставка за развитието на новата система. При разработването на научните концепции *системата възниква едва с тяхното развитие.*

Същността на научната концепция или генерализацията е в обогатяването на непосредственото възприемане на реалността, която тя представлява, както и на непосредствените чувствени възприятия и съзерцание. Този процес е възможен, само ако се установят сложни връзки, зависимости и взаимоотношения между обектите, които са представени в концепциите и останалата реалност. Всяка концепция предполага наличието на определена система от концепции. Извън такава система тя не може да съществува.

3.2 Модел 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;

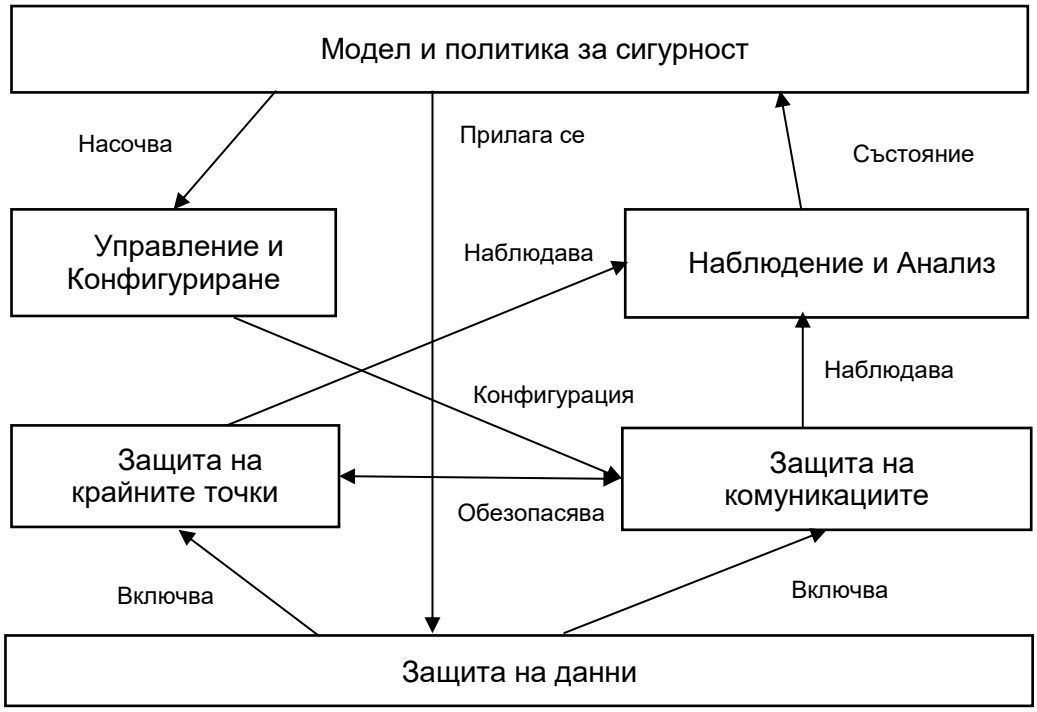
Резултатът от използване на концептуалното моделиране при създаване на Модел на анализа е концептуален модел, който представлява в своята същност абстракция, Всяка една концепция се разглежда като отделен компонент. Затова този модел представя и архитектурата на СИС.

3.2.1 Обобщен модел на проблемната област на системи за информационна сигурност в организации.

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

Компонентът *“Модел и политика за сигурност”* отразява околната среда, в която се проектира и реализира СИС. При анализа на ПО се уточни, че околната среда определя съвкупността от влияния и въздействия върху системата през целия й жизнен цикъл: технологични, бизнес, оперативни, организационни, политически, икономически, правни, регулаторни, екологични и социални влияния.

Този компонент определя как се прилагат приетите и формализирани политики и правила, съобразени с различните гледни точки на системата. Те отразяват изискванията на различните заинтересовани страни и формират определени области на интерес. Тези изисквания обикновено се обобщават в единна Политика за сигурност в организацията, за която се изгражда СИС и ясно определящи защо, какво, как, и къде трябва да се защитава, какви ограничения трябва да се спазват, както и задълженията и отговорностите на служителите в организацията.

Целите пред компонента *“Модел и политика за сигурност”* са гарантиране на Поверителността, Цялостността и Наличността на СИС. Той дирижира всички останали компоненти за осъществяване на тези цели и координира съвместната им работа. За целта останалите компоненти получават указания какво и къде се наблюдават и срещу какво се противодейства, какви ограничения да прилагат и за кои потребители, какъв тип и вид данни да защитават.

Целта на проектираната система за информационна сигурност е защита срещу изтичане на чувствителна информация от вътрешни лица в посока отвътре-навън. Това предопределя и политиката за информационна сигурност, за чието спазване отговаря компонента *“Модел и политика за сигурност”.* В политиката за ИС трябва да бъдат описани изискванията на конкретната организация за понятието „чувствителна информация“ и какви данни се включват в него. Това могат да бъдат например лични данни, според EU GDPR [67, 68], списъци с характерни ключови думи и изрази, определени типове данни (изображения, мултимедия, MS Excel файлове). Някои примерни чувствителни данни са показани в Таблица 8.

В политиката за ИС е дефинирано кои служители с какви права за достъп разполагат, до какви ресурси и данни, и при какви обстоятелства. Една от задачите на компонента е разпределянето на тези права до останалите компоненти. Едновременно с това се дефинира разбирането на организацията за пробив в сигурността, необходимите действия, които трябва да се предприемат при констатиране на пробив, както и процедурите за смекчаване на последствията и възстановяване на работоспособността на организацията. В политиката за сигурност се дефинират и съответните роли и отговорности на служителите, участници в процеса на осигуряване процеса на информационна сигурност в организацията.

Компонентите *“Защита на крайните точки“*, *“Защита на комуникациите“ и „Защита на данни”* осигуряват защитните свойства на СИС. Те осигуряват платформи на реализация на основни защитни модели като Периметрова защита и Многослоен модел на защита (Фигура 4). Целта на тези защитни модели е да осигурят съответствие с базови принципи за информационна сигурност като „ПЦН Триада“, „Принцип на тройното А“ и/или „Принцип на най-слабото звено“. Трите блока постигат тези цели като използват различни подходи за информационна сигурност (ПИС) за постигане на конкретните цели, зададени към тях от компонента „*Модел и политика за сигурност“.*

Компонентът *“Защита на крайните точки“* е отговорен за защитните способности на крайните точки на системата. Това са елементи на СИС, притежаващи изчислителни и комуникационни възможности. В зависимост от това в кои слой на Многослойния модел на защита (Фигура 4) се намира крайната точка– в рамките на

вътрешната мрежа, в мрежовия периметър или външна за организацията мрежа, крайните точки могат да използват различни подходи за ИС за да се изпълнят задачите за защита, както са показани в Таблица 1. Такива например са: Демилитаризирани зони, Виртуални частни мрежи, Тестове за проникване, Защитни стени, Прокси сървъри, Криптиране, Контрол на достъп, Архивиране на данни.

Задачите пред компонента *“Защита на крайните точки“* са:

- Неутрализиране на уязвимостите на системата,
- Противодействие на заплахите към системата.

Неутрализирането на уязвимостите на системата може да бъде постигнато по различни начини и с различни ПИС. Това може да стане например чрез пряко елиминиране или „запушване“ на уязвимостите. Необходимо е уязвимостите да бъдат идентифицирани, описани и класифицирани според степента на риска, който носят за системата. Не всички уязвимости могат да бъдат неутрализирани предварително, например т.нар. уязвимости от последния ден (0-day vulnerability). За тяхното неутрализиране е необходимо да се следят новостите за последните заплахи в бюлетините за информационна сигурност, да се прилагат най-новите поправки на системния софтуер, софтуера за защита от зловреден софтуер и останалите критични системи, свързани с информационната сигурност.

Невъзможно е, а и не е необходимо да се неутрализират всички уязвимости. Усилията трябва да бъдат насочени към най-критичните от тях. Например при систематизиране на уязвимостите на операционната система и различните приложения приоритет имат уязвимостите на системата защото приложенията се стартират върху нея и при успешна атака всички приложения и данни са подложени на риск. Следват приложенията, които използват или обработват критичните за системата данни, чувствителните данни, след което най-използваните приложения и т.н. Поредността и приоритетите зависят от целите пред СИС и съответната одобрена и заложена за изпълнение политика за информационна сигурност.

По-ефикасния подход за неутрализиране на уязвимостите е не чрез тяхното „запушване“ а чрез подходящи мерки за елиминиране или смекчаване на причините за тях – такава може да бъде мотивацията на агентите на заплахата (Таблица 3) и източниците на заплахата (Фигура 9, Таблица 2). Тези мерки са различни по характер, както е показано в Таблица 6. Така например повишаване мотивацията на служителите с подходящо възнаграждение и бонуси за постигнати резултати намалява желанието за отмъщение, унищожаване или изнасяне на чувствителна информация. Редовните обучения за повишаване на информираността по информационна сигурност (Security Awareness), както и подходящите административни санкции водят до намаляване на неумишлените и умишлените опити за нарушения на сигурността.

Системата за Информационна Сигурност, която проектираме, трябва да защитава от изтичане на чувствителна информация от вътрешни лица с достъп до ресурсите и данните на организацията – т.нар. „инсайдъри“. Разбира се, системата защитава и от други видове заплахи, но нашия фокус е защитата от неоторизирано изтичане или кражба на чувствителна информация в посока отвътре-навън чрез вътрешни лица.

Най-подходящия ПИС за целта са системите за предотвратяване на изтичане на данни СПИД, известни с английския акроним DLP или Data Leak Prevention. Системите, реализиращи този подход са резултат от комплексни хардуерни и софтуерни решения, контролиращи информационните канали на работните станции, лаптопи и сървъри. Тези решения позволяват наблюдение на данните, протичащи през тези канали,

анализ на тяхното съдържание и идентифициране на чувствителните за организацията данни чрез сравняване на съдържанието с предварително дефинирани ключови думи и изрази. При идентифициране на опит за изнасяне на данни извън защитената среда на организацията, СПИД са способни да блокират тези данни и да предотвратят изтичането им.

Подходящи мерки в случая са и подходи за информационна сигурност като Контрол на достъпа, Стриктна политика за формиране на пароли, Мултифакторна автентикация, Криптиране и Системи за предотвратяване на изтичането на информация. Тези ПИС могат да бъдат реализирани в крайните точки, поради факта че те разполагат с изчислителни и комуникационни възможности. Тези ПИС намаляват или напълно неутрализират причините за уязвимостите и защитават ефикасно системата при евентуална атака като я възпират (Контрол на достъп, Стриктна политика за паролите на организацията, Мултифакторно удостоверяване) или елиминират нейния резултат – изтичането или кражбата на криптирани със силен криптиращ ключ данни, на практика не водят до негативни резултати, защото данните не могат да бъдат използвани.

Компонентът е подходяща платформа за неутрализиране на заплахи, според модела за извършване на кибер-атаки на Lockheed Martin от Фигура 11. Модела включва последователност от процеси и действия за идентифициране и извършване на атаки. При осъществяване на атака (Фигура 9), агентът на заплахата експлоатира определени уязвимости, позволяващи му да проникне в системата и да получи достъп до ресурсите които го интересуват. За противодействие на атаката е необходима комплексна защита с комбиниране на методите за защита, посочени в Таблица 5.

Компонентът *“Защита на комуникациите”* отговаря за защитата на комуникацията между крайните точки, чрез прилагане на съответните ПИС (Таблица1). Целта на компонента е осигуряването на сигурен пренос на данни между крайните точки. За да се гарантира Поверителността, Цялостността и Наличността на комуникацията са необходими подходящи ПИС, като Валидация на данни, Криптиране, СПИД и Класификация на данни.

Една от най-често използваните ПИС в компонента е механизма на Контролната сума. Използва се при предаването на данни, за да се провери дали те са предадени правилно. Контролната сума представлява хеш-функция, чрез която се изчислява контролен код на базата на данните които се предават. Резултатът от изчислението се изпраща към получателя, които от своя страна я проверя като изчислява свои контролен код по същия алгоритъм и ги сравнява. Ако двете контролни суми са различни, се констатира грешка при предаването на данни и се инициира тяхното повторно изпращане. Това може да се дължи на опит за подмяната им по време на комуникацията или просто на смущения или прекъсвания по канала. Използват се различни хеш-функции като CRC, MD5 и други.

Компонентът *„Защита на данни”* осигурява защитата на данните в системата. Обхватът се простира от „Данните в покой“ и „Данните в употреба“ в крайните точки, през „Данните в движение“ в комуникационните канали, данните, резултат от наблюдение и анализ, както и всички данни за конфигурацията и управлението на системата [21, 22]. Компонента получава инструкции от централния компонент “*Модел и политика за сигурност*” какви данни, как, къде и от кого (какво) трябва да се защитават. На свои ред *„Защита на данни”* управлява останалите защитни компоненти *“Защита на крайните точки“* и *“Защита на комуникациите“,* инструктирайки ги по отношение на защита на данните. Компонентът *“Защита на данни”* директно и

индиректно поддържа и модулите *“Наблюдение и Анализ” и “Управление и Конфигуриране“,* генериращи данни при своята дейност, осигурявайки тяхната защита.

Освен ПИС, използвани в останалите защитни компоненти, *„Защита на данни”* изпълнява и дейности по запазване на работоспособността на системата, както и за възстановяване след бедствия и аварии. Такива са възстановителни ПИС като архивиране на данни и системни конфигурации, репликация на данни, коректив ни ПИС като дублиране на дисково пространство с RAID технологии, мерки за управление на инциденти, Компенсативни като процеси за възстановяване, процедури от плана за възстановяване след бедствия и други дейности (Таблица 6).

Примерен ПИС за защита на данни, осъществен чрез компонентите *“Защита на крайните точки“* и *“Защита на комуникациите“* е изолация на данни в мрежата. Осъществява се чрез създаване на канал за данни. Каналът е независимо идентифициран, управляван и контролиран поток от данни в транспортния или приложния слой. Състои от три основни комуникационни канала: канал за данни, контролен канал и канал за управление. Всеки канал трябва да бъде изолиран от останалите, като се управлява и наблюдава отделно, например чрез използване на отделни TCP връзки или отделни безжични честоти. Каналът за данни служи за докладване на оперативна информация и състоянието на крайната точка. Контролният канал се използва за контрол на крайната точка и различни процеси. Каналът за управление пренася служебна информация за състоянието на други компоненти, политики за сигурност или конфигурация на крайната точка. Използването на отделни комуникационни канали може да намали разходите и сложността на управлението и наблюдение на комуникациите. Всяка крайна точка може да има няколко активни екземпляра от всеки от трите типа канали. За всеки канал може да се дефинират отделни ПИС като криптиране, мрежово сегментиране и упълномощаване на комуникациите, контроли на целостта на съобщенията. Към всеки канал могат да бъдат приложени отделни изисквания за качество на услугата (QoS) за осигуряване на предаване на съобщения в рамките на дефинирани допустими отклонения.

Компонентът *“Наблюдение и Анализ”* осигурява запазване на състоянието на системата през целия и жизнен цикъл. Той осигурява наблюдение, анализ и контрол на състоянието на останалите компоненти на системата и извършва наблюдение на ключови параметри на системата, като ги сравнява с заложените контролни стойности. При наличие на отклонение се извършват коригиращи действия, с помощта на компонента *“Управление и Конфигуриране“.*

Целите, поставени пред компонента *“Наблюдение и Анализ”* са:

- Запазване на целостта на системата;
- Контрол на работоспособността на останалите компоненти;
- Коригиращи действия в случай на необходимост;
- Осигуряване спазване на приетата политика за сигурност.

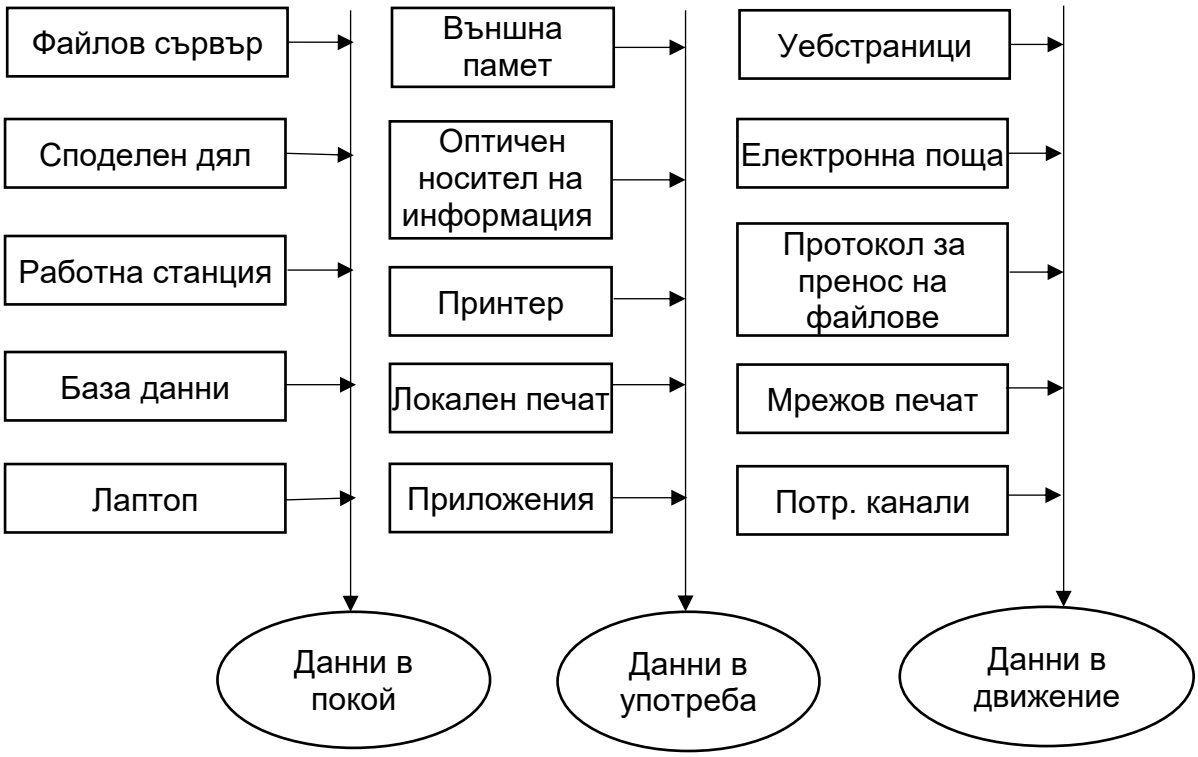
Компонент *“Управление и Конфигуриране”.* Основната му функция е управлението и контрола на работата на останалите компоненти в системата. Той осигурява изпълнението на заложените в централния компонент “*Модел и политика за сигурност*” политики за сигурност, разпределяйки задачите в защитните компоненти. Компонентът разчита на обратна връзка от *“Наблюдение и Анализ*“ за информиране относно текущото състояние на останалите компоненти. При констатиране на аномалии в работата на даден компонент, той извършва корекции на неговите конфигурационни параметри, осигурявайки нормализиране на работата му.

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) 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.

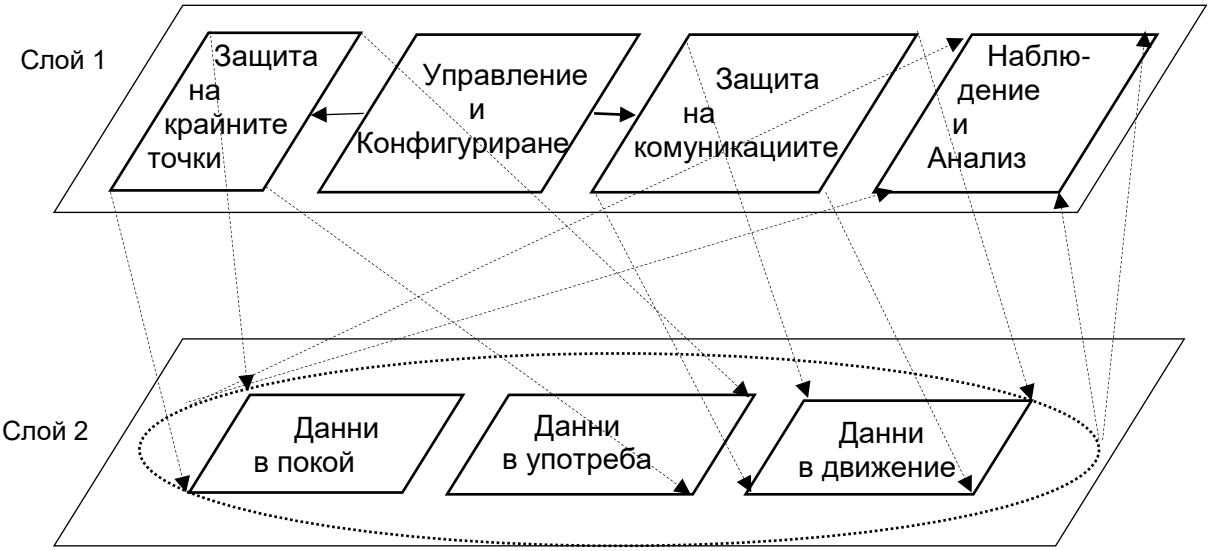
Показаният на Фигура 16 многослоен мета-модел представя гледните точки “Информационна сигурност” и “Обработка на информация” и взаимовръзките между тях. Като структура получения концептуален мета-модел съответства на Многослойния модел на защита от Фигура 4.



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.



Фигура 16. Многослоен концептуален модел на СИС

Отделните компоненти на мета-модела изпълняват следните функционалности по защита:

- Компонент *“Защита на крайните точки”* защитава Данните в покой и Данните в употреба в крайните точки. Компонентът използва подходящи подходи за информационна сигурност като: контрол на достъпа, пароли, антивирусен софтуер, одитни пътеки, физически мерки за сигурност.
- Компонент *“Защита на комуникациите”* предпазва данните в движение, чрез прилагането на ПИС като криптографски техники, мрежова сегментация, периметрова защита, шлюзове, защитни стени, Системи за откриване на аномалии, контрол на достъпа до мрежата, анализ на мрежовите журнали и др.
- Компонент *“Управление и Конфигуриране”* защитава конфигурационните данни, данните, резултат от мониторинг и анализ, както и оперативните данни чрез криптографски методи.
- Компонент *“Наблюдение и анализ”* е отговорен за защитата на данните за текущото състояние на системата, както и за наблюдението на ключовите системни параметри и показатели на системата. Типичните ПИС, използвани в този блок са криптографските техники.

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 описание на проблемната област

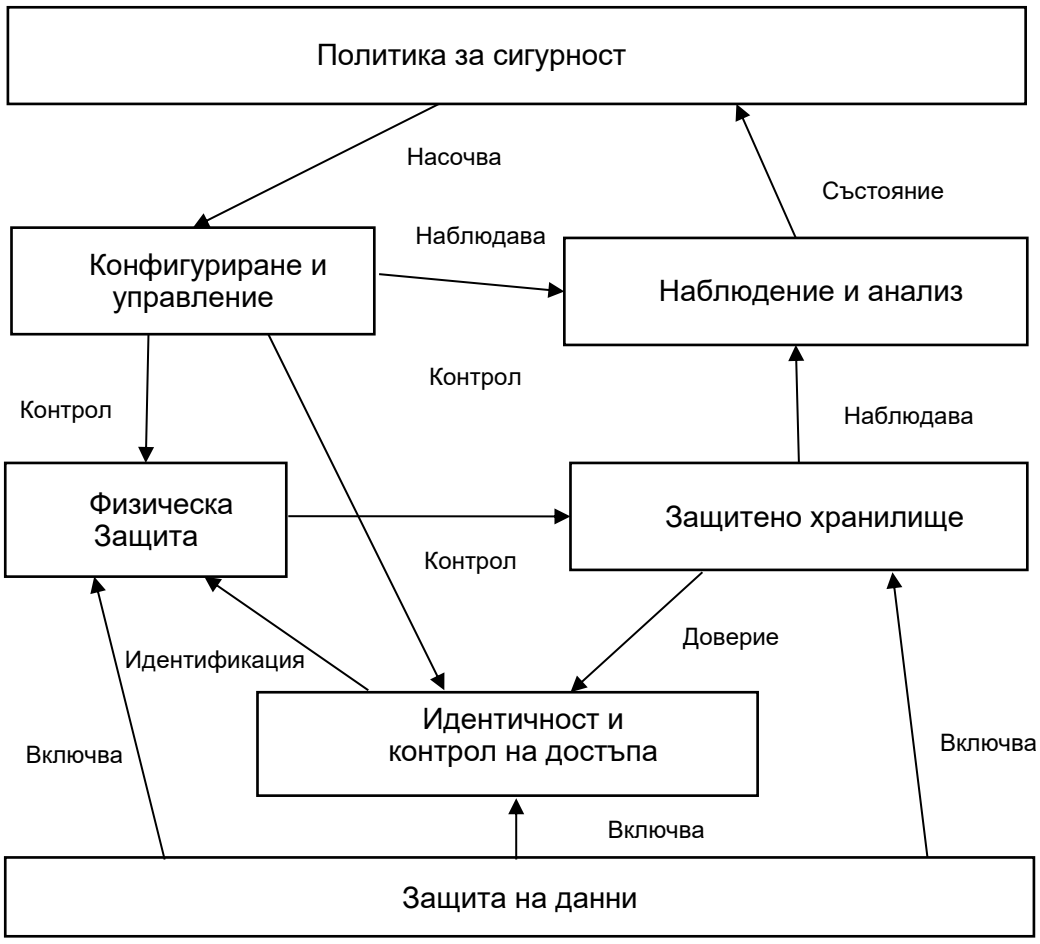
На основата на обобщения модел на СИС се създава детайлен модел на проблемната област на СИС. Ще се разгледат детайлните концептуални модели на два от показаните компоненти – *„Защита на крайните точки“* и *„Защита на комуникациите*“.

