БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ПО ИНФОРМАЦИОННИ И
КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

ТОДОР ВЕЛЕВ ВЕЛЕВ

МОДЕЛИРАНЕ И АВТОМАТИЗАЦИЯ НА СТАНДАРТИЗИРАНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Д И С Е Р Т А Ц И Я

за придобиване на образователната и научна степен „доктор“

област на висше образование 4 Природни науки, математика и информатика, професионално направление 4.6 Информатика и компютърни науки, научна специалност „Информатика”

Научен ръководител:
проф. д-р Нина Добринкова

София, 2025 г

Съдържание

Фигури

Таблици

Списък на използвани съкращения и означения

Съкращение	Описание
BPMN	Business Process Model and Notation - моделиране и нотация на бизнес процеси
EISA	Enterprise information security architecture - архитектурата на информационната сигурност в една организация.
ISO	Международната организация по стандартизация
UML	Unified Modeling Language - унифициран език за моделиране
SQL	Structured Query Language - Език за структурирани запитвания
ИКТ	Информационни и комуникационни технологии
ИС	Информационна сигурност
НМ	Невронни мрежи
ООП	Обектно ориентирано програмиране
Платформа	Платформа за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията
СУСИ	Система за управление на сигурността на информацията

Увод

Актуалност на темата

В съвременното цифровизирано информационно общество информацията е основен актив и същевременно основна уязвимост, както за компаниите, така и за физическите лица. Електронното съдържание еволюира в два ключови аспекта непосредствено въздействащи върху професионалната и потребителската среда. Първият се отнася до обема на генерираното съдържание, а вторият до промяната на произхода му. Наблюдава се експоненциален растеж на цифровата вселена, характеризиращ се с разширяване на обхвата ѝ до ключови сектори. Тези сектори включват, но не се ограничават до финансовия сектор, електронната търговия, логистиката, управлението на лични данни и корпоративното ноу-хау. Паралелно с това се регистрира значително повишаване на свързаността и диверсификацията на комуникационните канали. Процесите са съпроводени от неконтролируема инвазия на мрежово-свързани устройства, обхващащи индивидуални, корпоративни, домашни и публични комуникационни платформи.

В тази динамична среда информационната сигурност е задача с висок приоритет и нарастващо значение. Системите за управление на информационната сигурност не са адекватни без автоматизирани платформи с елементи на изкуствен интелект, които да овладеят нарастващите по обем и видове информационни потоци и взаимодействия.

Всяка организация или компания, независимо от мащаба си, извършва дейността си във вътрешна и външна работна среда. Вътрешната се определя от ресурсите на фирмата (човешки, материални и нематериални активи и др.) и от работните процеси, свързани с предмета на дейност. Външната среда се изгражда от клиентите, доставчиците, партньорите и институциите, с които компанията взаимодейства. Международно признатите стандарти определят, регулират, управляват, наблюдават, записват и архивират вътрешната и външната среда на функциониране чрез документната система на компанията. Целта на изследвания модел е да използва най-новите технологични постижения, за да цифровизира, индексира и съживи матрицата на документите на организацията и да реализира оперативна ефективност и автоматизация на управлението и контрола. [1]

Документите на хартиен носител са пасивни. Те не позволяват едновременна употреба от няколко потребители, трудно се проследяват многобройните връзки между тях, сложно е решенията да се мултиплицират и още по-трудно да се управляват процесите въз основа на тези документи. Когато документите бъдат цифровизирани, връзките между тях се визуализират и образуваната документна матрица се облече в подходяща функционалност, резултатът е високоефективна система за наблюдение, контрол и управление на всички нива и ресурси в компанията или организацията.

Основната концепция е проектирането на отворена платформа, която позволява моделиране и ефективно управление на системи за информационна сигурност, съобразени с международно признати стандарти.

Актуалността на темата произтича от основните предизвикателства пред съвременното информационно общество, свързани с информационната сигурност и развиващи се прогресивно в условията на експанзия на ИКТ сектора, а именно: свързаност 6G; индустрия 4.0; изкуствен интелект; дигитални устройства от всякакъв вид; непрекъснато увеличаваща се изчислителна мощност и облачни технологии.