Детайлно описание 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 следните компоненти (Фиг.17):

1. Компонент „Физическа Защита“ - осигурява физическа защита на крайната точка за предотвратяване на неразрешени промени или физическо увреждане или разрушаване. Защитата се реализира чрез Превантивни (Ключалки, Сейфове, Охрана, ЗС, СПП, Контрол на достъп, ПС, обучения по сигурност, Криптиране) или Възпиращи ПИС (Огради, Политики за сигурност, Мултифакторна автентикация, СПП) - Таблица 6, както и ПИС за Физическа сигурност от Таблица 7 (Ключалки, Сейфове, Алармени системи, Портали, Врати, Огради, Предупредителни табели)



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

2. Компонентът „*Защитено хранилище*“ представлява трезор, който пази най-чувствителните активи на системата, защитава изпълнението на най-чувствителните приложения, създава основите за сигурност на платформата и осигурява целостността на компонентите на крайната точка. Компонентът е комплексна система от апаратни средства, процедури за сигурност, хора и организационни процеси. Той поддържа както хардуера, така и софтуера, (включително фърмуер), операционна система и приложения. Пример за такава платформа е новия Унифициран Разширен Интерфейс за Фърмуер (UEFI), който замества традиционната фърмуер система (BIOS), осигуряваща инициализацията на хардуера по време на процеса на зареждане на операционната система и предоставяща услуги по време на изпълнението на операционната система, потребителски и системни приложения. Новата платформа измерва цялостта на фърмуера, съхраняван във флаш паметта, като гарантира невъзможността за неговата модификация без разрешение. Целта, поставена пред компонента е осигуряването на увереност че дадено устройство или приложение не са подложени на неразрешена промяна и по този начин да гарантира правилната им работа и изпълнение на зададените функции.
3. Компонентът „*Идентичност и контрол на достъпа*“ осигурява механизми за еднозначна идентификация, удостоверяване и упълномощаване на отделните компоненти, преди предоставяне на достъп до услугите. ПИС, осигуряващи такава функционалност са Контрол на достъп, Мултифакторна автентикация, Административни мерки за управления на пароли, Списъци с одобрени IP и MAC адреси, както и добре познатите Възпиращи ПИС и ПИС за Физическа сигурност от Таблица 7.
4. Компонентът „*Конфигуриране и управление*“ осигурява контрола на изпълнението на зададената политика за сигурност и управлява конфигурацията на отделните компоненти на крайната точка – включително осигуряването на актуализации на софтуер и фърмуеър.
5. Компонентът „*Наблюдение и анализ*“ осигурява мониторинг на останалите компоненти и ключови точки от системата. Чрез него се извършва откриване, предотвратяване и възстановяване от всяко отклонение от политиката за сигурност на крайната точка. Той осигурява откриване на злонамерени приложения, дейности тип „отказване на услуга“, прилагане на политики за сигурност и проследяване на показателите за ефективност на сигурността.
6. Компонентът „*Защита на данните*“ осигурява Поверителност, Цялостност и Наличността на данните в отделните компоненти на крайната точка, включително оперативни данни, данни за наблюдение и конфигурация: Използва ПИС като контрол на достъпа, криптиране и изолиране.
7. Компонентът „*Политика за сигурност*“ осигурява управление на изпълнението на заложената в компонента политика за сигурност. Тя се дефинира от Околната среда, която въздейства върху системата. В това въздействие се включва нормативната и регулаторна среда, действащото законодателство, изискванията към системата от страна на организацията, бранша в които оперира и изискванията към него, изискванията към информацията която се използва или генерира, условията на работа и много други. Компонента диефинира чувствителните данни, които трябва да бъдат контролирани, кои има достъп до тях, по какъв начин, какви права има. Той дирижира останалите компоненти,

наблюдава и анализира отклоненията от зададените политика и задава съответните команди за изпълнение.

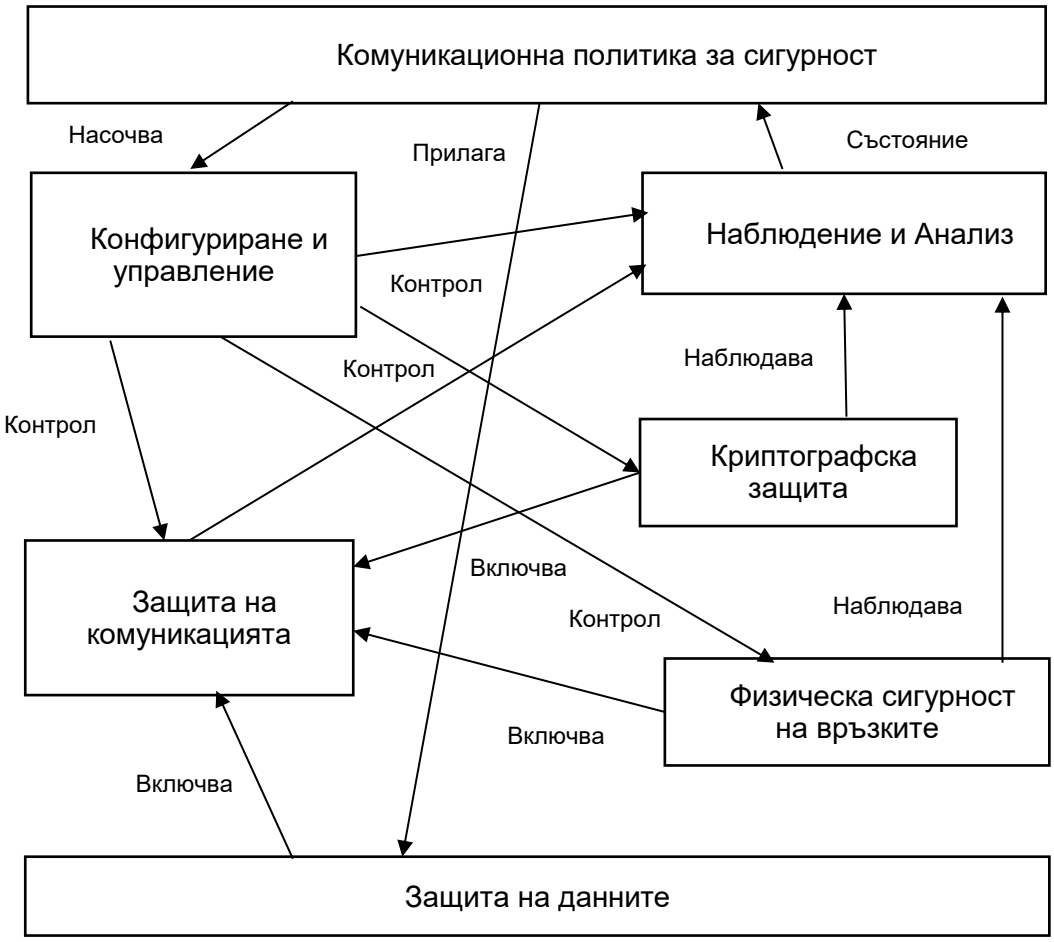
Детайлно описание на концепцията *„Защита на комуникациите*“

Концепцията *„Защита на комуникациите*“ осигурява сигурност на комуникационните канали и свързаните крайни точки. Състои се от следните компоненти (Фигура 18):

1. Компонент „Физическа сигурност на връзките“ осигурява защита на комуникационните канали от физическо увреждане или разрушаване. Подобно на физическата сигурност при крайните точки, защитата се реализира чрез Превантивни и Възпиращи ПИС (Таблица 6), както и ПИС за Физическа сигурност (Таблица 7).
2. Компонент „Защита на комуникацията“ осъществява защита на информационни потоци от тип "Данни в движение". Те включват IP съобщения, серийни комуникации, потоци от данни, контролни сигнали, данни, копирани на сменяеми носители или разпечатвани на принтер. Компонента използва ПИС като мрежова изолация на данни, сегментиране и различни механизми за филтриране на мрежовите съобщения на база IP или MAC адреси като защитни стени, прокси сървъри или виртуални мрежи [2, 5]. Осигурява се удостоверяване на комуникиращите страни чрез ПИС за взаимно удостоверяване на комуникиращите страни и съобщенията, като схеми за цифров подпис, например DSA и DSS, кодове за удостоверяване на съобщения като HMAC [5], протоколи за сигурност SSL (RFC 6101) и TLS (RFC 5246), услуги за отдалечено удостоверяване като RADIUS (RFC 2865) и Kerberos (RFC 1510) [2, 4, 5]. Такава техника например е прилагането на взаимно удостоверяване чрез Kerberos и последващо установяването на TLS () тунел за защита в транспортния слой [2, 3, 5]. Използването на подобен механизъм избягва предаването на пароли по мрежата. Други техники, използвани от компонента са механизми за оторизация и контрол на достъпа, дефинирани от приетата политика за сигурност като списъци за контрол на достъпа (ACL), групови политики (Group policies) и ограничения на акаунтите [5].
3. Компонент *„Криптографска защита“* се грижи за сигурността на обменяните данни чрез криптографски техники за осигуряване на цялостност и поверителност на информацията. Използват се симетрични (AES) и асиметрични (RSA) криптографски алгоритми [2, 4, 5]. Криптографските механизми използват предварително дефинирани или установени по време на процеса на взаимно удостоверяване ключове.
4. Компонент „К*онфигуриране и управление“* осигурява прилагане и контрол на политиката за сигурност, управлява и конфигурира останалите компоненти. Компонента осигурява конфигуриране на шлюзове и защитни стени, сегментиране на мрежата, както и актуализация на софтуер и фърмуеър.
5. Компонент *„Наблюдение и Анализ“* извършва мониторинг и анализ на мрежовите данни. Той събира и съхранява данни за събития и инциденти, свързани с нарушение на сигурността, идентифициране на заплахи и с успешно предотвратяване на атаки. Събраните данни позволяват анализ на текущото състояние на системата и заплахите към нея, както и извършване на прогнози за бъдещи рискове. Събраните данни представляват конфиденциална информация, която също трябва да бъде надеждно защитена. Изтичане и може

да доведе до допълнителни, много по-успешни атаки, защото директно показват слабите места на системата. Съществен момент е възможността агента на заплахата да инжектира фалшиви данни в компонента, като по този начин да се маскират успешните атаки и те да останат скрити. Компонента включва ПИС като контрол на достъпа, дълбочинна проверка на пакети, откриване на проникване и анализ на журнали.

6. Компонентът *„Защита на данните“* осигурява поверителност, цялостностност и наличност на данните които се комуникират, както и на оперативните данни, и данните за наблюдение и конфигурация. В зависимост от заложената политика за сигурност в компонента *„Комуникационна политика за сигурност“*, се взимат в предвид различни разпоредби, регулации и изисквания, регулиращи предаването на различни типове данни. Обикновено те касаят чувствителните за организацията данни и личните данни. Чувствителните данни трябва да бъдат защитени както докато са в покои, така и при тяхната комуникация. Съществуват регулации, които регулриарт транспортирането и съхраняването на лични данни в различни географски региони, което също трябва да бъде съобразено от компонента, респективно системата. Компонентът използва ПИС като контрол на достъпа, криптиране, изолиране, филтриране и др.



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

7. Компонент „Комуникационна политика за сигурност“ осигурява изпълнението на политиките за сигурност и определя как мрежовите компоненти комуникират помежду си. Политиката за сигурност на системата отразява околната среда – изискванията на всички заинтересовани страни и техните гледни точки. Тя включва нормативни изисквания, регулаторна среда, действащото законодателство, изискванията към системата от страна на организацията, в зависимост от бранша в които оперира, различни изисквания към комуникираните данни, условията на работа и други изисквания.

3.3. Проектен модел на системи за информационна сигурност в организации. 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.

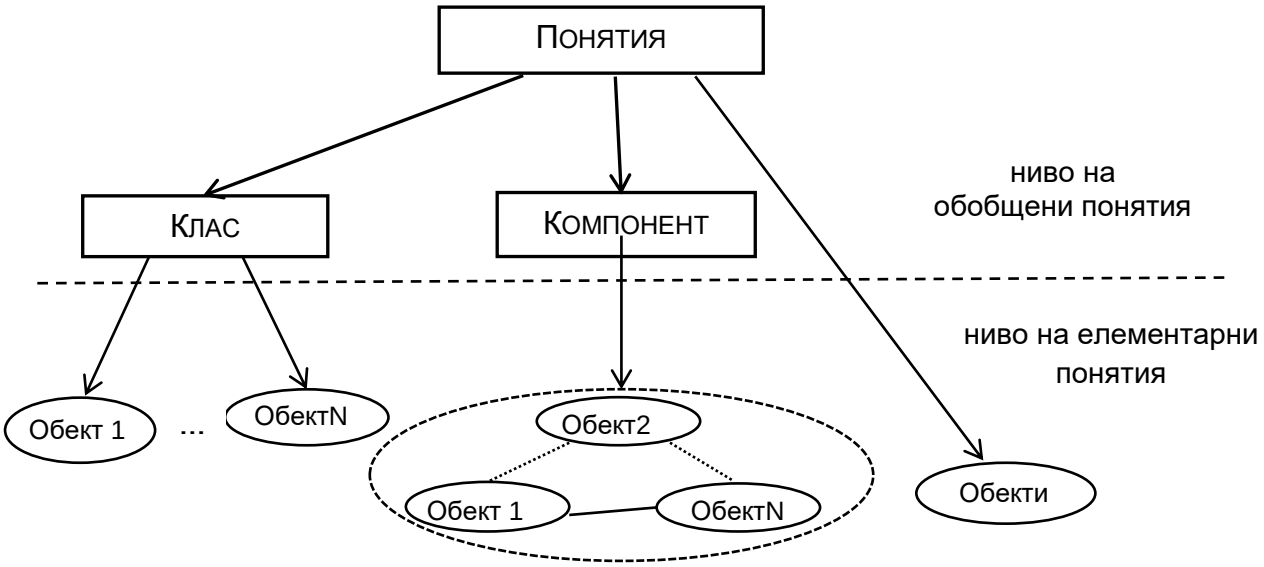
Преминаване от понятия в обекти

От Фигура 19 се вижда, че понятията може да се разглеждат на две нива – ниво на обобщени понятия и ниво на елементарни понятия. Вторите отразяват главно несъставни прости обекти. Понятията от първо ниво съдържат в себе си някаква идея, която е резултат на обобщение от определена степен. Такива идеи обикновено се свързват с разбирането за категория. В някои случаи това е категория, отразяваща обобщена идея от вид *Клас*. Класът включва в себе си подобни несвързани обекти. Категорията *Компонент* представлява нещо цялостно, което е част от нещо по-голямо, например система. Компонентът се състои от свързани помежду си обекти.
Вижда се, че понятието може директно да се отнесе към един обект от обектно-ориентираната парадигма или към група от такива понятия, които са с подобни качества и не са свързани помежду си или към свързани по някакъв начин различни обекти (Фигура 19).

Когато концепцията е обобщено понятие, тя може да бъде както компонент, така и обект, представен чрез клас. Класът е обобщение на компонента и обхваща няколко подобни обекта. Нашия подход за създаването на проектен модел включва трансформация на концептуалния модел, представен чрез мета-модели включени от нас в СИС. Мета-моделите се състоят от основни компоненти, като всеки компонент може да бъде представен като обект.

Обобщеният модел на проблемната област на СИС, представен с концептуалния модел от Фигура 14 може да бъде трансформиран в обектно-ориентиран проектен модел чрез използването на инструментариума на UML Чрез различните диаграми, поддържани от езика лесно можем да представим проектния модел.

Проектният модел се състои от две части - архитектурен и функционален модел показващи неговата архитектура и начина му на функциониране. Архитектурния модел на СИС може да бъде представен чрез статични UML диаграми, а Функционалния модел – чрез динамични UML диаграми, представящи динамични характеристики, поведение и взаимодействие.



Фигура 19. Понятие, Клас и Компонент

3.3.1 Обектно-ориентиран (ОО) подход за моделиране чрез използване на унифициран език за моделиране (UML)

Обектно-ориентиран език за описание UML

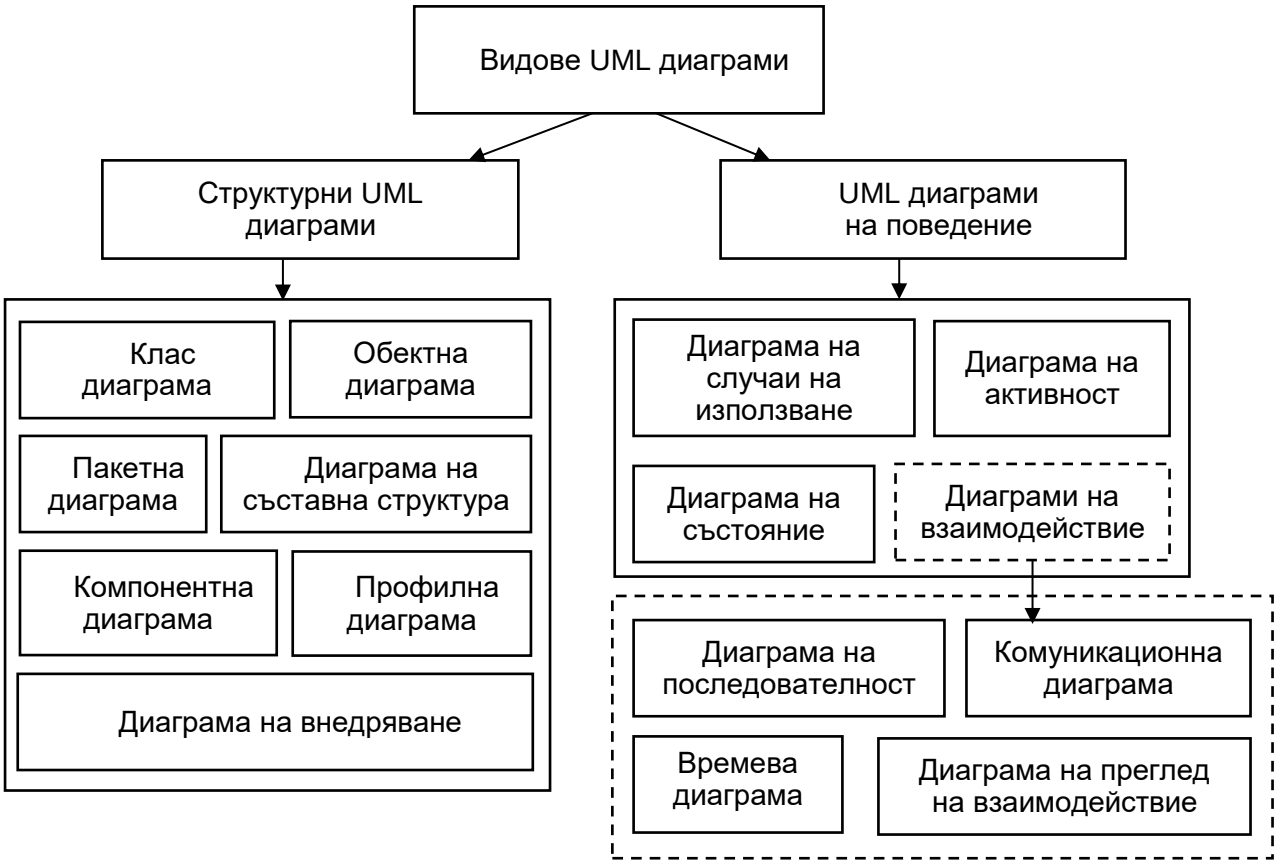
UML поддържа няколко вида диаграми, които могат да варират според версията на езика и осигуряват различни изгледи на системния модел (Фигура 20).

Първият вид са т. нар. „Структурни диаграми“ (Structural Diagrams), представящи 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).

„Клас-диаграма“ (Class Diagram)

Клас-диаграмата е структурна диаграма, представяща статичен изглед на обекта. Тя описва колекции от класове, атрибути, интерфейси, асоциации и операции на класа, както и ограниченията, наложени на системата. Клас-диаграмите се използват широко при моделирането на обектно ориентирани системи, защото те са единствените UML диаграми, които могат да се представят директно чрез обектно-ориентирани програмни езици. Основните компоненти на клас диаграмите са класове, представяни с правоъгълник и съдържащи атрибути и методи на класа. Отношенията между класовете или обектите могат да бъдат няколко вида: „Връзка“, „Асоциация“, „Агрегация“, „Композиция“, „Генерализация“ и „Зависимост“. Броят на отношенията се отбелязва с число върху връзката.



Фигура 20. Видове UML диаграми

Отношение „*Връзка*“ обозначава връзка между два обекта, например между два атрибута или между атрибут от единия клас и метод от другия клас.

При „*Асоциация*“ единият обект указва (реферира) другия чрез определена зависимост. Асоциацията може да бъде еднопосочна и двупосочна.

„*Композиция*“ е отношение, указващо множествена съставна връзка между класовете/обектите, което се запазва само ако всички съставни връзки са налице. Това отношение реализира логическа операция „И“.

„*Агрегация*“ е отношение на един клас/обект с друг, обозначаващо множествена съставна връзка между тях и притежаващо свойството да не се разпада при отпадане на единична връзка, т.е. реализира се логическа операция „ИЛИ“.

Отношение тип „*Генерализация*“ указва, че един клас/обект включва (наследява)

всички атрибути и операции на друг клас/обект, но добавя към тях и допълнителни атрибути и операции

Отношението „*Зависимост*“ указва, че двата класа/обекта са зависими един от друг, като всяка промяна на единия предизвиква промяна в другия. Тази зависимост се указва с прекъсната линия и посока на зависимостта

„Обектна диаграма“ (Object Diagram)

Тази диаграма може да се разглежда като частен случай на "*Клас-диаграмата*". Обектната диаграма визуализира връзката между конкретни обекти или примери на класа (instance) на класове от "*Клас-диаграмата*" в даден момент от времето. Тя отразява поведението на системата в реално време. За разлика от класовете, обектите включват конкретни данни и атрибути. Визуализират се в правоъгълници включващи име на обекта и класа към които той принадлежи. Диаграмата показва и връзките между обектите в даден момент, като поддържа същите типове връзки (отношения) като клас диаграма.

„Пакетна диаграма“ (Package Diagram)

Пакетната диаграма показва как системата може да бъде разделена на физически или логически групи чрез групиране на семантично свързани елементи в единна структура. Чрез тях се представя организацията на уедрени в пакети други типове и връзките между тях. Най-често се организират "*Клас-диаграми*" и „*Диаграми на употреба“.*

„Диаграма на съставна структура“ (Composite Structure Diagram)

Този вид структурна диаграма показва вътрешната структура на класовете, представлявани с "*Клас-диаграми*", включително тяхното взаимодействие с други части на системата. Тя показва конфигурацията и връзката на отделните съставни елементи, които заедно осигуряват функционалността на съдържащия ги класификатор. Диаграмата на съставна структура визуализира портове и интерфейси. Портовете са точките на взаимодействие на класификатора с външната среда, а интерфейсите показват по какъв начин протича това взаимодействие (протоколи, обменяна информация).

„Компонентна диаграма“ (Component Diagram)

Компонентната диаграма представя системата чрез нейните основни елементи, наречени в UML „компоненти“, връзките между тях, техните интерфейси и зависимости. Диаграмата се използва за визуализиране на структурата на системата, моделиране на връзките между елементите, както и физическите аспекти на системата. Тази диаграма не описва функционалността на системата, а визуализира нейните физически елементи, осигуряващи тези функционалности. Тези елементи са подсистеми, устройства, библиотеки, пакети, файлове и други. Компонентната диаграма описва организацията на елементите в определен момент - статичния изглед на системата. Тя представя само част от системата. За да се представи цялата система се използва колекция от компонентни диаграми. Компонентната диаграма представя връзките между отделните елементи (компоненти) , които от своя страна се състоят от отделни части, интерфейси и портове -точки на взаимодействие с външната среда, като всеки порт може да разполага със собствен интерфейс. Връзките (отношенията) между компонентите са същите като в „*Клас диаграма*“.

„Диаграма на внедряване“ (Deployment Diagram)
Диаграмата за внедряване се използва за моделиране внедряването на проектираната система в реални условия. Този вид диаграма показва конфигурацията на физическите устройства (хардуер), както и връзката и взаимодействието им със софтуерните пакети. Диаграмата на внедряване се състои от Възли, Артефакти, Контейнери, Интерфейси и съставни елементи, наричани „Компоненти“ в UML.
Възела е среда за изпълнение на софтуер. Той може да бъде както апаратно устройство (хардуерен сървър, работна станция, запаметяващо устройство), така и софтуерен продукт (операционна система, фърмуеър, база данни, уеб сървър). Артефактът е продукт, получен в процеса на разработване на софтуера. Контейнерът е вид възел, които може да съдържа в себе си няколко съставни елемента, например софтуерни и/или апаратни средства. Интерфейсът служи за комуникация между отделните съставни елементи.

„Профилна диаграма“ (Profile Diagram)
Профилната диаграма осигурява механизъм за разширяване и персонализиране на UML, чрез дефиниране на нови групи конструкции, със специфични за домейна или платформата свойства и ограничения. Разширенията се дефинират чрез стереотипи, които добавят нови класове към даден мета-клас. Стереотипа може да добави към мета-класа нови атрибути или ограничения. Например може да бъде добавен нов клас чрез стереотипи „Рутер“ и „Защитна стена“ към съществуващ мета-клас „Мрежова Комуникация“. Профилните диаграми осигуряват механизъм за разширяване и персонализиране на UML, чрез дефиниране на нови групи конструкции, със специфични за домейна или платформата свойства и ограничения. Разширенията се дефинират чрез стереотипи, добавящи нови класове към даден мета-клас. Стереотипа може да добави към мета-класа нови атрибути или ограничения.

Вторият вид UML диаграми са „*Диаграмите на поведение*“ *(Behaviour Diagrams),* Те представят взаимодействието и моментните състояния на компонентите в модела, показват 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:

- „Диаграма на случай на употреба“ (UseCase Diagram),
- „Диаграма на активност“ (Activity Diagram),
- „Диаграма на състояние“ (State Chart Diagram).

„Диаграма на случаи на използване (Use Case Diagram)
Този вид диаграма отразява изискванията към функционалността на системата. Тя е средство за описание на комуникацията с потребителите и други заинтересовани страни относно целите на системата. Диаграмата на случай на използване показва взаимодействието между системата и различни субекти, например потребители и предоставят описание на начина по които системата взаимодейства с тях. "Случай на използване " или "Казус" се нарича единична задача, изпълнявана от системата или част от системата. Той осигурява абстрактен поглед към начина на изпълнение на дадената задача, като се абстрахира от конкретно изпълнение и може да се опише чрез блок диаграма. Чрез този вид диаграма се описват сценарии за използването на системата и взаимодействието и с различни субекти или обекти - потребители, софтуер, хардуер или подсистеми. Диаграмата използва няколко основни примитива - Потребителски казуси, Актьори и Взаимодействия. Потребителските казуси се визуализират чрез елипса и представят определена функционалност на високо ниво.

Актьорите са субектите, взаимодействащи със системата. Такива са например потребителите, но могат да бъдат и техническа поддръжка, разработчици и др. Актьорите изпълняват различните сценарии на използването на системата. Сценариите могат да се изпълняват от един обобщен актьор или от множество различни актьори. Освен хора, актьори мога да бъдат и други системи или подсистеми, ако системата изпълнява задачи за тях. Основните типове взаимодействие са асоциация, включване, разширение и обобщение между казусите и/или актьорите. При взаимодействието от тип *„асоциация“* се обозначава връзката между даден актьор и потребителски случай (казус). Асоциацията указва че актьора осъществява този потребителски случай. Взаимодействието от тип „в*ключване*“ означава че един казус включва функционалността на друг казус. Чрез този тип връзка се избягва повторение на сценарий в по-сложни (съставни) случаи. Аналогията е извикване на външна процедура. Взаимодействието от тип „р*азширение*“ указва че даден потребителски случай допълва или разширява друг случай, като по този начин се променя и неговото поведение или резултат. Връзката тип „*обобщение*“ (генерализация) указва че дадения потребителски случай е разновидност на друг, обобщен случай.

„Диаграма на активност“ (Activity Diagram)
Диаграмата на активността се използват за визуализиране на последователността на дейностите в даден процес. Те показват работния поток от начална точка до крайната точка, и описват подробно вариантите за взимане на решения (условни разклонения), логиката на поведение, детайлизиране на процеси, при възникване на паралелна обработка на изпълнение на определени действия. Този тип диаграми са особено полезни за моделиране на различни дейности, например бизнес процеси, алгоритми на действие на различни блокове или детайли. Диаграмата на активност се състои от следните примитиви: начало, преходи, действия, разклонение, обединение, сливане, условно разклонение и край.

„Диаграма на състояние“ (Statechart Diagram)
Диаграмата на състояние се използват за моделиране на динамичния характер на системата. Чрез нея се представя поведението на системата и на нейните елементи (класове, подсистеми, пакети). Диаграмата на състояние визуализира последователността на състоянията, през които даден обект или елемент преминава по време на жизнения си цикъл, в отговор на различни събития, заедно с неговите реакции на тези събития. Този тип диаграми са полезни за моделиране на реактивни системи - системи, които реагират на външни или вътрешни събития. Съставните елементи на диаграмите на състояние са същите като елементите на диаграмите на активност, с тази разлика че примитива „Действие“ е заменен с примитив „Състояние“.

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

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

„Диаграма на последователност“ (Sequence Diagram)

Диаграмата на последователност показва времевата последователност на взаимодействията между обектите в системата. Тя представя взаимодействието като комуникация, а събитията които ги задействат като съобщения или „обаждания“ и „отговори“. Тази диаграма не е предназначена за показване на сложна процедурна логика, а по-скоро за опростена линейна последователност от взаимодействия между обектите, представяща тях и комуникацията им един с друг. Фокусът при диаграмата е върху комуникацията. Тя се състои от: име на обекта, представен като правоъгълник с име на клас:име на обект; жизнена линия в посока надолу, представяща събитията в течение на времето; съобщения и отговори между обектите, които могат да бъдат синхронни и асинхронни; активиране изпълнение на дадено действие, предизвикано от съобщение; отговор с резултат; както и съобщения към самия обект.

„Комуникационна диаграма“ (Communication Diagram)
Следващият тип диаграма на взаимодействие е *„Комуникационна диаграма“,* позната и като *„Диаграма за Сътрудничество“ (Collaboration Diagram).* Тя показва взаимодействията между обектите и връзките между тях, представени като комуникация чрез съобщения. Съобщенията са номерирани, като номерацията показва тяхната последователност. Диаграмата моделира потока на съобщенията между обектите, без да се взима предвид времето. Изборът между двата вида диаграми зависи от изискванията към системата. Ако е важна времевата последователност, се използва *„Диаграма на последователност“*. Ако се изисква представянето на организацията на взаимодействието между обектите в системата, се използва *„Комуникационна Диаграма“.*

„Времева диаграма“ (Timing Diagram)
Тази диаграма представя промяната в състоянието или стойността на един или повече елементи с течение на времето. Тя показва и взаимодействието между събитията във времето, както и ограниченията за време и продължителност, които системата налага към тях. Времевата диаграма могат да имат 2 вида жизнени линии – Жизнена линия на състоянията и Жизнена линия на стойностите. Линията на състоянията показва промяната на състоянието на даден елемент с течение на времето. Оста X показва изминалото време в избраните единици, а оста Y е отразява състоянията. Линията на стойностите показва промяната на стойността на даден елемент с течение на времето. Оста X показва изминалото време в избраните единици, а оста Y е отразява промяната на стойностите.

„Диаграма на преглед на взаимодействие“ (Interaction Overview Diagram).
Тази диаграма представя комуникацията между обекти в системата. Тя се фокусира най-вече върху предаването на съобщения и как тези съобщения съставляват дадена функционалност на системата. Целта на диаграмата е да покаже как обектите реализират конкретни изисквания на системата. Диаграмата на преглед на взаимодействието представлява форма на *Диаграмите на активност*, при която възлите представляват *Диаграми на взаимодействие*. Те могат да включват други диаграми на взаимодействие - *Диаграми на последователност, Комуникационни диаграми и Времеви диаграми*. Въпреки че елементите на Диаграмата на преглед на взаимодействието повтарят тези на *Диаграмите на активността*, те въвеждат два нови елемента – „Възникване на взаимодействие“ и „Елемент на взаимодействие“. Елементите „Възникване на взаимодействие“ са препратки към вече съществуващи диаграми на взаимодействие. Възникването на взаимодействие се представя като правоъгълна рамка с означение „ref“ в горния ляв ъгъл и име. „Елементите на взаимодействие“ са подобни на елементите "Възникване на взаимодействие", но

показват самите диаграми на взаимодействие, вградени в правоъгълна рамка и с означение “sd” в горния ляв ъгъл.

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].

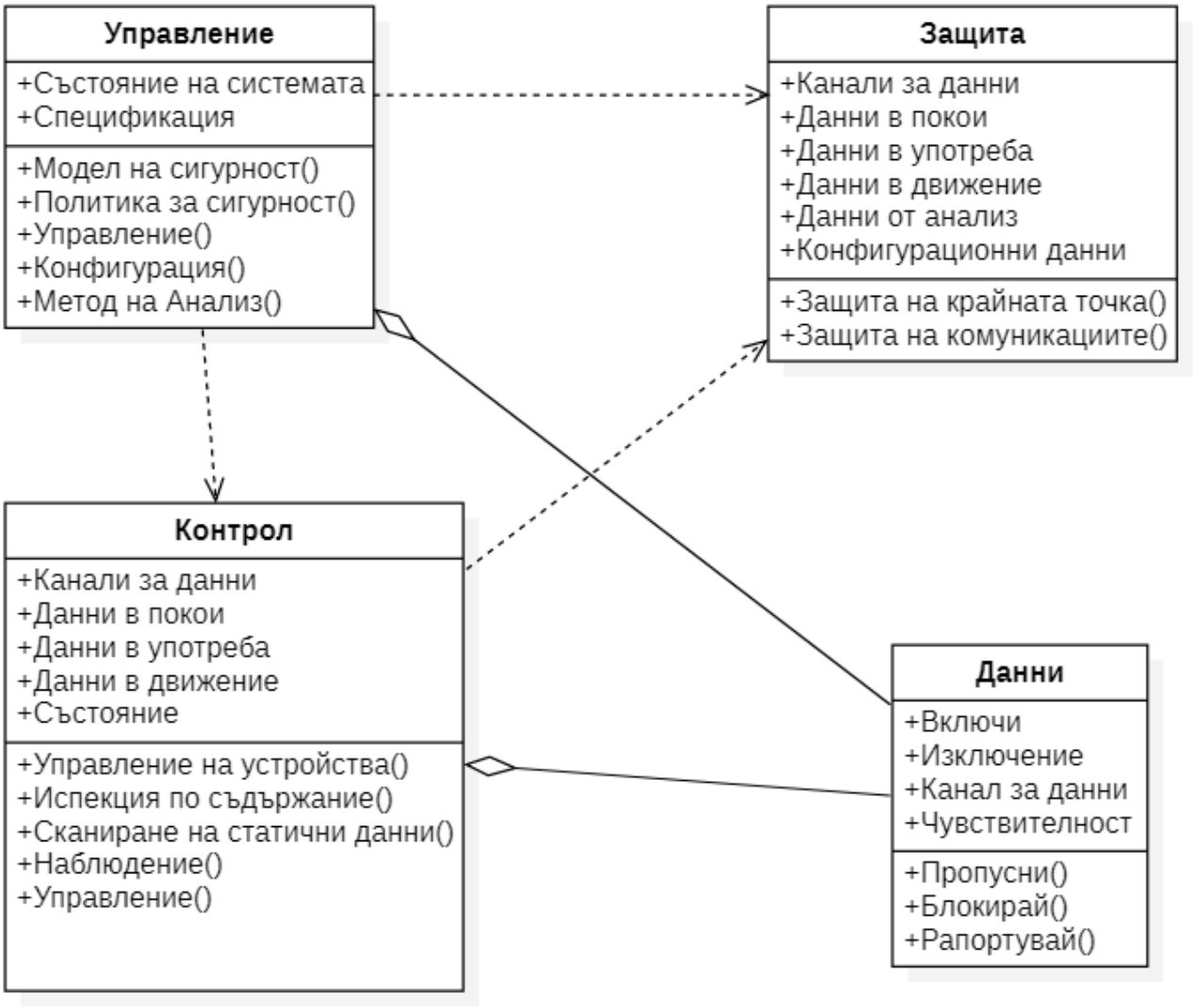
Концепцията на СИС, представена чрез обобщения мета-модел (Фигура 14) може да бъде описана чрез „Клас-диаграма“, както е показано на Фигура 21. Използваме същите понятия като в мета-модела, разделени като методи на четирите основни класа. Дефинираме четири класа – клас „Управление“, клас „Защита“, клас „Данни“ и клас „Контрол“:

- Класът „Управление“ притежава следните атрибути: “+Състояние на системата”, “+Спецификация” и съответните методи: “+Модел на сигурност ()”, “+Политика за сигурност()”, “+Управление ()”, “+Конфигурация ()” и “+Метод на Анализ ()”.
- Класът „Защита“ притежава следните атрибути: “+Канали за данни”, “+Данни в покои”, “+Данни в употреба”, “+Данни в движение”, “+Данни от анализ”, “+Конфигурационни данни” и съответните методи: “+Защита на крайната точка()” и “+Защита на комуникациите()”.
- Класът „Данни“ притежава следните атрибути: “+Включи”, “+Изключение”, “+Канал за данни”, “+Чувствителност” и съответните методи: “+Пропусни ()”, “+ Блокирай ()” и “+Рапортувай ()”.
- Класът „Контрол“ притежава следните атрибути “+Канали за данни”, “+Данни в покои”, “+Данни в употреба”, “+Данни в движение”, “+Състояние” и съответните методи „+Управление на устройства“, „+Испекция по съдържание“ и „+Сканиране на статични данни“, „+Наблюдение“ и „+Управление“.

На компонента “Модел и политика за сигурност” отговарят методите “Модел на сигурност”” и “Политика за сигурност” на компонента „Управление и Конфигуриране” отговарят методите „Управление“ и „Конфигурация“, на компонента „Наблюдение и Анализ“ отговарят методите „Наблюдение“ в класа „Контрол“ и „Метод на анализ“ в класа „Управление“. 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".

Тези методи изпълняват съответната функционалност като компонентите от мета-модела "Модел и политика за сигурност", конфигурират и управляват останалите класове чрез атрибутите "Спецификация","Състояние на системата" от класа „Управление" и методите "Наблюдение" и „Управление" от класа „Контрол". Методите "Защита на крайната точка" и "Защита на комуникациите" осъществяват защитата на



Фигура 21. UML „Клас диаграма" на СИС

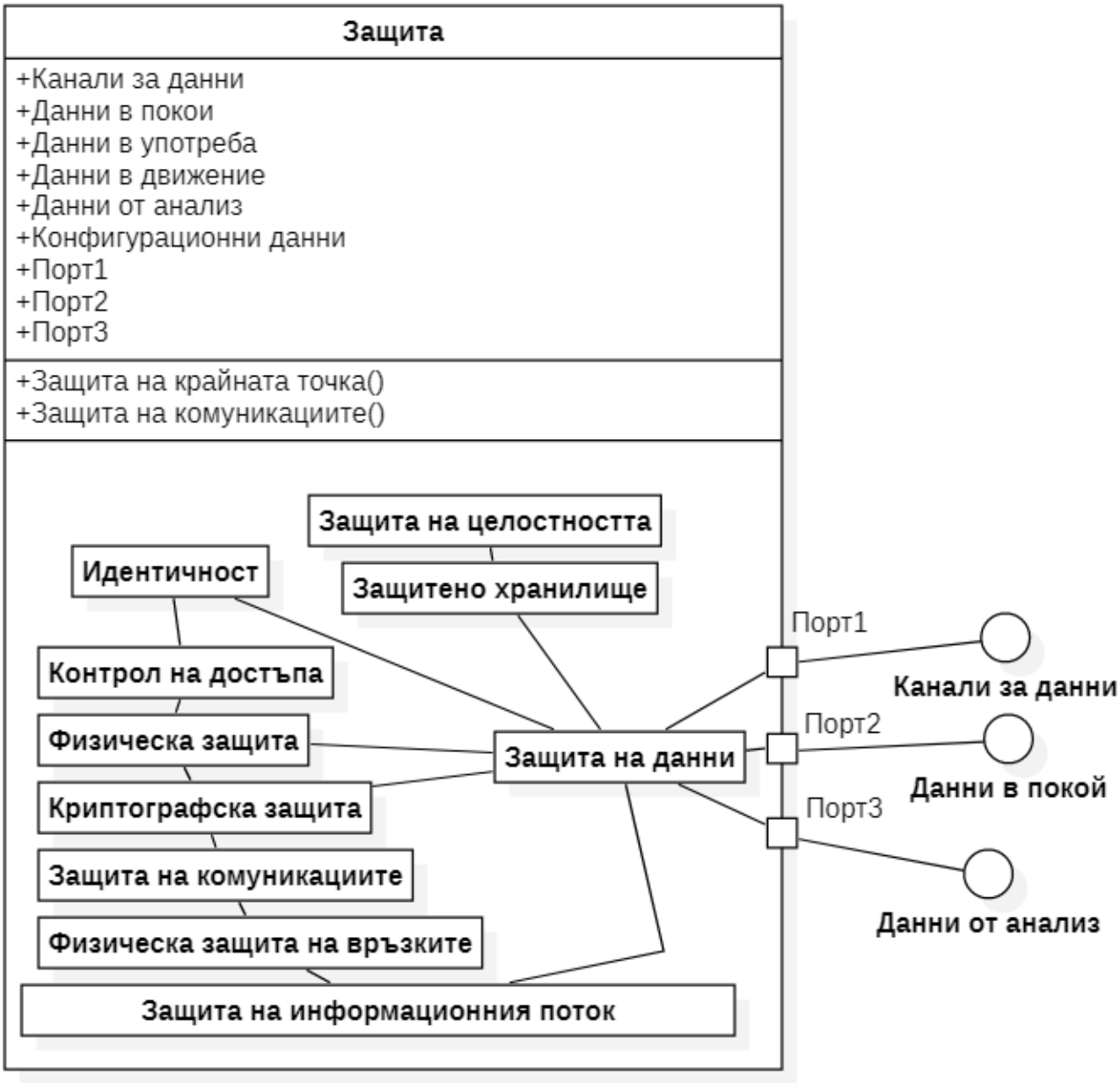
данни в крайните точки при комуникация. Данните могат да са в три основни състояния „Данни в движение", „Данни в употреба" и „Данни в покой", представени като атрибути на класовете „Защита" и „Контрол". Методите „Управление на устройства", „Испекция по съдържание" и „Сканиране на статични данни", „Наблюдение" и „Управление" на класа „Контрол" осигуряват контрола на съдържание на данните при преминаване през периферни или комуникационни устройства и при сканиране на статични данни, разположени в запаметяващи устройства, дискови масиви и мрежови шерове. Така

дефинирани, класовете, методите и атрибутите в тях описват точната функционалност на обобщения мета-модел (Фигура 14), чиято функционалност и функция на отделните компоненти вече е разгледана в глава 3.2.1.

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. Структурните елементи на класа отговарят на детайлните модели на



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

концепциите „Защита на крайните точки“ от Фигура 17 и „Защита на комуникациите“ от Фигура 18. В основата на тази структура са компонентите „Защита на цялостността“ и компонента „Защитено хранилище“, които създават защитена база, гарантиращи че системата не е компрометирана, функционира точно както е проектирана, и осигуряващи нейната Поверителност, Цялостност и Наличност. Компонентите „Идентичност“ и „Контрол на достъпа“ осигуряват точната идентификация на данните и че тяхната комуникация или обработка е потвърдена от системата, т.е. нямаме „инжектирани“ отвън токсични данни, целящи компрометиране на системата и нейната функционалност. Компоненти като „Физическа защита“ и „Криптографска защита“ осигуряват Цялостността на данните и заедно със „Защита на комуникациите“, „Физическа защита на връзките“ и „Защита на информационния поток“ осигуряват сигурността на данните и тяхната комуникация. Класът „Защита“ притежава 3 порта за всеки от трите основни типа от данни: „Данни в покой“, „Данни в движение“ и „Данни в употреба“, както и отделни интерфейси за тях.

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.

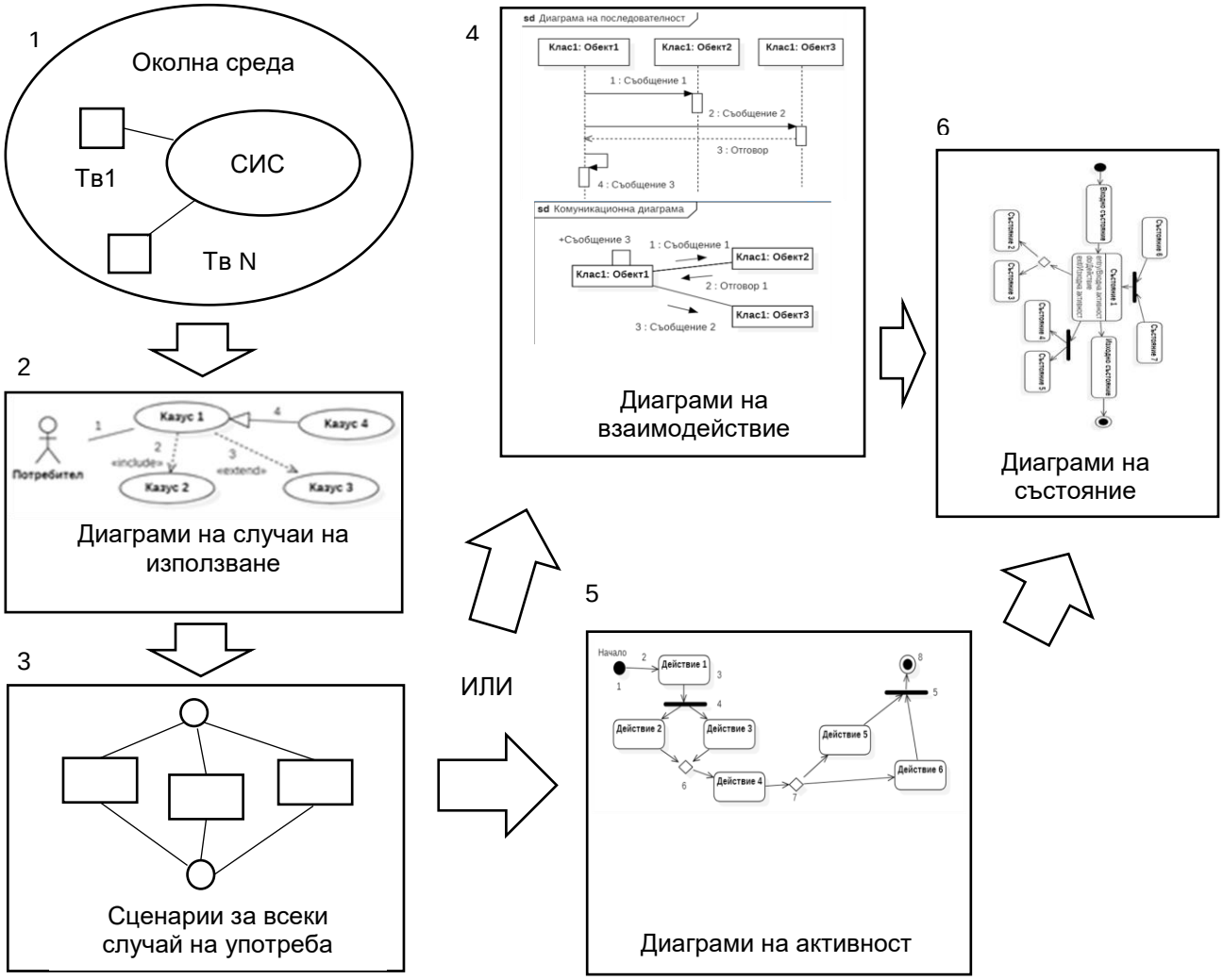
За всяко взаимодействие на СИС със външен субект/обект може да бъде съставена както базова диаграма на случаи на използване, описваща основното взаимодействие и поведение, така и разширени диаграми на случаи на използване, свързани с базовата диаграма и разширяващи базовата. Допълнителните диаграми наследяват 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.