Обект и предмет на изследването

Обектът на изследване са стандартизираните системи за управление на сигурността на информацията (СУСИ) и възможностите за автоматизация на функционалностите и управлението им.

Предмет на изследване е Модел на програмен продукт комплексна Платформа, която да моделира и автоматизира произволна система за управление на сигурността на информацията, изградена в съответствие с международно признат стандарт или стандарти в тази област.

Цел и задачи

Целта на дисертационната работа е да се разработи и апробира модел на платформа, която да управлява и автоматизира стандартизирани системи за управление на сигурността на информацията.

За реализиране на тази цел са формулирани следните задачи:

- Изследване и анализ на теоретичните основи на стандартизирани системи за управление на сигурността на информацията в аспекти:
  - Сигурност на информацията;
  - Стандарти за информационна сигурност;
  - Системи за управление на сигурността на информацията СУСИ;
  - Софтуерните приложения за ИС.
- Анализ на процесите, изискванията и характеристиките на платформата за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията. Задачата е разделена в съответствие с посочената методика на следните подзадачи:
  - Изследване и анализ на работни процеси, подлежащи на автоматизация и съответстващите им информационните потоци;
  - Определяне на функционалните и нефункционалните изисквания на платформата чрез изследване и анализ на данните, на потребителските групи и на стандартите за информационна сигурност;

- Идентифициране на общите характеристики на системата.

- Проектиране на оптимален модел на платформа за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията и прилежаща архитектура.

Методи

Темата на дисертационния труд налага прилагането на интердисциплинарен подход при провеждане на изследванията, затова за изпълнение на изследователските задачи са използвани следните методи:

- на теоретично равнище:
  - библиографичен;
  - сравнителен;
  - описателен;
- на емпирично равнище:
  - евристичен;
  - анализ, синтез, обобщение;
  - моделиране.

Структура и съдържание

Дисертационният труд се състои от увод, три глави, заключение, приложения и библиография.

В увода е изяснена актуалността на проблема и са представени методическите параметри на дисертационния труд, структурата, обектът, предметът, целите и задачите.

В Първа глава е направен теоретичен анализ на фундаменталните постаменти върху които се изгражда модела на Платформата за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията, а именно: Сигурност на информацията; Стандарти за информационна сигурност; Системи за управление на сигурността на информацията СУСИ; и Софтуерни приложения за ИС. Дефинирани са терминологията и аспектите на информационната сигурност, методите, технологиите и инструментите за защита на информацията и предизвикателствата, провокиращи изследването. Анализирани са стандартите за информационна сигурност, както и терминологията, същността и целите на стандартизацията. Изследвани са основните елементи, архитектурата и процесите по разработка и внедряване на СУСИ, както и видовете и функционалния обхват на програмните продукти, свързани с управлението на СУСИ.

Във Втора глава е представена методология за изследване и моделиране на автоматизирана стандартизирана платформа за управление на сигурността на информацията и съобразно нея е извършен анализ на процесите, определяне на

изискванията и идентифициране на общите характеристики на системата. Изследват се стандартизираните работни процеси, които платформата автоматизира и кореспондиращите с тях информационните потоци. Дефинирани са функционалните и нефункционалните изисквания въз основа на анализ на данните, на потребителските групи и на стандартите за информационна сигурност. Общите характеристики на платформата са определени чрез изследване на добрите практики за потребителско поведение, продуктивност, сигурност и администрация на информационните системи. Използван е унифицираният език за моделиране – UML™ и Business Process Model and Notation (BPMN) стандарта за визуално моделиране на бизнес процеси под формата на диаграми.

В трета глава е представена авторската теория за **документна матрица**, като основа за оперативно управление на организация и компания. Описаната е методиката за моделиране и концептуалният модел на Платформата. Изработен е оптимизиран модел, изграден съобразно теоретичните постаменти и направените изследвания и анализи, представени в Глава 1 и Глава 2. Предложена е логическа и физическа архитектура за реализация на платформата.

В приложенията са представени основната терминология, одитиращите организации, изследване на данните, UML код на модела, както и реализация на модела и базата данни с SQL Alchemy и Python.