Функционалният модел на СИС представяме чрез набор от следните UML диаграми:

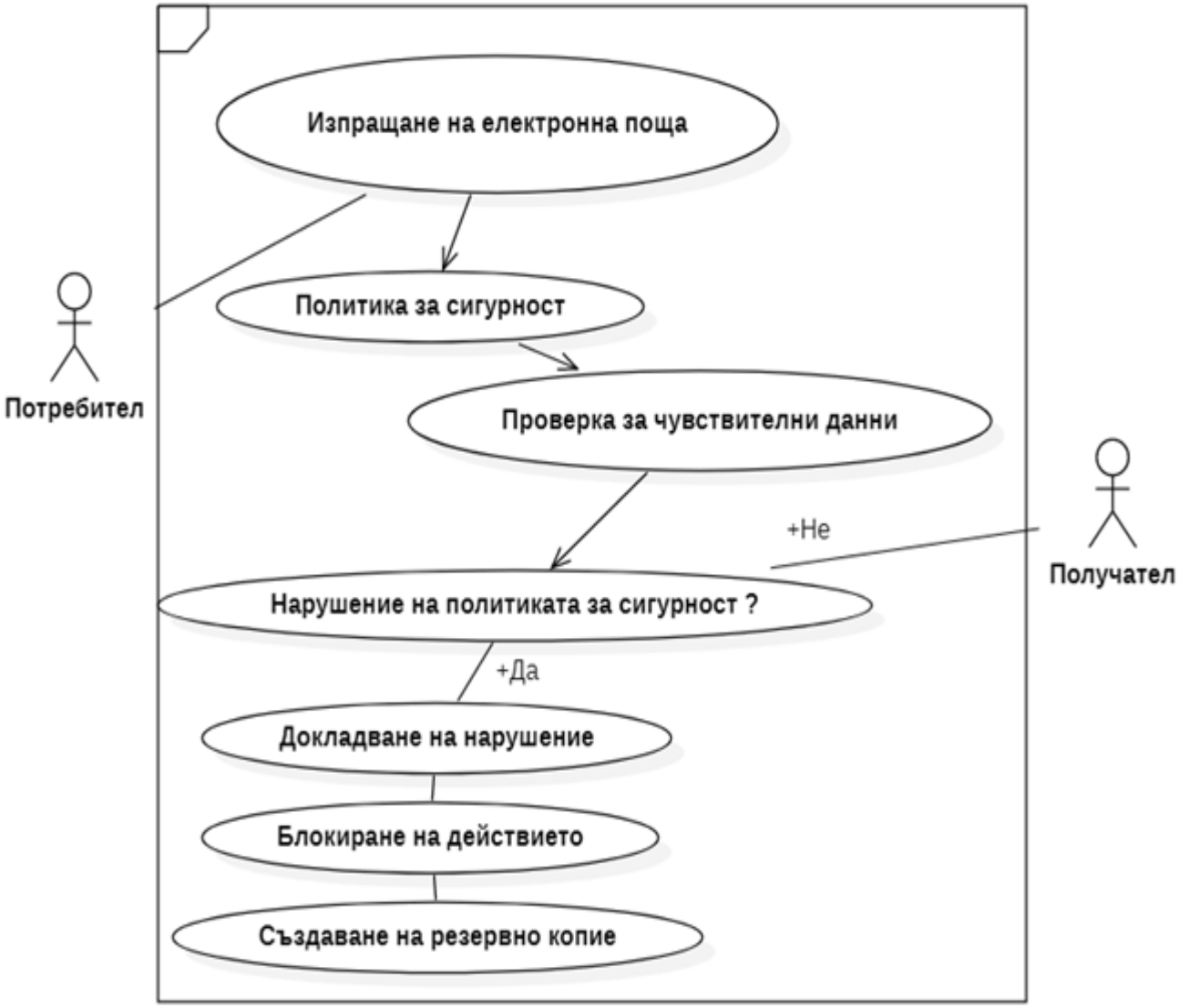
1. Диаграма на случай на използване;
2. Диаграма на преглед на взаимодействие на класове „Управление“, „Контрол“ и „Данни“;
3. Диаграма на преглед на взаимодействие на класове „Управление“, „Контрол“ и „Защита“;
4. Диаграма на последователност;
5. Диаграма на активност;
6. Диаграма на състояние.



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

Диаграма на случай на използване (Use Case Diagram)

Чрез Диаграмата на случай на използване от Фигура 24 се описва следния сценарий на взаимодействие на СИС с външен за нея субект: изпращане на електронна поща до външен за организацията получател. СИС проверява дали писмото съдържа чувствителни за организацията данни. Ако данните са чувствителни, политиката за сигурност определя дали потребителя има право да изпраща тези данни и кои получател има право да ги получава. Проверява се дали според политиката за сигурност времето на изпращане е разрешено. Например организацията може да забранява изпращане на всякакви данни извън официалното работно време. Ако времето за изпращане е разрешено, комуникацията може да бъде извършена, а данните изпратени. При нарушаване на политиката за сигурност комуникацията се забранява и се изготвя доклад за нарушението. Възможно е да се създаде резервно копие на писмото (документа) за по-нататъшно разследване.



Фигура 24. UML Диаграма на случай на използване „изпращане на електронна поща“

Аналогични сценарии могат да бъдат съставени в случай на копиране на информация върху външен носител (USB флаш памет), разпечатване на документ и т.н. При всяко

действие, свързано с комуникация с външен за системата субект и възможност за изтичане навън на чувствителна за организацията информация е необходима проверка на данните. Извършват се и допълнителни действия, съгласно политиката за сигурност на организацията – блокиране на действието, забрана на информационния канал, доклад, запазване на резервно копие и други.

Следващите UML диаграми, формиращи функционалния модел са диаграми на взаимодействие, описващи взаимодействието на класовете „Управление“, „Контрол“ и „Данни“ (Фигура 25) и класовете „Управление“, „Контрол“ и „Защита“ (Фигура 26). Класовете са част от Клас-диаграмата от архитектурния модел на СИС (Фигура 21).

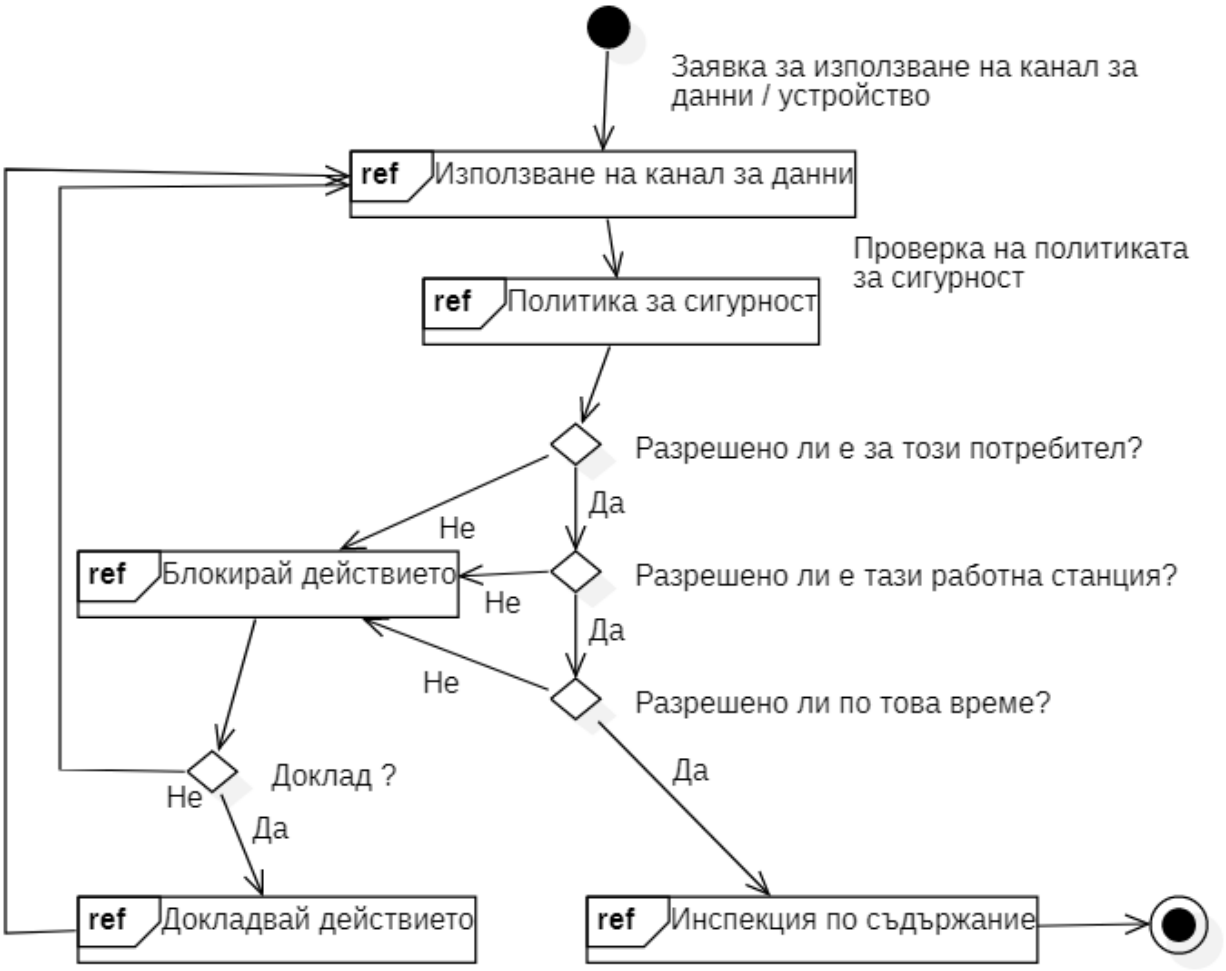
Показаната на Фигура 25 диаграма отразява взаимодействие на класове „Управление“, „Контрол“ и „Данни“ при инспекцията на потока от информация, преминаващ през даден комуникационен канал за съдържание на чувствителни за организацията данни.

Диаграми на преглед на взаимодействие на класове „Управление“, „Контрол“ и „Данни“

Фигура 25. Преглед на взаимодействие на класове „Управление“, „Контрол“ и „Данни“

При преминаването на данните през комуникационния канал - локална мрежа, безжична (Wi-Fi) връзка, USB порт, интерфейс за печат или приложения, услуги или действия като изпращане на електронна поща, печат на документ, запис на флаш памет и др, данните се сравняват с предварително зададените критерии, дефиниращи чувствителните за организацията данни. Това може да бъдат речници с ключови думи, RegEx (Regular Expression) изрази или специфични за организацията етикети и маркировки в документите и метаданните във файловете. Ако данните не отговарят на зададените критерии, СИС приема че те не са чувствителни и не нарушават политиката за сигурност. Данните се разрешават за комуникация и се изпращат до получателя, или се разрешава съответната операция – например копиране на външна флаш памет. Ако данните са идентифицирани като чувствителни се проверява политиката за сигурност относно необходимите действия, заложени в нея. Те евентуално се докладват и допускат към изхода или се докладват и блокират, като се извършват заложените при нарушение на политиката действия. Те могат да бъдат например изпращане на съобщение към администраторите или отговорните субекти, изпращане на сигнал към друга система или подсистема, блокиране на даден канал, операция или приложение, блокиране на потребителя и други.

Диаграма на преглед на взаимодействие на класове „Управление“, „Контрол“ и „Защита“



Фигура 26. Преглед на взаимодействие на класове „Управление“, „Контрол“ и „Защита“

Следващата диаграма (Фигура 26) отразява взаимодействието на класовете „Управление“, „Контрол“ и „Защита“ в процеса на проверка за спазване на приетата политика за сигурност при използване на определен канал за данни, използването на дадено приложение, протокол или операция, например печат на документ или изпращане на електронна поща. Първоначално се проверява дали дадения канал/приложение/операция е разрешен за потребителя. Ако политиката за сигурност не го разрешава, действието се блокира. В зависимост от политиката за сигурност може да се генерира доклад. Възможно е създаване на копия на документа или файла за по-нататъшно разследване. Ако действието е разрешено се преминава към следващите проверки: разрешено ли е действието върху работната станция; разрешен ли е потребителя върху работната станция. Ако отговорът е положителен се продължава с проверките, ако не е – се извършва блокиране и евентуално докладване. Последната проверка е дали времето в което се извършва действието е разрешено за дадената операция, потребител и работна станция. При положителен отговор се продължава с инспекция на съдържанието за идентифициране на чувствителни данни. При неразрешено действие се предприемат вече описаните действия според действащата политика за сигурност.

Диаграма на последователност

Чрез диаграмата на последователност от Фигура 27 се визуализира времевата последователност на взаимодействията между елементите на системата, осъществени чрез съобщения между тях. Диаграмата описва инспекция по съдържание на данни, протичащи през определени канали за данни, чрез съответните съобщения между елементите на системата. Чрез съобщение (1) „Проверка“ се инициира проверка на данните за чувствителност на данните. Чрез съобщение (2) се проверява дали данните са чувствителни съгласно политиката за сигурност. Ако данните са чувствителни се задава съответната команда към канала за данни. В този случай имаме два варианта, изразени чрез съответните съобщение (3) „Да, пропусни и докладвай“, и съобщение (4) „Да, спри“. Ако не е идентифицирана чувствителна

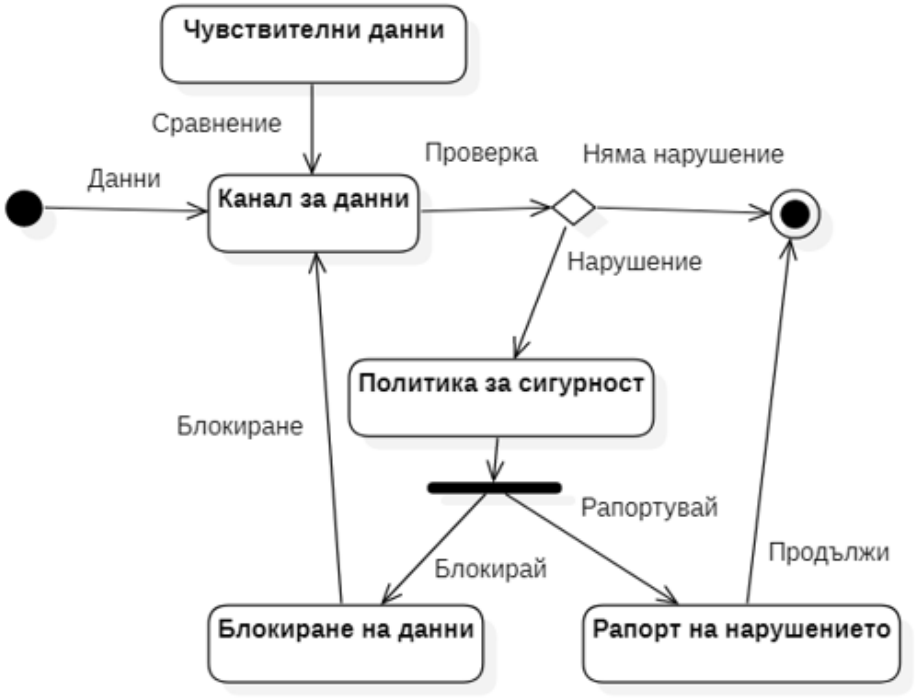
Фигура 27. UML Диаграма на последователност

информация се изпраща съобщение „Не, пропусни“ (5) и данните се изпращат на получателя. Чрез съобщение (6) се потвърждава извършеното действие и се изпраща съобщение „Доклад“ (7) към политиката за сигурност.

Диаграма на активност

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”. Подобни диаграми на активността могат да се създадат за всички методи от клас-диаграмата.

Каналите за данни се проверяват за чувствителна информация чрез сравняване на данните с критериите за чувствителни данни, заложени в приетата политика за сигурност. Ако има съвпадение, се констатира изтичане на данни и нарушение, след което се инициират предвидените в политиката за сигурност действия. Те могат да бъдат документиране на нарушението и/или блокиране, така че изтичането на данни да бъде възпрепятствано. Подобни диаграми на активност се създават за всички методи в съответните класове от клас-диаграмите.



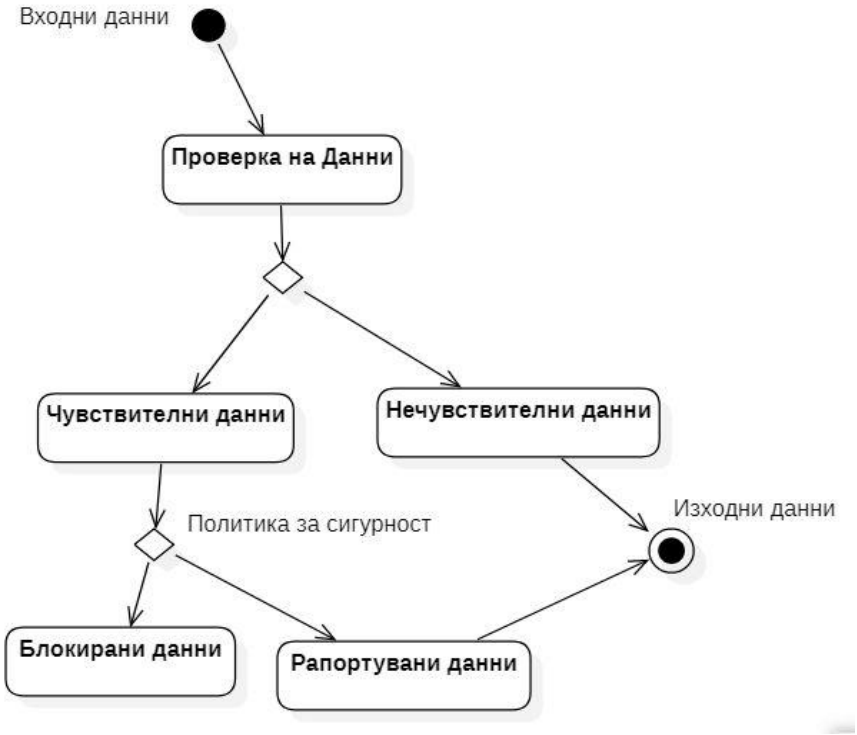
Фигура 28. UML Диаграма на активност на метода “Защита на крайна точка”

Диаграма на състоянието на клас „Данни“

Последният елемент от функционалния модел е диаграма на състоянието. Чрез набор от такива диаграми се описва динамиката в промяната на състоянието на основните елементи на СИС. На Фигура 29 е представена диаграма на състояние на клас „Данни“, представяща проверка за чувствителни данни в крайната точка от Обобщения модел на проблемната област на СИС от Фигура 12.

Диаграмата показва промяната в състоянието на данните при проверка за покриване на критериите за чувствителни данни, зададени в политиката за сигурност. Ако данните отговарят на критериите, заложени в модула „Модел и политика за сигурност“ в обобщения мета-модел, има два варианта: могат да бъдат блокирани и /или

докладвани. В първия случай те преминават в състояние „блокирани“ и не се допускат към изхода. Във втория случай те се рапортуват и се допускат към изхода.
Чрез диаграми на състоянието се представя промяната на състоянието на класовете от архитектурния модел на СИС.



Фигура 29. UML Диаграма на състояние на клас „Данни“

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;

Тези приноси на дисертационния труд са представени и публикувани в следните авторски публикации :

[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.

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 платформите 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 платформите 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 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 изгражда 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 типа СПИД.

Използвайки концептуалният мета-модел от Фиг.15, изграден от гледната точка „Обработка на информация“ е извършен анализ на водещи СПИД системи (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 (Таблица 9).

Изисквания към СПИД	СПИД				
	Cososys Endpoint Protector 5.0.2.1	Symantec Data Loss Prevention 14.6	McAfee DLP Endpoint 9.3.200	Forcepoint DLP 8.9	DeviceLock 8.2
Поддържани ОС					
MS Windows	✓	✓	✓	✓	✓
Apple Mac OS X	✓	✓	ограничено	✓	✓
Linux	✓	×	×	✓	✓
Реализация					
Софтуерна инсталация	✓	✓	✓	✓	✓
Хардуерен модул	✓	×	×	×	×

Виртуален имидж	✓	×	×	✓	×
Облачно базиран	✓	✓	×	✓	×
Управление на устройства (Device Control) **Data-in-Motion**	**Данни в движение (Data-in-Motion)**				
Управление на отдели	✓	✓	✓	✓	×
Списък с разрешени устройства	✓	✓	✓	×	✓
Позволява достъп "само за четене"	✓	✓	✓	✓	✓
Политики за устройство/ потребител/ компютър / група/ персонален клас	✓	✓	✓	✓	✓
Проследяване на файлове	✓	✓	✓	✓	✓
Копия на файлове	✓	✓	✓	×	✓
Офлайн временна парола	✓	✓	✓	✓	✓
Разрешаване само на криптирани устройства	✓	✓	✓	×	✓
Дистанционно задействане на USB криптиране	✓	×	×	×	✓
Проследяване на споделяне в мрежата	✓	✓	✓	×	✓
Аларма за използване на неоторизирано устройство	✓	✓	✓	✓	✓
Мерки против подправяне	✓	✓	✓	✓	✓
Инспекция по съдържание (Content Aware Protection)	**Данни в движение, Данни в употреба (Data in Motion, Data in Use)**				
Контрол на трансферите до: Външни памети /	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓

уеб браузъри / ел.поща/ ком. приложения/ споделяне на файлове/ социални медии /Други	✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓
Филтриране по тип на файлове	✓	✓	✓	✓	✓
Предварително дефинирани филтри за съдържание	✓	✓	✓	✓	✓
Поддръжка на регулярни изрази (RegEx)	✓	✓	✓	✓	✓
Персонализирани филтри по съдържание	✓	✓	✓	✓	✓
Списък с разрешени домейни	✓	✓	✓	×	✓
Списък с разрешени файлове по местоположение	✓	×	×	×	✓
Списък с разрешени мрежови споделяния	✓	✓	✓	✓	✓
Списък с разрешени адреси	✓	✓	✓	✓	✓
Наблюдение на клипборда	✓	✓	✓	✓	✓
Забрана на Print Screen	✓	✓	✓	✓	✓
Интеграция със SIEM	✓	✓	✓	✓	✓
Предварително дефинирани политики	✓	✓	✓	✓	✓
Хистерезис / Праг	✓	✓	✓	✓	✓
Сканиране на статични данни (eDiscovery)	**Данни в покой (Data in Rest)**				

Сканиране на съдържание и тип на файлове	✓	✓	✓	✓	✓
Криптиране на данни в покой	✓	✓	✓	✓	✓
Изтриване на данни в покой	✓	✓	✓	✓	✓
Забранителен списък по тип на файл	✓	✓	✓	✓	✓
Предварително дефиниран забранителен списък по съдържание	✓	✓	✓	✓	✓
Забранителен списък със съдържание	✓	✓	✓	✓	✓
Забранителен списък по име на файл	✓	✓	✓	✓	✓
Забранителен списък с (RegEx) регулярни изрази	✓	✓	✓	✓	✓
Защита на данни по HIPAA	✓	✓	✓	✓	✓
Хистерезис / Праг	✓	✓	✓	✓	✓
Разрешен списък по MIME	✓	✓	✓	✓	✓
Разрешен списък с файлове	✓	✓	✓	✓	✓
Пълно сканиране	✓	✓	✓	✓	✓
Инкрементално сканиране	✓	✓	✓	✓	✓

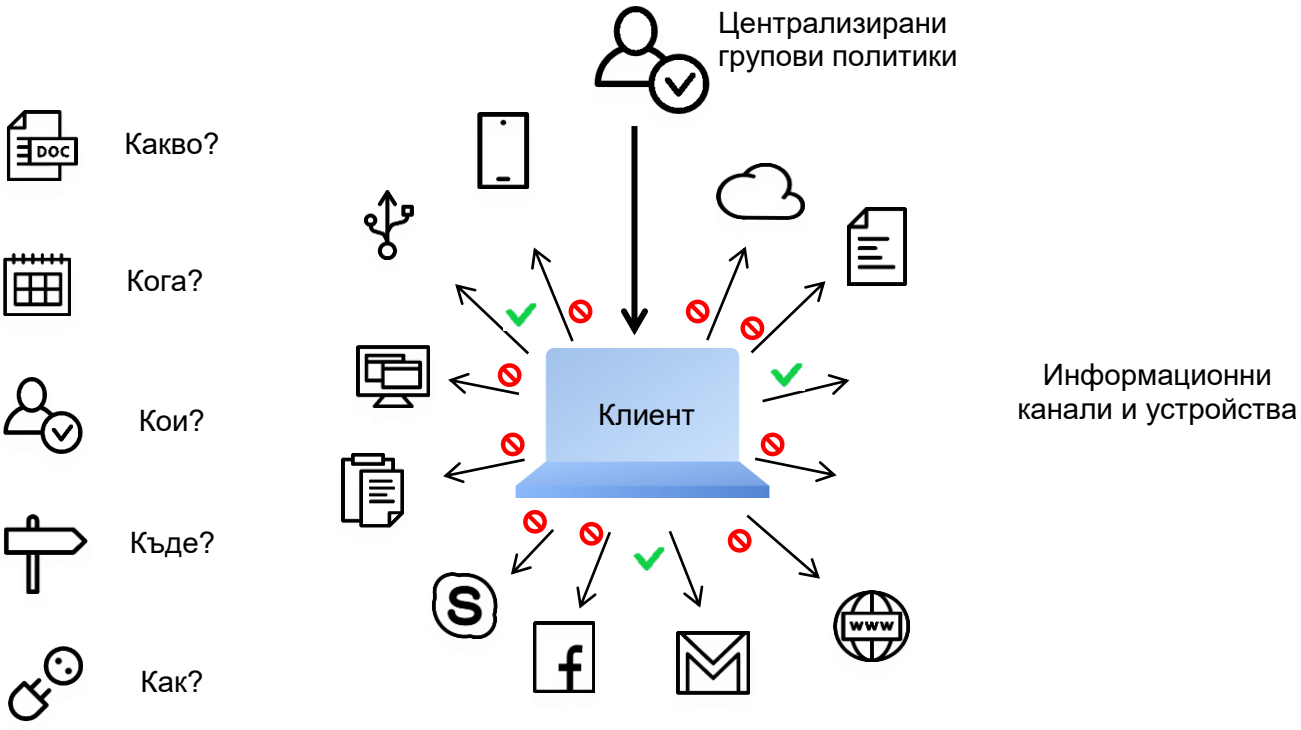
Таблица 9. Сравнителен анализ на съществуващи СПИД

Като резултат от анализа е избрана най-подходящата за нашите цели конкретна платформа за реализация. СПИД системата, избрана за реализация на СИС е част от нейната архитектура. В нашия случаи, на базата на анализа изборът пада върху СПИД системата 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

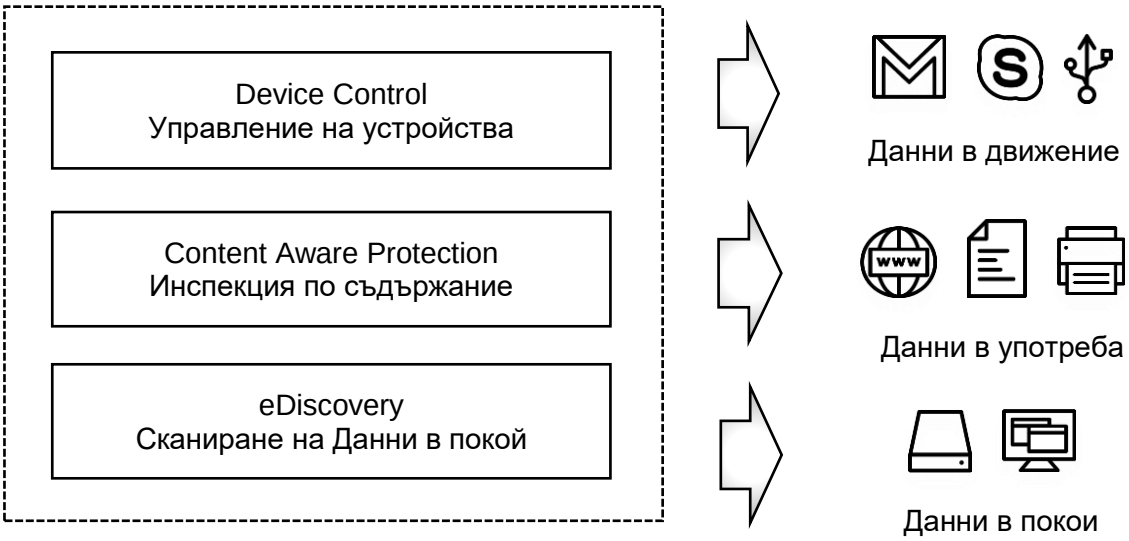
За създаването на ОО модел на реализация на СИС се използва избраната комерсиална СПИД Cososys EPP 5.0.2.1 [96]. Тя е базирана на клиент-сървър архитектура. Върху контролираните крайни точки (работни станции, лаптопи и сървъри) се инсталират клиенти, които комуникират с централния сървър и контролират комуникационните и информационните канали в съответствие с предварително дефинирана и централизирана политика за сигурност. СПИД платформата е в състояние да инспектира съдържанието на данните протичащи през комуникационните канали и по този начин да идентифицират чувствителна информация, зададена предварително с помощта на речници с предварително дефинирани специфични ключови думи, RegEx изрази или маркировки (етикети). Веднъж идентифицирани, чувствителните данни могат да бъдат блокирани, а действията докладвани. СПИД работят със всички видове данни от мета-модела на Фигура 15: “Данни в покой”, “Данни в движение” и „Данни в употреба”.

Платформата за реализация се състои от хардуерен сървър и софтуерни модули Device Control, Content Aware Protection и eDiscovery. Хардуерният сървър осигурява централизираното управление на СПИД, а отделните модули осигуряват различна функционалност: На Фигури 30 и 31 е показан принципа на действие и структурата на Cososys EndPoint Protector 5.0.2.1 [96], която е използвана за изграждането на ОО модел на реализация.



.

Фигура 30. СПИД „Cososys EndPoint Protector 5.0.2.1“ – Принцип на действие



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

Софтуерен модул Device Control
Този модул осъществява следните функции:

- Мониторинг, контрол и управление на всички портове и комуникационни канали, както и на всички свързани към контролираната работна станция периферни и запаметяващи устройства.
- Контролира данни от тип „Данни в движение“ и „Данни в употреба“, преминаващи през комуникационните канали изпращани извън организацията (изпращане на електронна поща, съхраняване в облачна услуга, копиране на външен флаш носител) или използвани от периферните устройства, например печат на документ от локален или мрежови принтер.
- Контролира каналите за данни и периферните устройства като разрешава или забранява тяхното използване от определени потребители или групи от потребители, отделни операции (четене, запис), както и контрол на тяхното използване според работното време.
- Създава „бял списък“ от разрешени устройства за определени потребители или отделни работни станции. По този начин в организацията може например да се забрани използването на неодобрени запаметяващи устройства от типа „USB флаш памет“ и да се разреши използването само на одобрени криптирани устройства.
- Забранява определени комуникационни канали или устройства извън работно време или за определени потребители.
- Позволява контрол на количеството данни които се обработват или използват от периферните устройства, например контрол на броя на разпечатаните от определени потребители екземпляри на даден документ.

Софтуерен модул Content Aware Protection
Чрез този модул се реализира инспекция по съдържание на всички данни, преминаващи през комуникационните канали в посока отвътре-навън. Данните преминаващи през тях могат да бъдат под формата на електронна поща, файлове, документи и други. Тяхното съдържание се инспектира за съдържание на чувствителна информация, като се сравнява с предварително дефинирани речници с ключови думи,

RegEx изрази или маркировки (етикети), чрез които дадената организация дефинира информацията като чувствителна. Системата осигурява различен достъп до чувствителната информация на отделни потребители, в зависимост от тяхното ниво на достъп и роля в организацията.

Софтуерен модул eDiscovery

С помощта на модула се сканира за наличието на чувствителни данни от типа „Данни в покой“, разположени върху работни станции, сървъри и мрежови дялове и които не се използват активно. Сканираните данни се сравняват с предварително дефинирани речници с ключови думи, RegEx изрази или маркировки (етикети). При съвпадение с критериите, данните се идентифицират като чувствителни, маркират се, докладват се и се изтриват или преместват ако политиката за сигурност го изисква.

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

За създаването на ОО модел на реализация на СИС се използват следните диаграми на езика UML:

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

UML „Пакетна диаграма“

Фигура 32. UML Пакетна диаграма на СИС

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

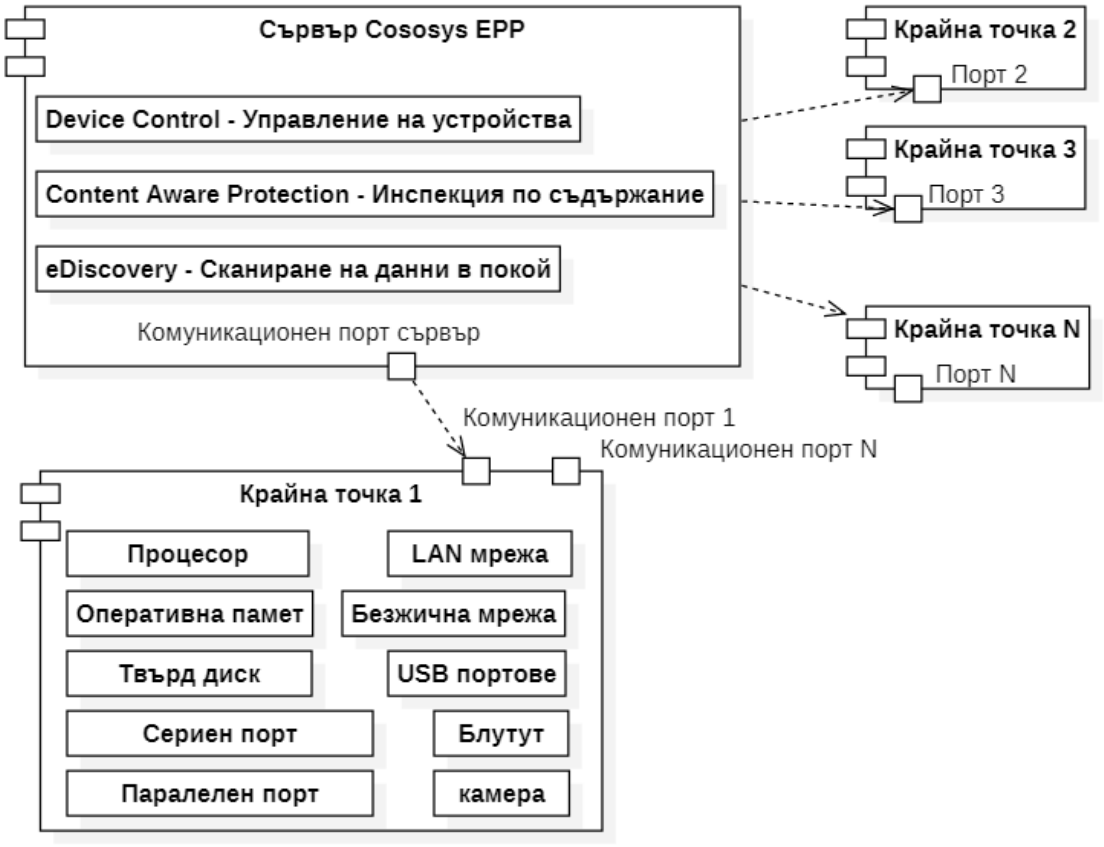
Пакетът *“Управление на устройства“* се състои от под-пакети с различна функционалност. Съответстващия модул от СПИД извършва контрол и управление на устройствата и информационните канали на всяка работна станция, (пакет „Устройства“), управлявайки правата за достъп (пакет „Права“) на отделни потребители или групи от потребители до списъка от „Устройства“, които са индивидуални за всяка работна станция (пакет „Работни станции“) и потребители (пакети „Потребители“ и „Групи“).

Пакетът *„Инспекция по съдържание“* се състои от отделни под-пакети. Под-пакетът „Политики“ съответства на възможността на модула Content Aware Protection“ да създава множество индивидуални политики за инспекция на списък от „Устройства“ за преминаването на чувствителни данни, които се идентифицират с помощта на списъци от „Черни списъци“ и „Бели списъци“. Тези списъци съдържат забранени и съответно разрешени ключови думи. В първия случай важи правилото всички е разрешено, с изключение на ключовите думи от „Черния списък“. Във втория случай правилото е „всичко, освен ключовите думи от белия списък е забранено“, т.е. пропускат се само данни от списъка. В двата списъка може да фигурират и списъци от устройства/канали за данни на работните станции във формата на забранени или разрешени за използване устройства от определени потребители или групи потребители.

Пакетът *„Сканиране на Данни в покой“* съответства на модула „eDiscovery“, осъществяващ сканиране за чувствителни данни в данни от типа „Данни в покой“. Модула използва дефинираните вече в предните два модула критерии за чувствителни данни, според правата за достъп на потребители или групи от потребители, които формират различни политики за сканиране, според списъците в под-пакета „Политики“ и списъци от автоматизирана обработка на резултатите в под-пакета „Резултати от сканиране“.

UML „Компонентна диаграма“

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 КОЙ 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.



Фигура 33. UML Компонентна диаграма на Cososys EPP 5.0.2.1

.

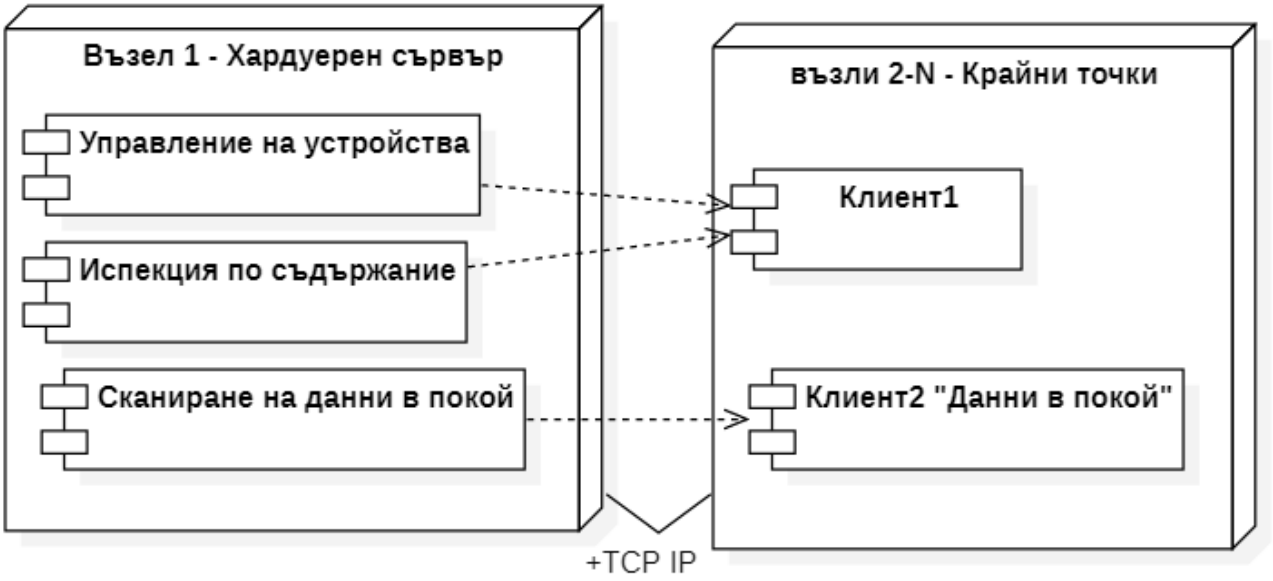
UML „Диаграма на внедряване“

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. Хардуерните компоненти, (СПИД, защитни стени, уеб сървъри, пощенски сървъри, сървъри за приложения) са представени като възли (nodes), софтуерните приложения, които се изпълняват в хардуерните компоненти, са представени като артефакти.

При съставянето на диаграмата за внедряване се преследват следните цели:

- Представя се общата топология и конфигурация на системата;
- Специфицират се възлите, необходими за разполагането и изпълнението на изпълнимите софтуерни компоненти;
- Показват се физическите връзки между отделните възли;
- Указва се местоположението на различни артефакти на отделни възли на системата;
- Отбелязват се критичните точки на системата, за да се даде възможност при необходимост за реконфигуриране на нейната топология с цел постигане на необходимата производителност

Примерна диаграма на внедряване на СИС 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 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 СИС

Чрез представената диаграма се указва топологията на СПИД. Върху хардуерен сървър, отбелязан като Възел 1 се инсталират софтуерните компоненти на СПИД, представени вече в компонентната диаграма на Фигура 33: “Device Control - Управление на устройства”, “Content Aware Protection - Инспекция по съдържание” и “eDiscovery – Сканиране на данни в покой“. Върху работните станции - Възли 2-N на Фигура 34 се инсталират два вида клиенти. Първият клиент (Клиент1) служи за контрол на данни в движение и данни в употреба и комуникира със софтуерните модули “Device Control - Управление на устройства” и “Content Aware Protection - Инспекция по съдържание”. Вторият клиент (Клиент 2 „Данни в покой) контролира данните в покой и комуникира с модула “eDiscovery – Сканиране на данни в покой“ от възел1. В диаграмата трябва да бъде посочена операционната система, необходима за съответния модул. Комуникацията между клиентите и съответните модули се осъществява чрез TCP/IP протокол. Възли 2-N, представляващи работните станции на потребителите могат да бъдат разположени на произволно географски отдалечено от сървъра място – централни или отдалечени регионални офиси, домашни офиси, лаптопи, използвани при командировка. При необходимост е възможно инсталирането на СПИД върху няколко хардуерни сървъра (възела), които да комуникират помежду си, или да са изолирани от другите с цел безопасност (секретни помещения).

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, пълно мащабна 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 механизми 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 и Таблици 1, 6 и 7. След влизането в сила на Общия регламент относно защита на личните данни - Регламент (ЕС) 2016/679 (GDPR) [67], 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 10. След това така описаните сценарии се добавят към съществуващата СИС, чрез избраната платформа за реализация от тип СПИД за осъществяване на защита в реални условия, съобразявайки се с отделните работни места и спецификата на работата им с различни видове 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 (UML диаграми)	Виж Приложение 1 1. Диаграма на случай на използване (Use Case Diagram) – Фигура 1.1 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 определени 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 10. 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 платформа от тип СПИД.

В два от субектите са направени подробни тестове и Доказване на концепцията (POC - Proof Of Concept) на платформа за реализация 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 Кибер сигурност 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 специфични 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 – Таблица 11.

Изпитания по 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.
Начин на провеждане	Създаване на политика за контрол трансфера на файлове или текстове, съдържащи лични/чувствителни данни чрез политики и правила за IBAN, ЕГН, ID, Passport, Credit Card Numbers, според описаният сценарий 1. Трансфер на файлове съдържащи лични/чувствителни данни чрез външни запаметяващи устройства (USB флаш памети). Проверка на резултатите..
Тестови операции	Минимум десет опита за трансфер на файлове или текстове, съдържащи лични/чувствителни данни чрез външни запаметяващи устройства (USB флаш памети).
Изпитания по 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.
Начин на провеждане	Създаване на политика за принудително криптиране на данни, пренасяни чрез USB флаш памети според описаният сценарий. Трансфер на файлове съдържащи лични/чувствителни данни чрез външни запаметяващи устройства (USB флаш памети). Използват се два вида външни запаметяващи устройства: хардуерно криптирани и обикновени, некриптирани. Проверка на резултатите..
Тестови операции	Минимум десет опита за трансфер на файлове или текстове, съдържащи лични/чувствителни данни чрез външни запаметяващи устройства (USB флаш памети).
Изпитания по 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 определени 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.
Начин на провеждане	Създаване на политика за контрол трансфера на файлове или текстове, съдържащи лични/чувствителни данни чрез политики и правила за IBAN, ЕГН, ID, Passport, Credit Card Numbers, според описаният сценарий 3. Трансфер на файлове съдържащи лични/чувствителни данни чрез електронна поща (email). Проверка на резултатите.
Тестови операции	Минимум десет опита за трансфер на файлове или текстове, съдържащи лични/чувствителни данни чрез чрез електронна поща (email).

Таблица 11. Изпитания на разширената СИС

Резултати и заключения от изпитанията

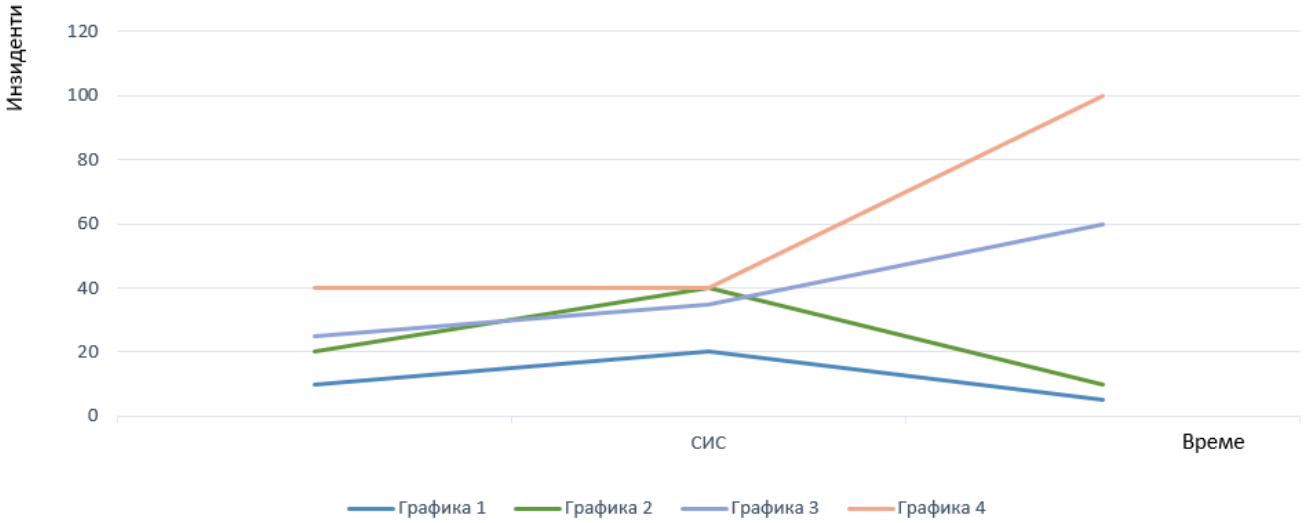
Използвайки предложеният от нас метод за проектиране на СИС, се разширяват възможностите на съществуващите системи за информационна сигурност. Детайлното описание на случаите на употреба за защита на чувствителни за организацията данни чрез проектните модели с помощта на UML диаграми още на етап проектиране осигуряват възможност на СИС точно да изпълнява поставените цели, свързани с политиките за вътрешна сигурност, правните разпоредби 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 (Фигура 12). 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. Дефинираме следните агенти:

- *„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“.*

„Агент по нарушенията“ – изчислява коефициентите на отклонения на отделните компоненти на системата спрямо зададените предварително параметри чрез „Агент на политика за ИС“. По този начин открива нетипични и подозрителни действия и активира „Агент за Защита“, които трябва да неутрализира заплахата.

„Агент за Защита“ – След откриване на отклонение, се инициира изпълнението на предварително заложени действия за противодействие на причината за отклонението

(заплахата). При успех заплахата е неутрализирана и се компенсира отклонението от нормалното състояние. Важна функция на тези агенти е самозащитата, която се гарантира нормалното функциониране на системата. Функциите на първите два вида агенти може да се обединят в един защитен агент.

„Агент на политика за ИС“ –грижи се за изпълнението на политиката за сигурност на системата и постигане на зададените цели. Агентът подава команди към някои от останалите агенти – например „Агент за защита“ или „Рапортуващ агент*“*, осигуряващи тяхното осъществява. Този агент задава стойности на параметрите, осигуряващи нормалната работа на системата към „Агент по нарушенията“, следящ за евентуални отклонения от тях.

„Агент за наблюдение“ – следи за информационния поток в СИС и подава информация към „Аналитичен агент“ и „Агент по нарушенията“. Целта е да се открият евентуални отклонения, индикиращи за нарушение на политиката за сигурност.

„Рапортуващ агент“ – докладва на останалите агенти информацията, подадена му от „Агента за наблюдение“.

„Комуникационен Агент“ - осъществява комуникацията между останалите агенти, като гарантира Поверителността и Цялостността на съобщенията.

„Обработващ агент“ – посредничи между останалите агенти, обработва подадената му информация от други агенти и връща резултатите към тях.

„Складиращ агент“ – основната роля на този агент е да съхранява информация, подпомагайки останалите агенти. Такава може да бъде например базова информация като политиката за сигурност, междинна информация, получена като резултат от работата на останалите агенти, доклади и други.

„Агент за реализация на услуги“ – предлага набор от услуги към останалите агенти, реализиращи изпълнението на вътрешни за системата задачи. Такава задача може да бъде например следене за нормалната работа на останалите агенти, осигурявайки Целостта на системата.

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 35).
На тази база приемаме, че класът "Контрол" се трансформира в клас “Агент“, които представя съвкупност от агенти, всеки от които има определена цел. В съответствие с отделните цели и нуждата от определени роли, класът „Агент“ обхваща:

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

„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).

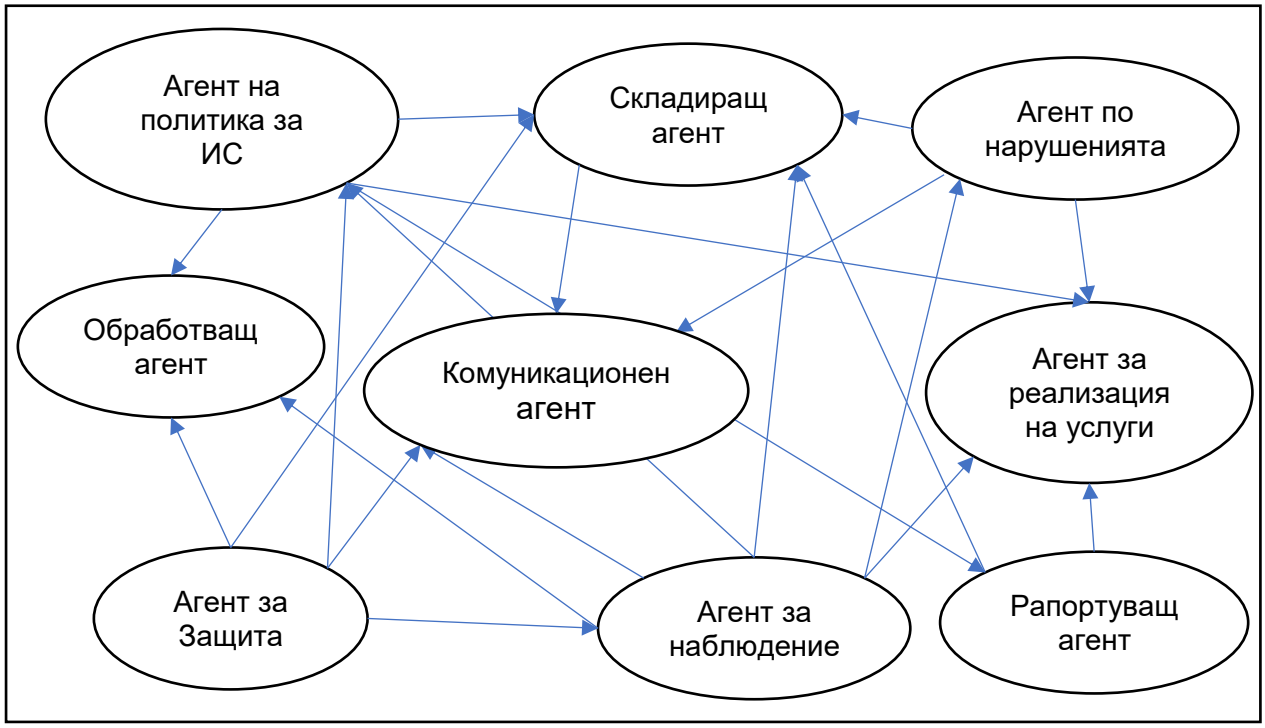
За да се опише ролята на всеки агент чрез използване на ОО език UML се използва– диаграма „случай на използване“, която описва взаимодействието на даден агент с околната среда, която в нашия случай се разглежда като ОО система.

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.