1. ГЛАВА 1. СТАНДАРТИЗИРАНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Стандартизираните системи за управление на сигурността на информацията **(СУСИ)** са ключови за защита на информацията в организациите. Те осигуряват рамка, която помага на предприятията да управляват своята информационна сигурност по систематичен и повторяем начин. [2]

Информационната сигурност е от съществено значение за организациите в наши дни, тъй като зависимостта от цифровите технологии нараства непрекъснато. Стандартизираните системи за управление на сигурността на информацията предлагат структурирани и ефективни методи за защита на информационните активи на организацията от различни заплахи, включително кибер атаки, кражби на данни, и други форми на злоупотреби.

Основните стимули за внедряване на СУСИ са:

- **Защита на информацията** - осигурява защита на конфиденциалността, целостта и достъпността на информацията, което помага на организациите да се справят със законови изисквания и да защитят чувствителните данни на клиенти и служители;
- **Устойчивост на бизнеса** - подпомагат бизнес устойчивостта, като гарантират, че критичната бизнес информация е защитена и достъпна дори в случай на инциденти или кризи;
- **Подобрение на репутацията** - прилагането на надеждни СУСИ може значително да подобри репутацията на компанията като надежден партньор или доставчик, което увеличава доверието на клиенти и партньори;
- **Съответствие с регулации** - създава рамка за спазване на регулаторни и законови изисквания, които се отнасят до защита на информацията и данните.

Системите за управление на сигурността се използват в различни сектори, включително критични инфраструктури, финанси, здравеопазване, образование и ИКТ, като осигуряват необходимата гъвкавост за адаптация към специфични бизнес модели и организационни нужди.

1.1 Сигурност на информацията

1.1.1 Дефиниране[1] и главни аспекти на информационната сигурност

Терминът "сигурност на информацията" се отнася до практиките и процесите, които се използват за защита на информация от неоторизиран достъп, употреба,

[1] Поради комплексният характер на концепцията за информационна сигурност, в специализираната литература могат да се открият голям брой различни дефиниции. В допълнение, поради все още

разкриване, разрушаване, промяна или нарушаване. Основната цел на сигурността на информацията е да осигури конфиденциалност, цялост и достъпност на данните.

Фигура 1Триада на информационната сигурност

Сигурността на информацията е приоритет за организации от всички размери и типове. Тя изисква всеобхватен подход, включващ технологии, процеси и човешки фактори. Неустойчивостта към нови и развиващи се заплахи е от съществено значение за защита на конфиденциалността, целостта и достъпността на ценните информационни активи. [3]

Обща дефиниция:

Информационната сигурност е практиката, използвана за защита на информацията от неоторизиран достъп, използване, разкриване, разрушаване/повреждане, промяна, прочит, преглед, запис или унищожаване. Това е най-обща дефиниция, която може да се използва независимо от типа/формата на данните (електронен, физически и др. ..)

Строга дефиниция на информационна сигурност:

„Запазване на поверителност, цялостност и наличност на информацията. в допълнение, могат също така да бъдат включени и други характеристики като автентичност, отчетност, не отхвърляне и надеждност.“ [4]

Дефиниция, ориентирана към бизнеса и управлението на бизнеса:

„Сигурност на информацията е защитата на информацията от заплахи с широк обхват, за да се гарантира непрекъснатост на бизнеса, да се минимизира рискът за бизнеса и да се максимизират възвращаемостта на инвестициите и възможностите за бизнес.“

Независимо от различията в дефинициите, всички в явен или неявен вид застъпват защитата на информацията от ***неоторизиран*** достъп или заплахи, като

неустановената терминология на български език, някои от понятията в материала са представени с повече от един взаимнозаменяеми термини.

главната цел е спазване на основния принцип: запазване на поверителността, цялостността и наличността на информацията.

1.1.2 Фундаментални аспекти

Елементите в триадата на информационната сигурност са както следва:

1.1.2.1 Конфиденциалност

Конфиденциалността на информацията се отнася до защитата на информация от неоторизиран достъп, използване, разкриване, промяна или унищожение. Целта е да се гарантира, че информацията остава сигурна и че достъпът до нея се контролира стриктно. Ключови компонента на конфиденциалността на информацията са: [5]

- **Защита на лични данни** - гарантиране, че личната информация на индивидите се съхранява и обработва по начин, който зачита тяхната лична неприкосновеност и съответства на законовите изисквания;
- **Контрол на достъпа** - ограничаване на достъпа до информация само до тези лица или системи, които имат легитимна нужда от нея;
- **Шифроване** - използване на технологии за шифроване за защита на данните по време на тяхното съхранение и предаване, за да се предотврати неоторизиран достъп;
- **Политики и процедури** - разработване и прилагане на политики и процедури, които уреждат как информацията се съхранява, обработва и защитава.

1.1.2.2 Цялост

Целостта на информацията се отнася до защитата и точността на данните през целия им жизнен цикъл. Това включва осигуряването, че информацията не е била променена по неправомерен начин, нито случайно, нито умишлено и че остава пълна и консистентна.

Основни елементи на целостта на информацията включват:

- **Предпазване от неоторизирани промени** - гарантиране, че само упълномощени лица или процеси могат да правят промени в данните;
- **Идентификация на нарушения в целостта** – внедряване на системи за идентифициране, които могат да открият и регистрират всеки опит за промяна на данните;
- **Хеширане и криптографски проверки** - използване на хеширащи алгоритми и криптографски методи за проверка на целостта на данните по време на тяхното съхранение и предаване;
- **Записи и одит** - създаване на подробни журнали, които записват всички операции, извършени върху данните, за да могат да бъдат прегледани и анализирани при нужда.

1.1.2.3 Достъпност

Достъпността на информацията в контекста на информационната сигурност означава способността на упълномощени потребители да получават достъп до информацията и ресурсите в нужния момент и по необходимия начин. Целта е да се гарантира, че информационните системи са налични и функционират ефективно, когато те са необходими на тези, които имат право на достъп.

Ключови елементи на достъпността на информацията включват:

- **Надеждност на системите** - увереност, че информационните системи и мрежи са устойчиви на сривове и грешки и могат да функционират непрекъснато по време на нужда;
- **Управление на ресурсите** - ефективно разпределение и управление на ресурсите, за да се осигури, че информационните системи са налични за упълномощени потребители;
- **Възстановяване след инциденти** - бързо възстановяване на системите и данните след срив или друг вид инцидент за минимизиране на прекъсванията в работата;
- **Планиране на бедствия и аварии** - разработване на планове за действие при аварии, които включват стратегии за възстановяване на системи и данни след катастрофични събития.

1.1.3 Методи за защита на информацията

1.1.3.1 Физическа сигурност

Физическата сигурност е фундаментален стълб в стратегията за защита на информацията на всяка организация и трябва да бъде внимателно планирана и регулярно преразглеждана в отговор на нови заплахи и променящи се условия. Защитата на физическите устройства и инфраструктура включва мерки за предпазване на хардуера, софтуера, данните и персонала от физически действия и събития, които биха могли да навредят на организацията. Тези мерки са насочени към предотвратяване на неразрешения достъп до важни ресурси и защита от природни бедствия, кражби и вандализъм.

Основни компоненти на физическата сигурност са:

- **Контрол на достъпа** - системи за контрол на достъпа осигуряващи, че само упълномощени лица могат да влязат в сигурни зони. Те могат да включват ключалки, карти за достъп, биометрични скенери (като отпечатъци или сканиране на ретина), и охрана;
- **Наблюдение -** видеонаблюдение и алармени системи за откриване и предотвратяване на неразрешен достъп или действия. Наблюдението може да бъде постоянно или по време на определени часове, в зависимост от изискванията за сигурност;
- **Физическа защита** – бариери, огради, врати, решетки на прозорците и

сейфове, ограничаващи физическият достъп до важни устройства и документи;

- **Защита от бедствия** - системи за пожарогасене, детектори за дим и вода, както и стратегии за управление на бедствия, необходими за защита на средствата и хората в случай на естествени или човешки катастрофи;
- **Защита на инфраструктура - з**ащита на физическата инфраструктура на ИТ системите, като кабелите и сървърите, срещу намеса или унищожение;
- **Сигурно унищожаване на данни** - машини за унищожаване на документи и софтуер за безвъзвратно изтриване на данни от твърди дискове предотвратяват изтичането на информация чрез изхвърлени или изоставени носители на данни.