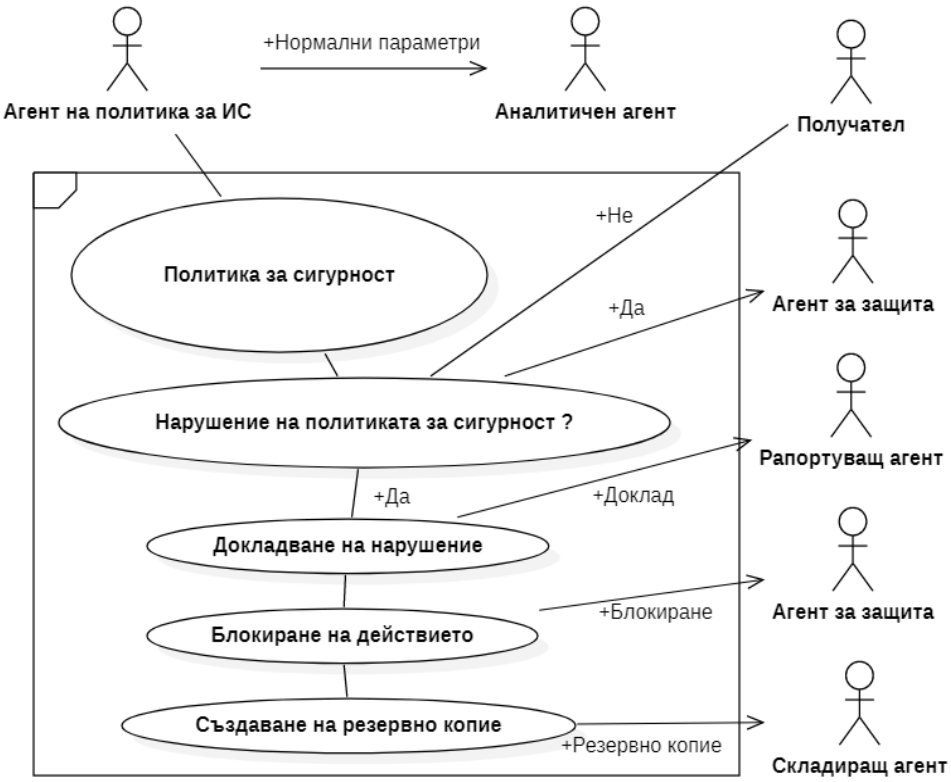
На Фигура 37 е показана диаграма на случай на използване за „Агент на политика за ИС“. Сценарият показан от диаграмата е следния: „Агента на политика за ИС“ следи спазването на политиката за сигурност. При нарушение се активира „Агента за защита“ и според предвидените действия в политиката за сигурност активира следните агенти: „Рапортуващ агент“, за изготвяне на доклад за нарушението, „Агент за защита“ за блокиране на действието, „Складиращ агент“ за съхранение на доклада и копие от документа нарушил политиката за сигурност за по-нататъшно разследване. Агента периодично подава параметрите индикиращи нормалната работа на системата към „Агента по нарушенията“, служещи за откриване на отклонение и съответно идентифициране на нарушение.

На Фигура 38 е показана диаграма на случай на използване за „Агент за Защита“. Агента се активира от „Агента по нарушенията“ при откриване на отклонение от нормалните параметри в системата, съответно нарушение. Агента инициира

изпълнението на предварително заложените действия за противодействие на нарушението или заплахата.

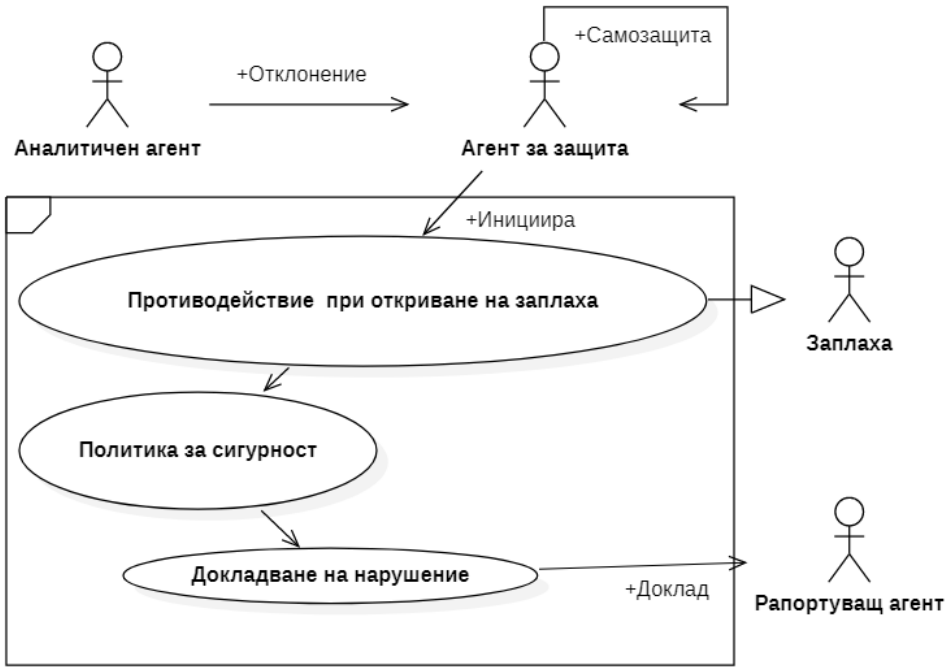


Фигура 37. Взаимоотношения на отделните представители на на клас „Агент“



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

Според приетата политика за сигурност се изготвя доклад и се активира рапортуващ агент за неговото изготвяне. От своя страна той използва Складиращия агент за запазването на доклада и документа за по-късно. Важна функция на Агента за защита е способността му за самозащита, запазвайки Целостта на системата.



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

Показаните диаграми и сценарии илюстрират само базовите действия за яснота. В практиката действията, изпълнявани от агентите са по-сложни и се активират повече агенти.

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

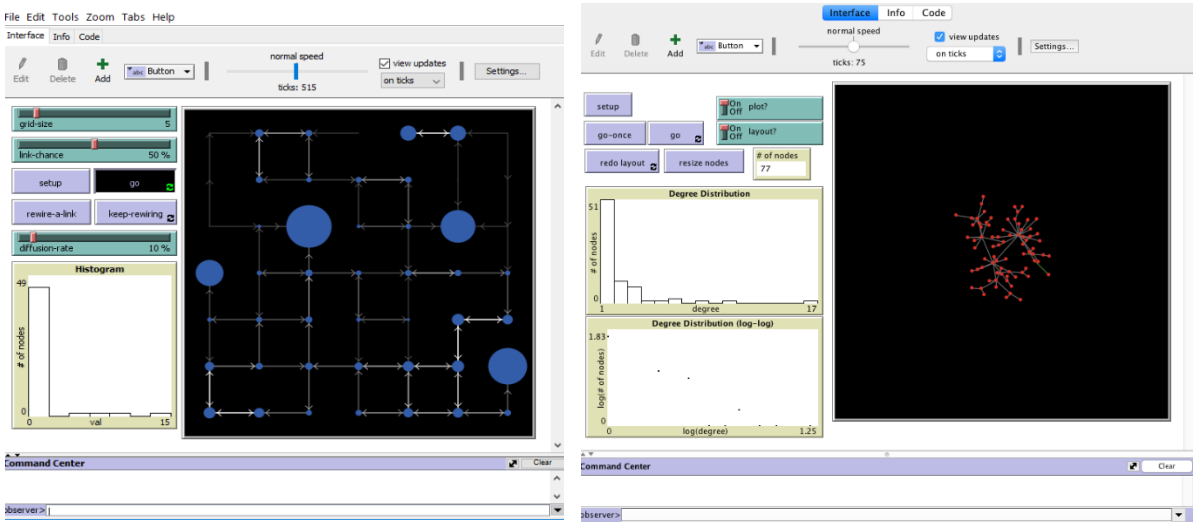
Реализацията на симулацията на архитектурния модел на СИС извършваме на базата на агентно- и мулти-агентно ориентирано моделиране в средите NetLogo и I-SCIP-SA, позволяващи смесена (експертна, сензорна и машинна) оценка на предложените архитектурни мета идеи [102].

Експерименти в средата NetLogo

NetLogo (Фигура 39) е мулти-агентна крос-платформена симулационна среда за симулиране на сложни системи във времето [47, 118]. Тя е предназначена за образователни цели и научни изследвания и се използва в широк кръг от дисциплини. Средата NetLogo е основана на агентно-базирани модели за симулиране на действията и взаимодействията на множество автономни агенти (индивидуални или колективни субекти като организации или групи), работещи едновременно. Това дава възможност да се изследват връзките между модели на микро ниво, които възникват от при тяхното взаимодействие и оценка на въздействието им върху системата, като цяло. На базата на мета-модела от 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. Като се отчита факта, че за момента средата NetLogo, по същество, е затворена и не е предвидено динамичното използване на външни източници на данни (сензорни, експертни и др.), получените модели имат основно изследователско значение за проучване на организационната страна на архитектурите на СИС по отношение на агентно-базираното и представяне.



Фигура 40. Екранни снимки от симулация в среда на NetLogo

Експерименти в средата I-SCIP-SA

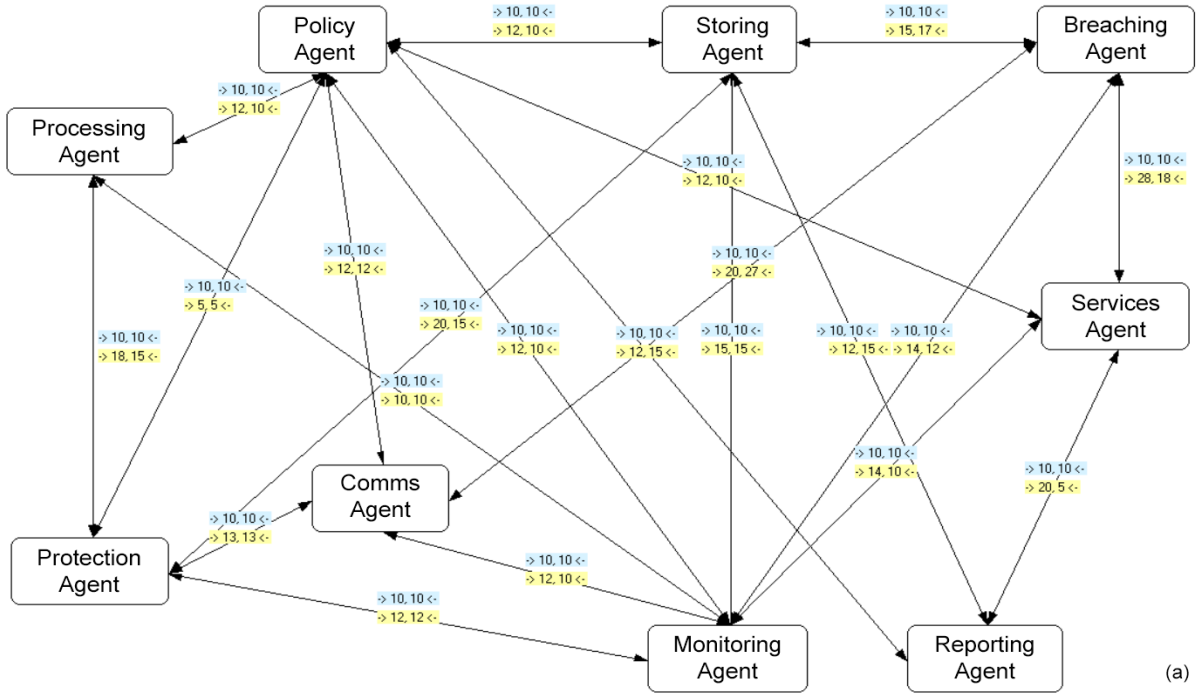
С цел по-голяма близост до реалността, позволяваща смесено изследване на предложените архитектурни решения на СИС е разработен мулти-агентен модел [28] от тип „система-от-системи“ [126] в средата I-SCIP-SA (Intelligent Scenario Computer Interface Program for System Analysis) [105]. При това е приложен 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.

Множеството на източниците на данни може да използва: сензори, API функции за директна връзка или използващи записи във файлове с различен произход (вкл.



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

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]).

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.

На Фигура 40 е представеният модел на Системи за предотвратяване изтичане на данни СПИД , известна и като DLP . СПИД за проактивно изследване на изтичанията на данни съдържа девет агента с различни роли: “Processing Agent” –

Фигура 42. Мулти-агентен модел на СПИД с допълнителни класификационни начални оценки на агентите в 3D ДЧ

„Обработващ агент“, “Policy Agent” – „Агент на политика за ИС“, “Storing Agent” – „Складиращ агент“, “Breaching Agent” – „Агент по нарушенията“, “Services Agent” – „Агент за реализация на услуги“, “Protection Agent” – „Агент за Защита“, “Comms Agent” – „Комуникационен Агент“, “Monitoring Agent” – „Агент за наблюдение“, “Reporting Agent” – „Рапортуващ агент“.

Между тях са идентифицирани двадесет и една комуникационни връзки описващи различни сценарии за изтичане на данни в корпоративна среда. Моделът е базиран на идеите от [104], както и някои емпирични данни от [102, 114], водещи до множество, начални критични агентни класификации, които са успешно решени в десет стъпки (Фигура 41), отдавайки лидерска роля на „Агент по нарушенията“ [107].

Допусканията в модела, дават следната стартова класификация на агентите в 3D ДЧ: Буферни – Buffering, $z < 0$: „Рапортуващ агент“ – “Reporting Agent” – 2, $z \geq 0$: „Обработващ агент“ – “Processing Agent” – 8; Критични – Critical, $z \geq 0$: „Агент на политика за ИС“ – “Policy Agent” – 1, „Агент по нарушенията“ – “Breaching Agent” – 4, „Агент за реализация на услуги“ – “Services Agent” – 7, „Агент за Защита“ – “Protection Agent” – 9, $z < 0$: „Комуникационен Агент“ – “Comms Agent” – 3, „Складиращ агент“ – “Storing Agent” – 5, „Агент за наблюдение“ – “Monitoring Agent” – 6.

На базата на някои промени в ролята и теглата на „Агент по изтичанията“ – “Breaching Agent”, е предложена финална класификация на агентите в 3D ДЧ: Буферни – Buffering, z < 0: „Рапортуващ агент“ – “Reporting Agent” – 2, z ≥ 0: „Обработващ агент“ – “Processing Agent” – 8; Пасивни – Passive, z < 0: „Агент по изтичанията“ – “Breaching

Фигура 43. Мулти-агентен модел на СПИД с допълнителни класификационни финални оценки на агентите в 3D ДЧ

Agent” – 4; Активни – Active, z ≥ 0: „Комуникационен Агент“ – “Comms Agent” – 3, „Агент по услугите“ – “Services Agent” – 7; Критични – Critical, z ≥ 0: „Агент на политика за ИС“ – “Policy Agent” – 1, „Агент по защитата“ – “Protection Agent” – 9; z < 0: „Складиращ агент“ – “Storing Agent” – 5, „Агент за наблюдение“ – “Monitoring Agent” – 6 (Фигура 42).
На базата на някои промени в ролята и теглата на „Агент по изтичанията“ – “Breaching Agent”, е предложена финална класификация на агентите в 3D ДЧ: Буферни – Buffering, z < 0: „Рапортуващ агент“ – “Reporting Agent” – 2, z ≥ 0: „Обработващ агент“ – “Processing Agent” – 8; Пасивни – Passive, z < 0: „Агент по изтичанията“ – “Breaching Agent” – 4; Активни – Active, z ≥ 0: „Комуникационен Агент“ – “Comms Agent” – 3, „Агент по услугите“ – “Services Agent” – 7; Критични – Critical, z ≥ 0: „Агент на политика за ИС“ – “Policy Agent” – 1, „Агент по защитата“ – “Protection Agent” – 9; z < 0: „Складиращ агент“ – “Storing Agent” – 5, „Агент за наблюдение“ – “Monitoring Agent” – 6.

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.

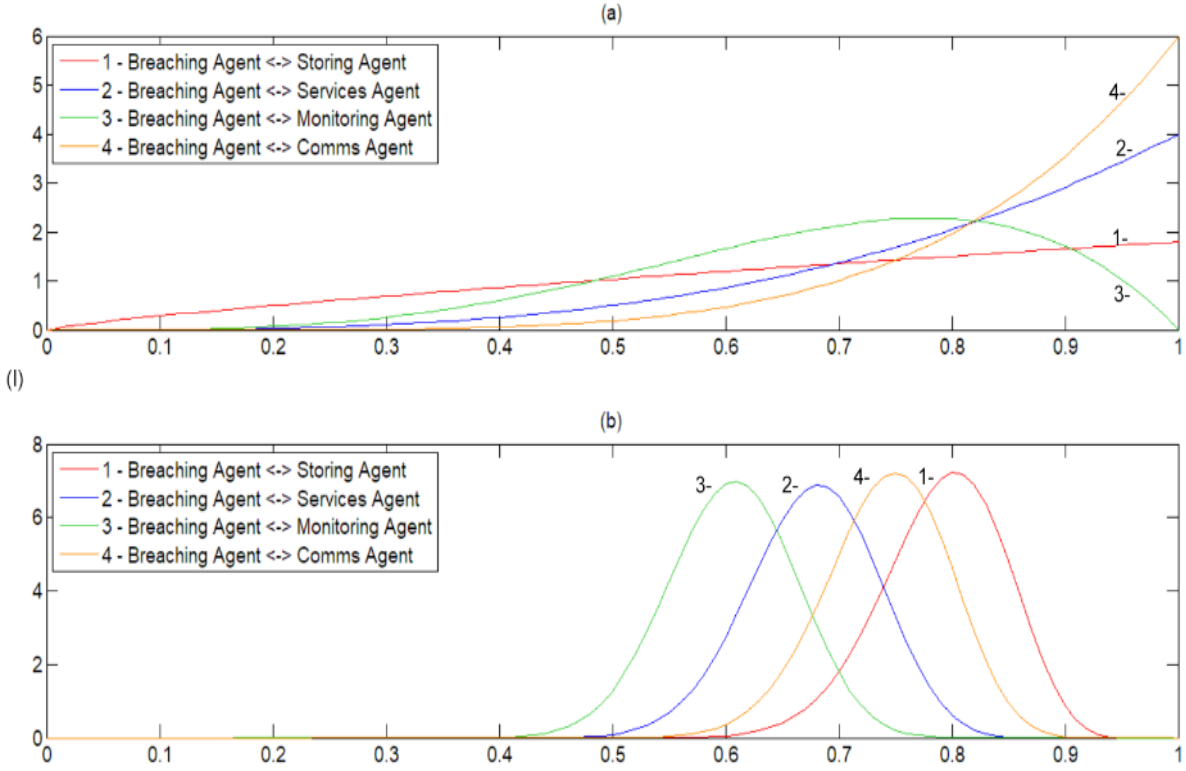
Стохастична валидация

Представено е про-активно стохастично решение за смесена валидация върху предложения системен модел (Фигури 41 и 42). То е основано на идеите от [110], но използва различен контекст и процедура за пресмятане на вероятностните стойности. Предвид факта, че реалните корпоративни системи за информационна сигурност са нелинейни и нестационарни, тяхното поведение е трудно предсказуемо в определени ситуации. По същество, се дефинира бета вероятностно разпределение за всяка от използваните връзки между агентите в модела. Формата на разпределенията се определя експертно, в съответствие с техните очаквания за бъдещите тенденции. Идеята тук е заимствана от добре познатите разглеждания на социалната динамика, предложени от Форестър [115], които в последствие са усъвършенствани в работата на Медоус и к-в [116]. В настоящото решение са използвани и някои модификации на параметрите „алфа“ и „бета“ на фамилиите от вероятностни криви, подобно на [110]. По-нататък, се извършва апостериорно машинно преоценяване за бъдещето на тенденциите във вероятностните разпределения, приложени върху връзките между агентите в модела. Новите стойности се изчисляват с използване на Бейсов подход по отношение на избрано сценарийно множество за еволюционно развитие. Основната идея е следната: Z (X, Y); Zj (Xj, Yj, Ti, Sk) = P (Xj|Dl|Lm|An|Ti|Sk) x P (Yj|Dl|Lm|An|Ti|Sk), където: P (…) – Бейсова вероятност, Xj – влияние, Yj – зависимост, Zj – чувствителност на j-я агент в модела, Dl – l-то състояние на данните, l = {Use, Motion, Rest}, Lm – m-то от множеството на изтичанията на данни (вж. напр. [114]), An – индекса на потърсения n-и агент, Ti – продължителността на i-я времеви период за динамично изследване на модела, Sk – избрания k-и еволюционен сценарий от множеството на експерименталните сценарии (вж. напр. [103, 110]).

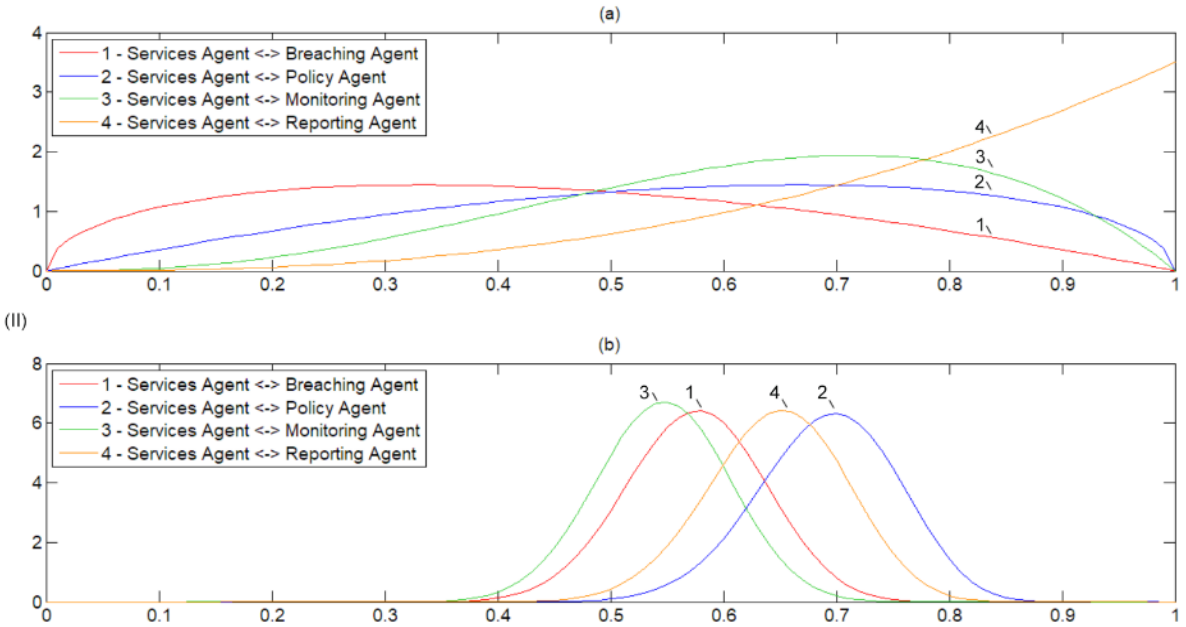
Графично представяне на предложената идея за априорните и апостериорни оценки на вероятностите върху бета разпределения (чрез смесена експертно-машинна валидация в среда на Matlab R2011b) за връзките на: “Агента по нарушенията” и свързаните с него: “Агент за реализация на услугите” и “ Комуникационен Агент” е показано на Фигури 43,44 и 45.

Представените резултати от вероятностната валидация на системния мулти-агентен СПИД модел за изследване на изтичанията на данни в корпоративна среда дават най-високи приоритети ($P < 0.9$) на: “Складиращ агент”, “Рапортуващ агент” и “Агент на политика за ИС”, контрастиращи с по-ниско приоритетните, но значими ($P > 0.4$) агенти: “Агент за наблюдение”,“ Агент за реализация на услуги” и “ Агент за Защита”. Тези факти очертават доста релативистична картина на корпоративната информационна среда за

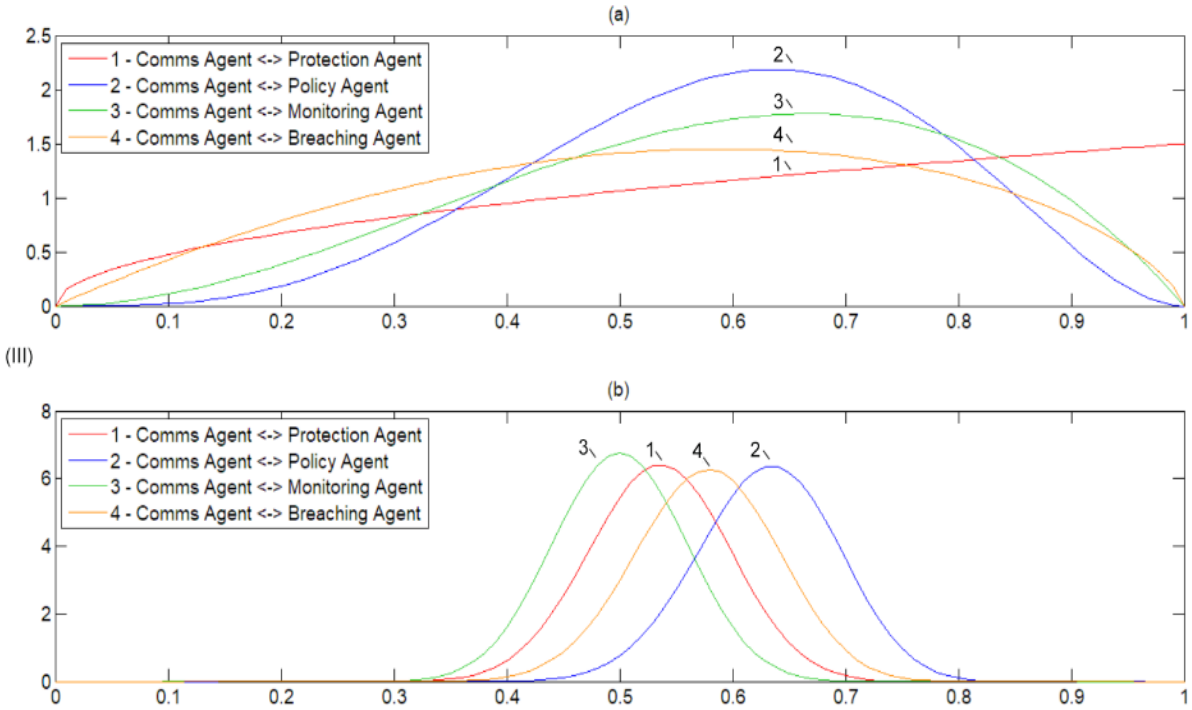
сигурност, предвид факта че има известни припокривания, паралелности и непълноти по отношение използването на “Агент по нарушенията”, “Комуникационен Агент” и “Агент за реализация на услуги” едновременно като референтни и активно оценявани.