1.1.3.2 Софтуерна сигурност

Софтуерната сигурност е съществена част от защитата на информацията и включва мерки за защита на софтуерните приложения и системи от злонамерени атаки или случайни грешки, които могат да доведат до изтичане или загуба на данни. Тя обхваща различни техники и практики, целящи да гарантират, че софтуерът функционира както е предвидено и че информацията, с която оперира, остава защитена от неоторизиран достъп или манипулация. [6]

Основни аспекти на софтуерната сигурност:

- Разработка на сигурен софтуер

Прилагане на най-добри практики по време на разработката на софтуер, като:

  - ***Кодиране с оглед на сигурността*** - използване на сигурни кодиращи практики за предотвратяване на уязвимости като SQL инжекции, Cross-site scripting (XSS), и буферни преливания; [7]
  - ***Автоматизирани тестове*** за ***сигурност*** - провеждане на редовни сканирания и тестове за сигурност, за да се открият и коригират уязвимости преди софтуерът да бъде пуснат в експлоатация;
  - ***Преглед на кода*** - ревюта на кода от други разработчици или специализирани инструменти за идентифициране на потенциални проблеми в сигурността.

- **Защита срещу зловреден софтуер -** инсталиране и поддържане на антивирусен софтуер и други защитни механизми за предпазване от вируси, троянски коне и друг зловреден софтуер;
- **Мениджмънт на пачове и актуализации -** редовно актуализиране на софтуера с последните пачове и версии, за да се гарантира, че всички известни уязвимости са коригирани;
- **Конфигурация на сигурността** - настройка на софтуерните системи по начин, който минимизира риска от атаки, като се деактивират ненужни услуги, настройват се правилно фаеруоли, и се прилагат принципи на най-малките права;

- **Мониторинг и логове** - поддържане на детайлни записи за активността на системата и редовен мониторинг за аномалии или признаци на злонамерена дейност;
- **Обучение на потребителите - п**овишаване на осведомеността сред потребителите, относно потенциални заплахи и най-добри практики за сигурно поведение онлайн.

1.1.3.3 Криптография [3]

Криптографията е метод за защита на информацията, който включва използването на математически алгоритми за преобразуване на ясен текст в криптиран текст и обратно. Това осигурява конфиденциалност, цялостност и автентичност на данните, като позволява само на упълномощени потребители да имат достъп и да ги интерпретират правилно.

Основни компоненти на криптографията са:

- **Симетрично криптиране** – използване на един и същ ключ за криптиране и декриптиране на данните.
- **Асиметрично криптиране** - използва на двойка ключове – публичен и частен. Публичният ключ може да бъде споделен с всеки, докато частният ключ остава таен. Асиметричното криптиране е подходящо за разпределени системи, където участниците не могат предварително да разменят тайни ключове. Примери за асиметрични алгоритми включват RSA, ECC (Elliptic Curve Cryptography).
- **Хеш функции** – преобразуване на данни от всякакъв размер в кратък, фиксиран размер хеш, който действа като уникален отпечатък на първоначалните данни. Използват се за проверка на целостта на данните и създаване на цифрови подписи. Примери за хеш функции включват SHA-256 и MD5.
- **Цифрови подписи** - комбинират асиметрично криптиране и хеш функции за създаване на подпис, който верифицира произхода и целостта на данните.
- **Протоколи за сигурност** - стандарти и методи за сигурен обмен на данни, включително TLS (Transport Layer Security) и SSL (Secure Sockets Layer), които защитават данните, предавани по Интернет.

1.1.3.4 Управление на достъпа [5]

Управлението на достъпа е критичен компонент в защитата на информацията, който се фокусира върху гарантирането на това, че правилните хора имат правилния достъп до ресурсите и данните. Този процес помага за предотвратяване на неоторизиран достъп и гарантира, че съответните лица могат да изпълняват своите задачи ефективно, без да застрашават сигурността на системите.