Фигура 44. Вероятностна смесена валидация на очакванията за “Агент по нарушенията” по отношение на априорните (a) и апостериорните (b) промени в трендовете за системния модел



Фигура 45. Вероятностна смесена валидация на очакванията за: “Агент за реализация на услуги” по отношение на априорните (a) и апостериорните (b) промени в трендовете за системния модел.



Фигура 46: Вероятностна смесена валидация на очакванията за “Комуникационен Агент” по отношение на априорните (a) и апостериорните (b) промени в трендовете за системния модел.

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

Интерактивна верификация

Верифицирането на резултатите от стохастичните симулации бе проведено емпирично, с използване на интерактивна симулация в трансформирана реалност, организирана в рамките на ученията CYREX 2018, 2019 и 2020 [109, 117, 122, 123]. Използван беше въображаем сценарий, който се играе в продължение на 180 минути от обучаемите в няколко интернационални екипа с участие на над 30 представители от България, Македония и Турция с включени наблюдатели от ИКТ бизнеса, съсловни и експертни организации у нас и в чужбина. Като резултат бе направена експериментална многокритериална оценка на вероятностната динамика на избрани потоци от данни в перспектива, по отношение влиянието на цифровата трансформация в дигиталната ера в контекста на проигравания сценариен скрипт.

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

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

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

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

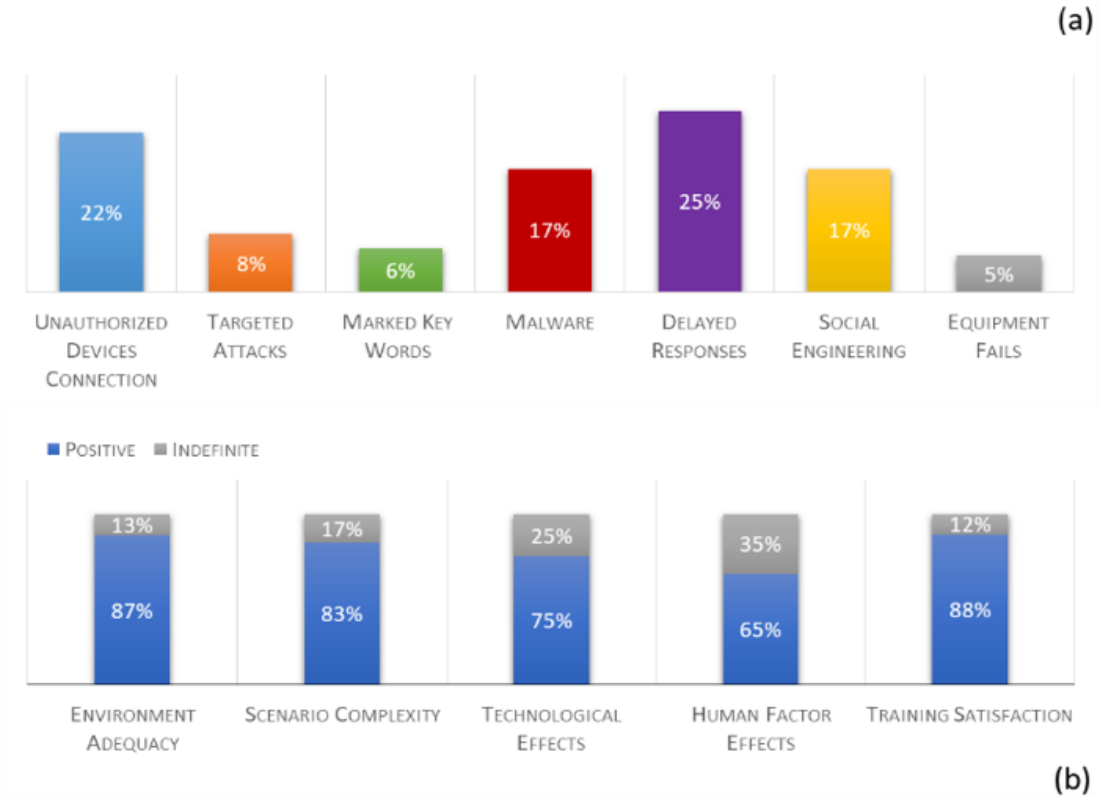
Поведението на играчите беше наблюдавано по отношение динамиката на техните действия по скрипта на сценария, като самата регистрация бе организирана дистанционно, използвайки система за мониторинг и видеозапис, както и платформа СПИД DLP CoSoSys My Endpoint Protector, v. 4.7.4.7. Решението е в състояние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

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

Емпирична по характер, осъществената рамка на CYREX беше количествено оценена (Фигура 46) от участниците (използвайки данни, както за положителните, така и за неопределените стойности на група индикатори, измерени в проценти). На базата на идеите, отбелязани в [103], бяха избрани пет ключови индикатора: “Environment Adequacy” – „Адекватност на средата“, “Scenario Complexity” – „Комплексност на сценария“, “Technological Effects” – „Технологични ефекти“, “Human Factor Effects” – „Ефекти от човешкия фактор“ и “Training Satisfaction” – „Удовлетвореност от обучението“.

Освен това, бяха използвани и обобщените, нормализирани данни, регистрирани от СПИД за изтичане на информация, чрез мониторинг на седем възможни атакуващи вектора: “Unauthorized Devices Connection” – „Неоторизирано свързване на устройства“, “Targeted Attacks” – „Насочени атаки“, “Marked Key Words” – „Маркирани

Фигура 47. Моменти и архитектура на CYREX.



Фигура 48. Резултати от СПИД мониторинга за векторите на атака (а) и обобщена оценка от участниците (б) за CYREX.

ключови думи“, “Malware” – „Атаки чрез зловреден софтуер“, “Delayed Responses” – „Забавени отговори“, “Social Engineering” – „Социален инженеринг“ и “Equipment Fails” – „Отказ на оборудването“.

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

4.7 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 представени 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.

Тези приноси на дисертационния труд са представени и публикувани в следните авторски публикации :

[1] 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

[2] 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,

[3] 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

Заключение

Резюме на получените резултати

В дисертационния труд е изследван нов метод и модели за разработване на системи за информационна сигурност, осигуряващи защита на чувствителна информация в различни по характер организации. Защитата е насочена срещу вътрешни заплахи в посока отвътре-навън, в резултат от действие на вътрешни лица с легитимен достъп до ресурсите на организацията. Разработеният метод е приложим за създаване на СИС, реализираща подход за защита на данни. Той е подходящ за приложение в различни по големина организации, предприятия и обекти от критичната инфраструктура, боравещи с чувствителна информация или индустриални тайни.

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 и Обработка на информацията. 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 създаване на нова квалификация на подходите за управление на информационната сигурност, както и до въвеждането на нови понятия и нов аспект за оценка на информацията – чувствителност.

За определянето на архитектурата на системата се използва 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, описан с помощта на обектно-ориентиран език за описание на модели UML. Представено е как могат да се моделират отделни аспекти на архитектурния модел, основани на съответните концептуални модели чрез използване на UML диаграми. 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.

На базата на проектен обектно-ориентиран модел се изгражда 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, се уточняват изискванията към архитектурата на разработваната СИС. Следва анализ на съществуващи платформи за реализация СПИД и избор на най-подходящата в съответствие с модела на анализа.

Моделът на реализация описва съществуваща платформа за създаване на система за информационна сигурност 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“.

Предложеният от нас 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. Представен е пример с конкретни сценарии на нови случаи на употреба (use cases), както и резултати от проведени изпитания на реазлизирано разширение на СИС.

Показано е изграждането на агентно-базиран модел на реализация. Целта е да се създаде симулационен модел на разработваната СИС, който може да се реализира в мулти-агентна крос-платформена симулационна среда за симулиране на сложни системи във времето NetLogo. Представен е подход за трансформиране от обектно-ориентиран модел в агентно-базиран модел. Осъществено е представянето на дейността на агентите и са реализирани интеракциите между тях. Получените модели имат основно изследователско значение за проучване на организационната страна на архитектурите на СИС по отношение на агентно-базираното и представяне.

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

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.

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

Цитирания

1. Gaidarski, I., Minchev, Z., Andreev, R.: Model driven architectural design of information security system. In: Madureira A., Abraham A., Gandhi N., Silva C., Antunes M. (eds) Proc. of Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018). Advances in Intelligent Systems and Computing, vol. 942, pp. 349-359, (2020), https://doi.org/10.1007/978-3-030-17065-3_35.

Цитира се в:

1.1. Tsochev G., Developing Monte Carlo Simulator of Reinforcement Learning Type, Laboratory of Telematics – BAS, Sofia, Bulgaria, PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS • 2020 • Vol. 73, pp. 39-46, p-ISSN: 2738-7356; e-ISSN: 2738-7364, doi: 10.7546/PECR.73.20.04, международно издание
https://www.iict.bas.bg/pecr/2020/73/4-PECR-39-46.pdf

1.2. Boneva Ani, Ivanova Veronika and Boneva Yordanka, An Approach to Create and Use Test (ECHO) Servers Based on Tcl/Tk, Georgian Electronic Scientific Journal (GESJ): Computer Sciences and Telecommunications, ISSN 1512-1232, Reviewed Electronic Scientific Journal, Publisher:Georgian Technical University and Muskhelishvili Institute of Computational Mathematics, ID: 3431, 2021,No.2(60), pp. 35-42
https://elibrary.ru/title_about_new.asp?id=3199

2. 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

Цитира се в:

2.1. Dimitrov W., Syarova S., Analysis of the Functionalities of a Shared ICS Security Operations Center, 2019 Big Data, Knowledge and Control Systems Engineering (BdKCSE), 27 February 2020, Sofia, Bulgaria, INSPEC Accession Number: 19411502, DOI: 10.1109/BdKCSE48644.2019.9010607, индексирано в Scopus и WoS
https://ieeexplore.ieee.org/abstract/document/9010607/

2.2. Dimitrov, W., Jekov, B., Kovatcheva, E., Ostrovska, T. A High-Efficient Low Budgetary Approach to Cyber-Security Exercises, In Proc. of 12th International Conference on Education and New Learning Technologies, July 6-7, 2020, pp. 3051-3059, ISBN: 978-84-09-17979-4, ISSN: 2340-1117, DOI: 10.21125/edulearn.2020.0901, индексирано в WoS
https://library.iated.org/view/DIMITROV2020AHI

Участия 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

Декларация за оригиналност на резултатите

Декларирам, че представената дисертация съдържа оригинални резултати, получени при проведени от мен научни изследвания. Резултатите, които са получени, описани и/или публикувани от други учени, са надлежно и подробно цитирани в библиографията.

Настоящата дисертация не е прилагана за придобиване на научна степен в друго висше училище, университет или научен институт.

Подпис: .....

/инж. Иван Гайдарски/

Благодарности

Бих искал да изкажа искрената си благодарност на своя научен ръководител доц. д-р Румен Андреев, за ползотворната съвместна работа, за напътствията, съветите и градивната критика.

Изказвам и благодарности към доц. д-р Златогор Минчев за оказаната помощ при симулациите и анализа на получените данни.

Горещи благодарности на моето семейство, родители, колеги и приятели, които ме подкрепяха и мотивираха през цялото време.

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

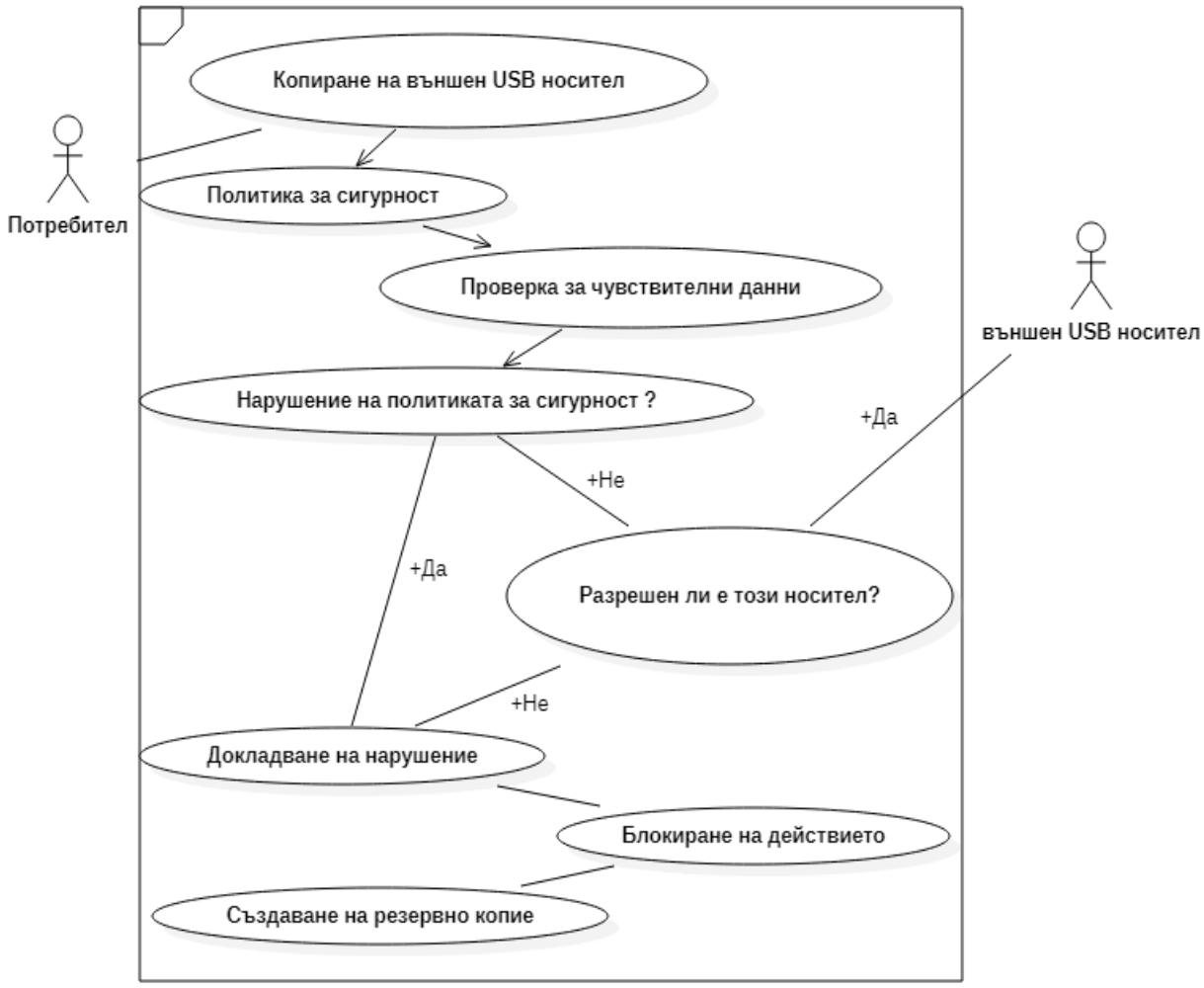
91. Горанов П., Тодорова Е., Георгиева Д., Концептуален модел на обектно-ориентирана библиотека от механични компоненти, Българско списание за инженерно проектиране, брой 35, януари 2018г, ISSN 1313-7530
92. Митрев Р., Компютърно моделиране и симулация, Пропелер, София, 2016г
93. A. Solvberg, Data and 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

ПРИЛОЖЕНИЕ 1. UML проектни модели, описващи случаи на защита на чувствителни данни в организация

1.1 Сценарий 1 - Диаграма на случай на използване (Use Case Diagram)

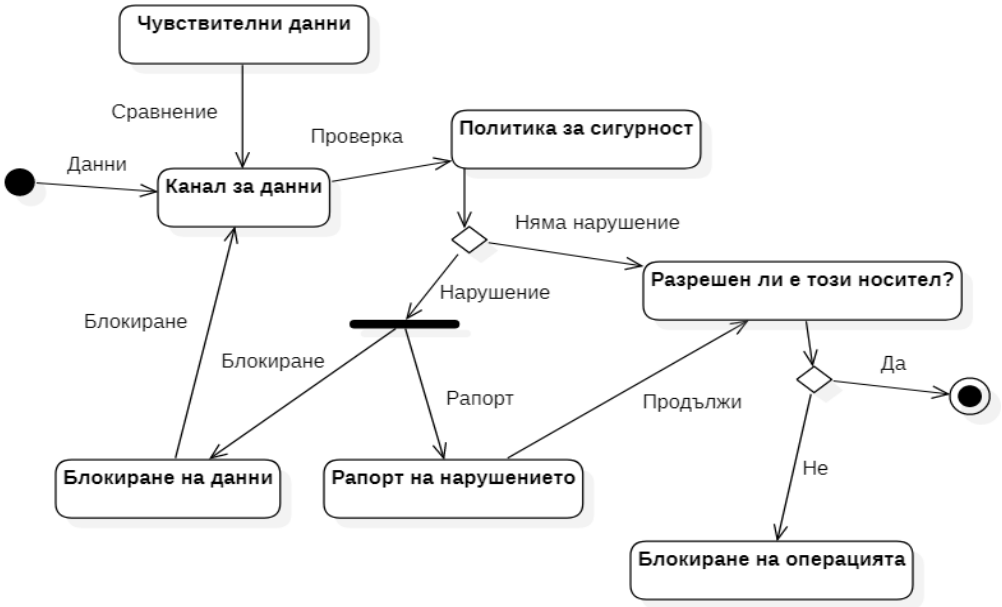


Фигура 1.1 Диаграма на случай на използване на Сценарий 1

Чрез диаграмите на случаи на използване са описани сценариите на взаимодействие на СИС с външни за нея субекти като копиране на файлове върху външен USB носител, изпращане на електронна поща до външен за организацията получатели или други.

Чрез показаната на Фиг.1.1 диаграма на използване се описва сценарий 1 от Таблица 10 за контрол на трансфера на лични/чувствителни данни, съдържащи IBAN, ID, Credit Card Numbers чрез външни запаметяващи устройства (USB флаш памети).

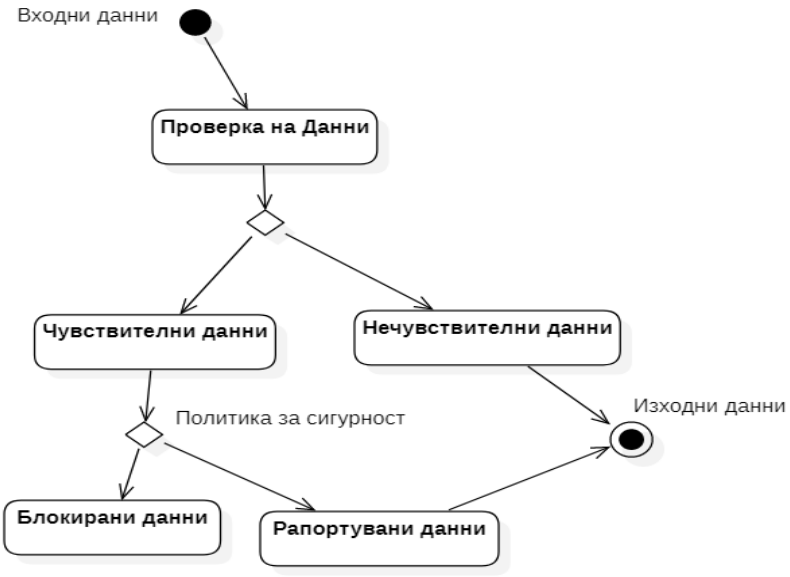
1.2 Сценарий 1 – Диаграма на активност



Фигура 1.2 Диаграма на активност на Сценарий 1

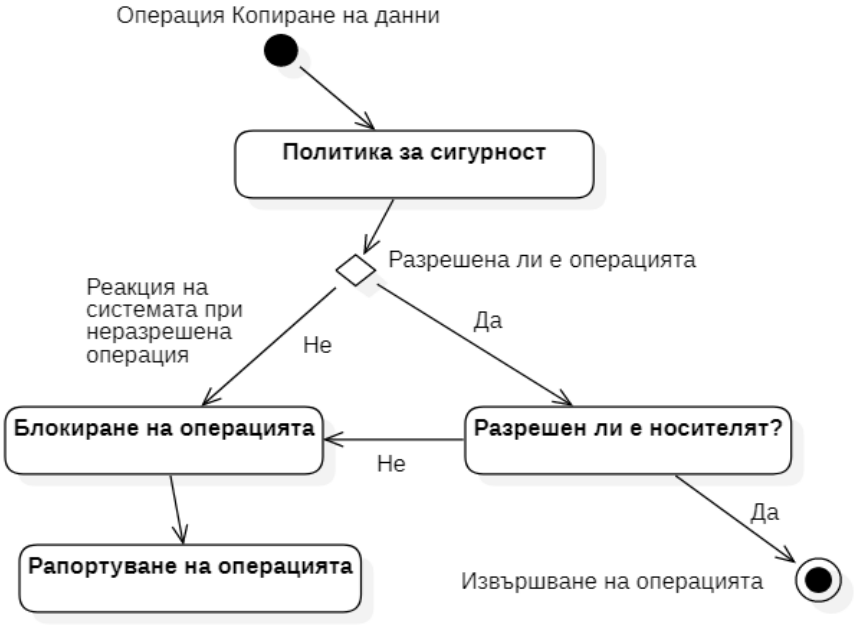
Чрез диаграмата на активност от Фиг.1.2 се описва динамичното поведение на системата, представено със сценарии 1 (Таблица 10). Каналите за данни се проверяват за чувствителна информация чрез сравняване на данните с критериите за чувствителни данни, заложени в приетата политика за сигурност. При съвпадение се констатира нарушение (изтичане на данни) и се инициират предвидените в политиката за сигурност действия - блокиране и/или документиране на нарушението. При липса на нарушение се проверява дали използваният носител е разрешен за даден потребител. Ако носителят е в разрешеният списък операцията копиране се изпълнява, ако не е операцията се блокира.

1.3 Сценарий 1 - Диаграми на състояние



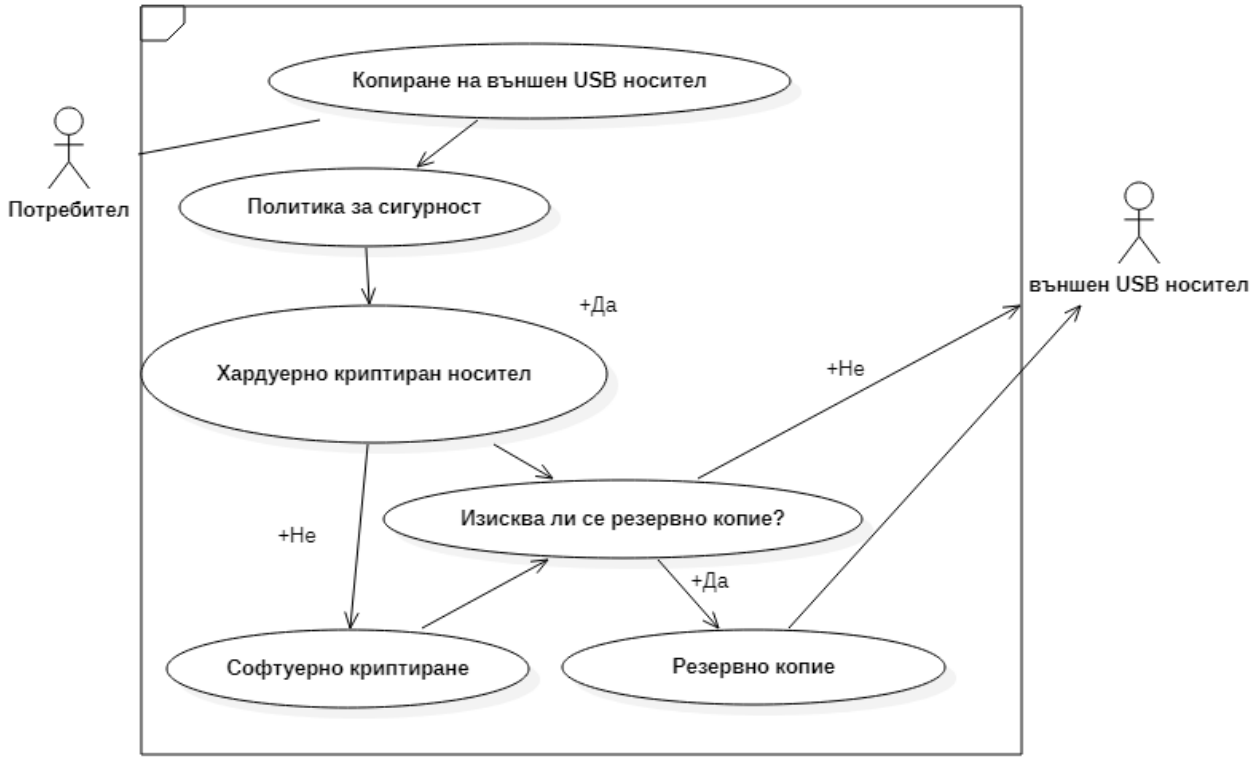
Фигура 1.3.1 Диаграма на състояние на данни по Сценарий 1

Чрез диаграмите на състояние се описва динамиката в промяната на състоянието на основните елементи на СИС. Фигура 1.3.1 представя промяната на състоянието на данните по Сценарий 1 от Таблица10, а Фигура 1.3.2 – промяната на състоянието на операциите.



Фигура 1.3.2 Диаграма на състояние на операции по Сценарий 1

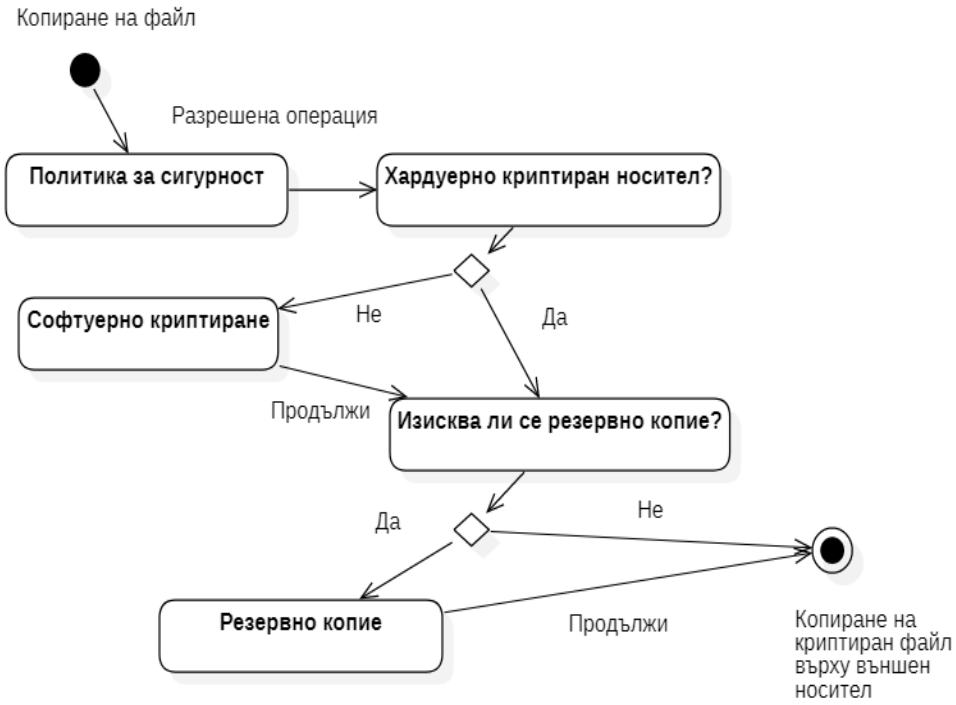
2.1 Сценарий 2 - Диаграма на случай на използване (Use Case Diagram)



Фигура 2.1 Диаграма на случай на използване на Сценарий 2

Диаграмата на случаи на използване от Фиг.2.1 описва сценарий 2 Таблица 10 за контрол на трансфера на лични/чувствителни данни, съдържащи IBAN, ID, Credit Card Numbers чрез външни запаметяващи устройства (USB флаш памети), чрез принудително криптиране на данните.

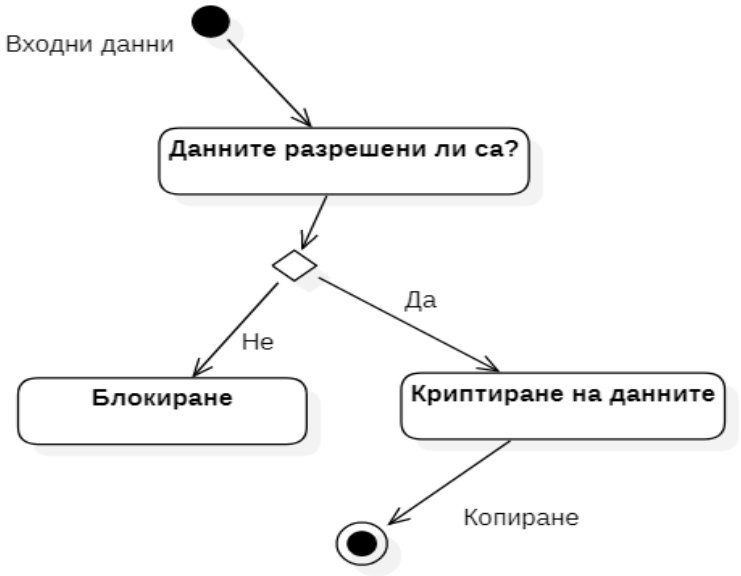
2.2 Сценарий 2 - Диаграма на активност



Фигура 2.2 Диаграма на активност от Сценарий 2

Чрез диаграмата на активност от Фиг.2.2 се описва динамичното поведение на системата, представено със сценарий 2 (Таблица 10).

2.3 Сценарий 2 - Диаграма на състояние



Фигура 2.3 Диаграма на състояние на данни от Сценарий 2

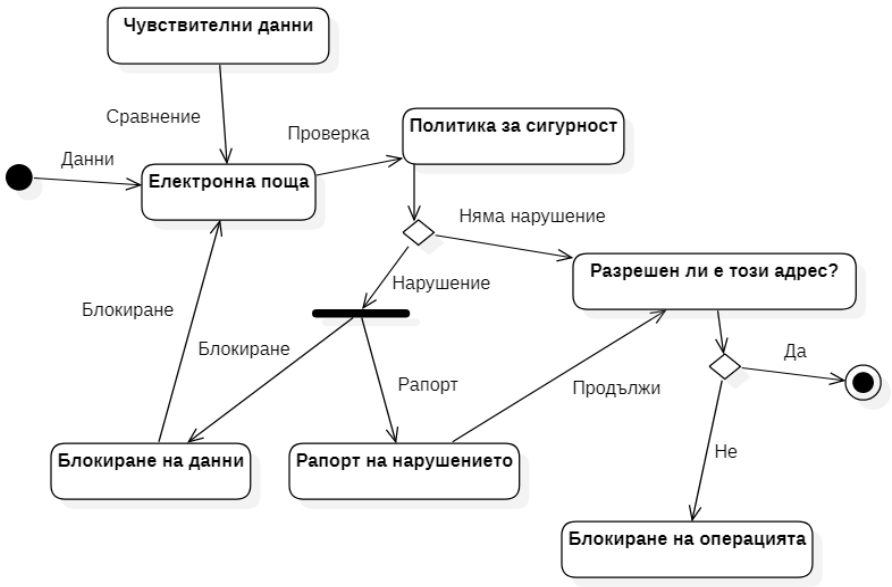
Чрез диаграмата на състояние от Фиг. 2.3 се описва динамиката в промяната на състоянието на данните по Сценарий 2 от Таблица10, при тяхното принудително криптиране при копиране на външни USB носители.

3.1 Сценарий 3 - Диаграма на случай на използване (Use Case Diagram)

Фигура 3.1 Диаграма на случай на използване на Сценарий 3

Чрез диаграмата на случаи на използване от Фиг.3.1 се описва сценарий 3 от Таблица 10 за контрол на трансфера на лични/чувствителни данни, съдържащи IBAN, ID, Credit Card Numbers чрез външни запаметяващи устройства (USB флаш памети), чрез електронна поща (email).

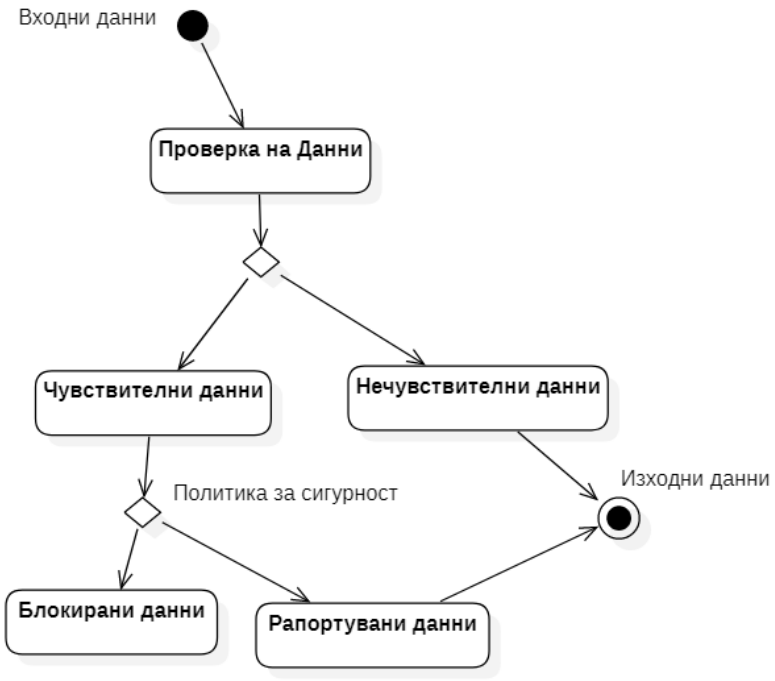
3.2 Сценарий 3 - Диаграма на активност



Фигура 3.2 Диаграма на активност от Сценарий 3

Диаграмата на активност от Фиг. 3.2 описва динамичното поведение на системата, представено със сценарий 3 от Таблица 10 при изпращане на данни чрез електронна поща.

3.3 Сценарий 3 - Диаграма на състояние



Фигура 3.3. Диаграма на състояние от Сценарий 3

Чрез диаграмата на състояние от Фиг. 3.3 се описва динамиката в промяната на състоянието на данните по Сценарий 2 от Таблица10, при трансфер данни чрез електронна поща (email).

ПРИЛОЖЕНИЕ 2. Технически описания

1. Техническо описание на платформа СПИД „Cososys Endpoint Protector 5.0.2.1“.

Обхват и архитектура

СПИД платформата за реализация EndPoint Protector 5.0.2.1 [96], на компанията CoSoSys Ltd. е решение за защита от изтичане на чувствителна за организацията информация от клас Data Leak Prevention (DLP).
Endpoint Protector 5.0.2.1 обхваща крайните точки (работни станции и лаптопи) и осигурява мониторинг, контрол и управление на всички крайни устройства (компютри, лаптопи, таблети и смартфони) през чиито информационни канали е възможно изтичането на чувствителна информация - принтери, запаметяващи устройства, преносими памети, TCP/IP и Wi-Fi мрежи, електронна поща, социални мрежи, облачни услуги и други (Фигура 30).

СПИД Endpoint Protector 5.0.2.1 е базиран на клиент-сървър архитектура. Върху контролираните крайни точки се инсталират агенти, които осъществяват контрол, мониторинг и управление на периферните устройства и информационните канали на конкретната крайна точка. Агентите комуникират чрез криптирана свръзка с централния сървър и налагат съответната политика за сигурност, подадена от сървъра върху конкретната крайна точка. Софтуерът дава възможност за работа на клиентските компютри без достъп до интернет („off-line“) и синхронизиране на данните от сървъра при работа “on-line“.

Модулна структура на Endpoint Protector 5

Endpoint Protector 5.0.2.1 се състои от отделни модули – “Device Control – Управление на устройства“, „Content Aware Protection – Инспекция по съдържание“, „eDiscovery – Сканиране на Данни в покой“. Модулната структура позволява инсталирането на отделни пакети за управление на различните по вид услуги и продукти, както и бъдещо разширяване на системата.

Модул „Device Control – Управление на устройства“

Модулът „Device Control - Управление на устройства“ е базовият модул на системата. Извършва централизиран мониторинг, контрол и управление на всички информационни шини и портове на крайните точки – работни станции и лаптопи, откъдето е възможно неоторизирано изтичане на информация, както и на всички крайни устройства, свързани към тях - принтери, запаметяващи устройства, преносими памети, Wi-Fi, Bluetooth устройства и други.

Функционалност на модула:

- Показване в реално време списък на всички контролирани потребители;
- Показване в реално време списък на всички устройства, свързани към съответните крайни точки – работни станции и лаптопи;
- Показване история на операциите, извършени върху дадено устройство;
- Задаване на различни права на достъп на външните устройства: Позволен достъп (Allow Access), Отказан достъп (Deny Access) или Достъп само за четене (Read Only) – Таблица 9;
- Позволява създаване на база данни с оторизирани (разрешени) за даден потребител устройства. При свързване на неоторизирано (непозволено)

устройство то може да бъде блокирано от системата, за предотвратяване на евентуално изтичане на чувствителна за организацията информация;

- Дава възможност на системния администратор при свързване на непознато външно устройство да извършва неговото оторизиране. Тази възможност е предвидена и в „off-line“ режим, чрез оторизираща парола, подадена от системния администратор.
- Чрез функцията „Проследяване на файл“ (File Tracing) СПИД Endpoint Protector има възможност за проследяване на действията, извършени върху даден файл, трансфериран към преносимите устройства, като: копиране на файл, преименуване, изтриване, достъп, достъп и редактиране.
- Възможност да се дефинира списък с разрешени файлове – File Whitelisting, които да бъдат трансферирани към оторизирани (разрешени) устройства. Всеки опит за трансфер на файлове, извън този списък ще бъде блокиран и администратора ще бъде уведомен за непозволеното действие.
- Чрез функцията „Създаване на резервно копие“ (File Shadowing), СПИД има възможност за запазване на копия на всички файлове, записвани на външни устройства за бъдещ преглед и по-детайлен анализ.

Устройства	Права
USB запаметяващи устройства	Позволен достъп / Отказан достъп / Достъп само за четене
Шина тип FireWire	Позволен достъп / Отказан достъп / Достъп само за четене
Оптично записващо устройство	Позволен достъп / Отказан достъп / Достъп само за четене
Дигитална камера	Позволен достъп / Отказан достъп
Смартфон – синхронизиране с USB	Позволен достъп / Отказан достъп
Вътрешен четец за смарткарти	Позволен достъп / Отказан достъп / Достъп само за четене
PCMCIA устройства	Позволен достъп / Отказан достъп / Достъп само за четене
ZIP устройство	Позволен достъп / Отказан достъп / Достъп само за четене
Флопидисково устройство	Позволен достъп / Отказан достъп / Достъп само за четене
Четец за карти (MTD)	Позволен достъп / Отказан достъп / Достъп само за четене
Четец за карти (SCSI)	Позволен достъп / Отказан достъп / Достъп само за четене
Портативни устройства под Windows	Позволен достъп / Отказан достъп
Мобилни телефони	Позволен достъп / Отказан достъп
Локални принтери	Позволен достъп / Отказан достъп
Блутут устройства	Позволен достъп / Отказан достъп
Безжична мрежа	Позволен достъп / Отказан достъп / Достъп само за четене
Смартфони BlackBerry	Позволен достъп / Отказан достъп
Уебкамера	Позволен достъп / Отказан достъп

Смартфони iPhone	Позволен достъп / Отказан достъп
Таблети iPad	Позволен достъп / Отказан достъп
Музикални плеъри iPod	Позволен достъп / Отказан достъп
Контролер Serial ATA	Позволен достъп / Отказан достъп
Сериен порт	Позволен достъп / Отказан достъп
Разширителна карта Teensy	Позволен достъп / Отказан достъп
Порт тип Thunderbolt	Позволен достъп / Отказан достъп / Достъп само за четене
Споделено мрежово дисково пространство	Позволен достъп / Отказан достъп
Инфрачервен порт	Позволен достъп / Отказан достъп
Паралелен порт (LPT)	Позволен достъп / Отказан достъп
Външна клавиатура	Позволен достъп / Отказан достъп
USB модем	Позволен достъп / Отказан достъп
Неизвестно устройство	Позволен достъп / Отказан достъп

Таблица 12. Списък на поддържаните устройства и права на достъп

Модул „Content Aware Protection – Инспекция по съдържание“

Чрез този модул СПИД има възможност за ограничаване неоторизираното изтичане на чувствителната за организацията информация. Модулът анализира съдържанието на данните, преминаващи през контролираните крайни точки и следи наличието на ключови думи, изрази, идентификационни номера, шаблони и друга предварително дефинирана чувствителна информация. При наличие на зададени от Възложителя критерии и при опит за промяна, копиране, принтиране, изпращане по е-поща, препращане чрез облачни услуги, през социални мрежи и т.н., неоторизираното действие се блокира и рапортува. При това е възможно и запазване на копие на документа като се отбелязват кой, къде и кога е извършил дадените действия.

Модулът предоставя възможност за филтриране на чувствително съдържание преминаващо през електронна поща (Microsoft Outlook), уеб браузери (Internet Explorer, GoogleChrome, Mozilla Firefox и др.), платформи за комуникация, клипборд, облачни услуги и социални медии -Таблица 10.

Модулът позволява създаването на потребителски речници с чувствителна информация, на базата на която филтрира съдържание на файлове. Тези речници могат да съдържат ключови думи, изрази, идентификационни номера и шаблони на различни езици, включително и на кирилица. Възможно е комбинирането им чрез използването на Regular Expressions (RegEx).

Уеб браузер	Електронна поща	Платформи за комуникация	Облачни услуги и Услуги за споделяне на файлове	Социални медии
• Internet Explorer • Chrome	• Outlook (Attachments) • Outlook (Body)	• ICQ • AIM	• Google Drive Client • Dropbox Client	• EasyLock • Windows DVD Maker

• Mozilla Firefox	• Mozilla Thunderbird	• Skype	• iCloud Client	• ALFTP
• Opera	• Mozilla Thunderbird (Body)	• Windows Live Messenger	• uTorrent	• FileZilla
• Safari	• IBM Lotus Notes v.6.5	• Yahoo! Messenger	• BitComet	• GoToMeeting
• AOL Desktop 9.6	• IBM Lotus Notes v.7	• Gaim	• Daum Cloud	• HTC Sync for Android
• Aurora Firefox	• IBM Lotus Notes v.8.0	• Pidgin	• KT Olleh uCloud	• InfraRecorder CD - DVD
• K-Meleon	• IBM Lotus Notes v.8.5	• Trillian	• Naver N Drive	• iTunes
• Maxthon	• IBM Lotus Notes v.9.0	• NateOn Messenger	• Azureus	• LogMeIn Pro
• SeaMonkey	• Windows Live Mail	• Spark	• Box Sync	• Samsung Kies
• Tor	• GroupWise Client	• Telegram Desktop	• SugarSync	• Nokia PC Suite 2008
• Camino	• Foxmail	• Messages	• Picasa	• Nokia PC Suite 2008 Main
• iCab	• Zimbra Desktop Mail	• XChat	• Amazon Drive	• Nokia PC Suite 2011
• OmniWeb	• Endora	• TweetDeck	• iBooks Author	• Nokia PC Suite 2011 Image Store
• Sleipnir	• eM Client	• Pink Notes Plus	• MediaFire Client	• Nokia PC Suite 2011 VideoTransfer
	• Sparrow	• Google Talk	• Novell Filr Client	• Team Viewer
	• GyazMail	• Twhirl	• SendSpace	• Total Commander
	• PowerMail	• QQ international	• AirDrop	• Sony Ericsson PC Companion
	• AirMail Beta	• mIRC	• Transmission	• Total Commander 64-bit
	• Posbox	• Daum MyPeople	• FileCloud Sync Client	
	• Mail	• Naver LINE		
	• Outlook Express	• KakaoTalk	• OneDrive (Skydrive) Client	
	• Windows Mail	• Facebook Messenger	• LimeWire	
	• AOL Mail	• eBuddy	• FTP Command	
	• Courier	•	• BitTorrent	

Таблица 13. Контролирани интернет приложения

Модул „eDiscovery – Сканиране на Данни в покой“

Модулът eDiscovery осигурява предотвратяване изтичането на данни от тип „Данни в покой“ (Data-in-Rest). Модулът извършва сканиране и идентифициране на чувствителни данни на ниво крайна точка под Windows, MacOS и Linux. Модулът осигурява съответствие с регулации като GDPR, HIPAA, PCI DSS и други.
eDiscovery осигурява видимост на Данните в покой, идентифициране къде се намират чувствителните данни и последващи действия като криптиране и изтриване.

Модулът сканира и е способен да идентифицира чувствителни данни, например:

- Лична идентификационна информация (PII): номера за социално осигуряване (SSN), номера на шофьорски книжки, имейл адреси, номера на паспорти, телефонни номера, адреси, дати и др.;
- Информация за финансови и кредитни карти: номера на кредитни карти (Visa, MasterCard и др), номера на банкови сметки и други.;

Файлове с конфиденциална информация: отчети за продажби и маркетинг, технически документи, счетоводни документи, бази данни на клиенти и др..

Настройки, справки и отчети

СПИД платформата Endpoint Protector 5.0.2.1 се управлява централизирано чрез уеб интерфейс. Софтуерът дава възможност за интеграция с Microsoft Active Directory - импортиране и синхронизация. Endpoint Protector показва в реално време списък на всички контролирани потребители, както и всички устройства, свързани към съответните крайни точки.

Различните права на достъп до външните устройства - Позволен достъп / Отказан достъп / Достъп само за четене могат да се прилагат от администратора на софтуера на различни нива:

- Глобално (Global) - правата се прилагат към всички потребители, компютри и групи;
- Група (Group) - правата се прилагат към всички потребители и компютри, обединени в група;
- Компютър (Computer) - правата се прилагат към специфични компютри;
- Потребител (User) - правата се прилагат към специфични потребители;
- Устройство (Device) - правата се прилагат към специфични устройства.

Endpoint Protector 5.0.2.1 има възможност за генериране и визуализиране на разнообразни справки и отчети за нуждите на техническия и експертния персонал на Възложителя. Софтуерът предоставя възможност за вадене на статистически справки, като броя на блокираните устройства на ден, броя на свързаните към даден компютър външни устройства за даден интервал от време, най-активни потребителски устройства, най-активно използвани външни устройства и други.

СПИД платформата има възможност за генериране на аларми по електронна поща до съответния администратор при определени действия при случаи като прехвърляне на чувствителна информация, свързване на конкретно външно устройство към някой от портовете, изпращане на файл с чувствителна информация чрез електронна поща или уеб базирани приложения и други. Сървърното приложение на софтуера Endpoint Protector може да се конфигурира за достъп от предварително дефинирани IP адреси, които подлежат на преконфигуриране.

Endpoint Protector има възможност за конфигуриране на различни нива на достъп за системните администратори:

- супер системен администратор, имащ пълен достъп до всички видове настройки, справки и доклади;
- стандартен системен администратор, които има ограничен достъп.

СПИД дава възможност за създаване на административни структури, всяка със собствен системен администратор, който да няма достъп до другите административни структури. Endpoint Protector има възможност за настройка на шаблони с базови конфигурации на политиките за сигурност, които да бъдат приложени към определени потребители и/или крайни точки.

Системни изисквания

Сървър - системни изисквания:

- Минимални хардуерни изисквания към сървър: 2 x CPU, 8 GB RAM и 500 GB HDD;
- Поддържани виртуализационни среди:
  - VMware Workstation 7.1.4 или по-висока версия;
  - VMware Player 3.1.4 или по-висока версия;
  - VMware vSphere (ESXi) 5.0.0 или по-висока версия;
  - Oracle VirtualBox 4.1.16 или по-висока версия;
  - Parallels Desktop for Mac 7.0.1 или по-висока версия;
  - Microsoft Hyper-V (2008 R2) 6.1 или по-висока версия;
  - Citrix XenServer 5.5/32bit,Citrix XenServer 6.1/64bit или по-висока версия.
- Мрежова свързаност с работните станции и сървъри върху, които са инсталирани клиентските софтуерни агенти.

Клиентски софтуерни агенти - системни изисквания:

- Минимални хардуерни изисквания към работни станции: 4 GB RAM и 1 GB свободно пространство;
- Отворени локални портове 443,80 и 22;
- Поддържани ОС:
- Windows XP/7/8/10 (32/64bit);
- Windows Server 2000-2016 (32/64bit);
- NET framework 2.0;
- Mac OS 10.6-10.11;
- Linux Ubuntu,OpenSuse,CentOS,RedHat;
- eDiscovery RedHat 7+;
- Мрежова свързаност и видимост със сървъра Endpoint Protector 5.

2. Техническо описание на среда за симулация NetLogo 6.2.0

Netlogo е платформа за моделиране и симулация, базирана на агенти. NetLogo е безплатен софтуер с отворен код, издаден под GNU General Public License (GPL). Платформата предоставя програмна среда за изследване, изграждане и публикуване на агентно-базирани модели и е подходяща за използване в научни изследвания и за целите на образованието. Разработена е от проф. Uri Wilensky от Центъра за свързано обучение и компютърно базирано моделиране (CCL) на NorthWestern University, САЩ.

Netlogo притежава удобен графичен потребителски интерфейс, както и сериозен набор от вградени библиотеки с примерни модели. Чрез платформата моделите могат да бъдат описани чрез програмен език Logo, разширен за поддръжка на модели и агенти.