Основни компоненти на управлението на достъпа:

- **Идентификация** - процес, при който потребителят предоставя уникален

идентификатор (като потребителско име) за потвърждение на своята самоличност пред системата;

- **Автентификация** - следващата стъпка след идентификацията, при която потребителят доказва правото си на достъп чрез представяне на доказателства, обикновено под формата на парола, биометрични данни, или многофакторна автентификация;
- **Авторизация** - определяне на това какви действия или ресурси са разрешени за потребителя, след като той бъде успешно идентифициран и автентициран. Авторизацията се базира на ролите, правилата и политиките, установени от организацията.
- **Управление на права -** разработване и поддържане на политики, които контролират как потребителите получават или губят достъп до различни системи или данни, включително автоматизация на процесите за предоставяне и отнемане на права.
- **Мониторинг и регистрация на събития** - непрекъснато проследяване и записване на всички действия, свързани с достъпа до информационни ресурси, за анализ на тенденции и потенциални нарушения на сигурността.

1.1.4 Технологии и инструменти

1.1.4.1 Мрежова сигурност [44]

Мрежовата сигурност е област в защитата на информацията, фокусирана върху защитата на мрежовата инфраструктура и данните, които се предават чрез мрежата. Това включва предпазването от атаки, неоторизиран достъп и злонамерен трафик, което изисква комплексен подход, включващ различни технологии, инструменти и стратегии.

Основни технологии и инструменти за мрежова сигурност са:

- **Фаеруоли (Firewalls)** - фаеруолите действат като бариера между защитената вътрешна мрежа и външния свят. Те контролират входящия и изходящия трафик на базата на предварително зададени правила и политики;
- **Системи за откриване на проникване (IDS)** и предотвратяващи проникването системи (IPS) - IDS мониторират мрежата за подозрителни дейности и нарушения, докато IPS действат за блокиране на трафика, който се идентифицира като злонамерен;
- **Виртуални частни мрежи (VPN)** - VPN технологията позволява сигурно свързване към корпоративната мрежа от разстояние чрез криптиран тунел, като по този начин се предпазва трафикът от подслушване и манипулации;
- **Антивирусен и антималуер софтуер** - тези инструменти сканират и предпазват мрежовите устройства от вируси, троянски коне и друг зловреден софтуер;
- **Системи за управление на сигурността на информацията и събития**

(SIEM) - SIEM системите събират, анализират и представят данни от различни мрежови устройства, позволявайки на специалистите по сигурността да идентифицират и реагират на инциденти в реално време.

- **Сегментация на мрежата** - разделянето на мрежата на по-малки сегменти помага за ограничаване на достъпа до ресурси и управление на трафика, като по този начин се увеличава сигурността и се улеснява управлението.
- **Разширена защита от заплахи (ATP)** - ATP решенията анализират мрежата, облака и мобилните устройства за идентифициране и реагиране на сложни заплахи, които традиционните инструменти може да не засекат.

1.1.4.2 Биометрични системи [10]

Биометричните системи са инструмент за защита на информацията, използващи уникални физиологични или поведенчески характеристики на индивидите за идентификация и автентификация. Те предлагат повишена сигурност в сравнение с традиционните методи като пароли и PIN кодове, тъй като биометричните данни са трудни за копиране, споделяне или откradване.

Основни видове биометрични системи:

- **Отпечатъци на пръсти -** най-широко използваната форма на биометрична идентификация, използва уникалните модели на пръстовите отпечатъци за разпознаване на лица;
- **Разпознаване на лица** - анализира фасциални черти за идентифициране на индивиди. Тази технология се използва все повече в мобилни устройства, системи за наблюдение и контрол на достъп;
- **Ирисово сканиране** - сканира уникалните модели на ириса на окото, който е изключително труден за подражание поради сложната си структура;
- **Разпознаване на гласа** - идентифицира и верифицира лица чрез анализ на гласовите им характеристики. Полезно за телефонни системи и приложения за виртуални асистенти;
- **Динамиката на набиране** - оценява начина, по който потребителите пишат на клавиатура или мобилно устройство, включително ритъм и скорост на набиране;
- **Разпознаване на поведенчески ходове** - анализира начина на ходене или други двигателни модели за идентификация на индивиди.

1.1.4.3 Криптиране на данните [3]

Прилагането на силни алгоритми за криптиране, както на трансмитирани, така и на съхранявани данни, е от съществено значение за поддържането на сигурността на информацията във всички среди. Това подходящо защитава данните срещу различни заплахи, включително хакерски атаки, неоторизиран достъп и физическо откradване на носители на данни.

- **Криптиране на трансмитирани данни**

Използване на TLS/SSL за защита на данните, които се предават между клиент и сървър или между две крайни точки. Тези протоколи криптират информацията, преди тя да бъде изпратена през интернет, което осигурява конфиденциалност и защита срещу "man-in-the-middle" атаки. Виртуалните частни мрежи (VPN) също използват криптиране за защита на трафика, особено когато данните трябва да пътуват през обществени или незащитени мрежи. [8]

- **Криптиране на съхранявани данни**

Използва се пълно дисково криптиране (FDE) което криптира целия диск, включително системните файлове, програмите и личните файлове. Това гарантира, че всички данни на диска са защитени и не могат да бъдат прочетени без съответния ключ за декриптиране. Прилагането на криптиране на отделни файлове или бази данни е друг подход, който позволява по-фин контрол върху кои данни се криптират. Това е полезно, особено в среди, където различни видове данни имат различни изисквания за защита.

- **Избор на силни алгоритми**

AES (Advanced Encryption Standard) се препоръчва широко и се счита за златния стандарт за криптиране. Той поддържа ключове с дължина 128, 192 и 256 бита и се използва както от правителствени организации, така и от частния сектор. RSA е друг широко използван алгоритъм за асиметрично криптиране, ефективен за криптиране на малки блокове данни или за създаване на цифрови подписи.

- **Управление на ключовете**

Ефективното управление на ключовете е от решаващо значение за успеха на криптирането. То включва:

  - Генериране и съхранение на ключове - ключовете трябва да бъдат генерирани по безопасен начин и съхранявани в защитена среда, като хардуерни модули за сигурност (HSM);
  - Ротация и отмяна на ключове - регулярната ротация на ключове помага за намаляване на риска от компрометиране и улеснява управлението на ключовете.

Прилагането на тези стратегии и практики подсигуряват защитата на трансмитираните и съхраняваните данни от злонамерен достъп и кибератаки, като същевременно поддържат целостта и конфиденциалността на информацията.

1.1.5 Обучение и осведоменост

1.1.5.1 Обучение на служителите

Обучението на служителите има съществена роля в стратегията за защита на информацията на всяка организация. Често хората са най-слабото звено в веригата на сигурността и затова образованието и осведомеността на персонала могат значително

да повишат общата защита на информационните активи. Обучението трябва да бъде регулярно, за да отговаря на непрекъснато развиващите се заплахи и технологии.

Целите на обучението на служителите относно защита на информацията са:

- **Повишаване на осведомеността за заплахите** – служителите трябва да разбират различните видове киберзаплахи, като фишинг, социално инженерство, малуер и атаки чрез злонамерен софтуер;
- **Обучение за добри практики за сигурност** - това включва безопасно сърфиране в интернет, използване на силни пароли, регулярна смяна на паролите, използване на двуфакторна автентификация и безопасно споделяне на информация;
- **Разбиране на корпоративните политики и процедури** - служителите трябва да знаят вътрешните политики на компанията за защита на информацията, включително политиките за защита на данни, управление на устройства и отговор при нарушение на сигурността;
- **Разработване на отговор на инциденти** - обучението трябва да включва процедури за действие при забелязване на инцидент, като кого да уведомят и какви стъпки да предприемат.

Ефективно обучение се реализира с:

- **Регулярни обучителни сесии** - провеждане на обучения на регулярна основа, за да се гарантира, че служителите са информирани за най-новите заплахи и тенденции в сигурността;
- **Интерактивни и ангажиращи формати -** използване на интерактивни обучения, като симулации на фишинг атаки и работилници, които помагат на служителите активно да участват и да запомнят информацията;
- **Персонализирани обучения** - адаптиране на обучението в зависимост от ролята и отговорностите на служителите, осигурявайки по-специфична информация за тези, които работят с по-чувствителни данни;
- **Използване на онлайн платформи за обучение** - електронните платформи могат да предоставят гъвкавост и лесен достъп до обучителни материали и да позволят на служителите да учат в удобно за тях време;
- **Оценка и обратна връзка** - редовно оценяване на знанията на служителите чрез тестове или въпросници и събиране на обратна връзка за подобряване на обучителните програми.

Обучението на служителите е непрекъснат процес, който изисква ангажираност от страна на управлението и активно участие от страна на служителите. Подходящото и целенасочено обучение може значително да увеличи нивото на сигурност и да помогне за създаването на култура на осведоменост за сигурността в цялата организация.

1.1.5.2 Култура на сигурност

Културата на сигурност в организацията е елемент, който влияе на всички аспекти на защитата на информацията. Тази култура обхваща възприемането на норми, поведения и стандарти, които подкрепят и укрепват мерките за сигурност на данни. Целта е да се създаде среда, в която всички служители са информирани, отговорни и ангажирани с защитата на корпоративните и клиентските данни.

Основни компоненти на културата на сигурност са

- **Лидерство и ангажираност** - ръководителите трябва активно да подкрепят инициативите за сигурност и да демонстрират своя ангажимент чрез ресурси и личен пример. Лидерите са отговорни за задаването на тон, който въздейства на цялата организация.
- **Политики и процедури** - ясно формулирани и лесно достъпни политики и процедури за сигурност, които са съобразени със съвременните заплахи и регулаторни изисквания; Те трябва регулярно да се преразглеждат и актуализират.
- **Обучение и осведоменост** - редовни обучения и кампании за повишаване на осведомеността, които поддържат високо ниво на знания и предпазливост сред служителите относно потенциални заплахи и добри практики за сигурност;
- **Отворена комуникация** - създаване на канали, през които служителите могат свободно да дискутират въпроси свързани със сигурността, да докладват инциденти или подозрения за нарушения без страх от възмездие;
- **Интегриране на сигурността в корпоративната култура** - сигурността трябва да бъде вградена в ежедневните дейности и решения на компанията, а не само да се разглежда като отделна или второстепенна задача.

Подобрена култура на сигурност намалява риска от информационни нарушения и повишава общата сигурност на организационните данни. Организации със силна култура на сигурност могат по-ефективно да идентифицират, отговорят и възстановяват от нарушения на сигурността. Това води до доверие от страна на клиентите и партньорите, демонстрирайки сериозен подход към сигурността.

За създаването и поддържането на ефективна култура на сигурност е необходимо постоянно внимание и усилия. Това включва:

- **Проактивно планиране** - идентифициране на потенциални рискове и разработване на стратегии за предотвратяване;
- **Адаптивност** - бърза адаптация към нови заплахи и тенденции в сигурността;
- **Оценка и мониторинг** - Редовна оценка на ефективността на текущите мерки за сигурност и въвеждане на подобрения, където е необходимо.

Културата на сигурност е непрекъснат процес, който изисква ангажираност на всички нива на организацията. Създаването на такава култура е от съществено

значение за осигуряване на дългосрочна защита на информацията и поддържане на доверието и интегритета на организацията. [9]

1.1.6 Предизвикателства

Основните предизвикателства пред съвременното информационно общество, свързани с информационната сигурност са класифицирани в три основни групи:

- Кибератаки;
- Уязвимости на софтуера;
- Човешки фактор.

Тези групи предизвикателства се развиват прогресивно в условията на експанзия на ИКТ сектора, а именно: свързаност 6G; индустрия 4.0; изкуствен интелект, дигитални устройства от разнороден вид, непрекъснато увеличаваща се изчислителна мощност и облачни технологии.

1.1.6.1 Кибератаки

Кибератаките представляват основно предизвикателство в областта на сигурността на информацията, като техният брой, сложност и тежест непрекъснато нарастват. Във всяка организация е важно да се разбере какви форми на кибератаки съществуват и как могат да бъдат предотвратени или минимизирани техните въздействия. Хакерите непрекъснато развиват своите методи и техники, което прави предотвратяването на атаки все по-трудно. В същото време с нарастващата зависимост от цифровите технологии, възможностите за потенциални атаки също нарастват. Недостигът на обучени професионалисти в областта на киберсигурността затруднява защитата и реакцията на организациите. Предизвикателство е и интегрирането на сигурността във всички аспекти на бизнеса, което е сложно, но жизненоважно за предпазване от кибератаки. [10]

1.1.6.2 Уязвимости на софтуера

Уязвимостите на софтуера водят до сериозни нарушения на сигурността, ако не бъдат адекватно управлявани. Тези уязвимости могат да бъдат резултат от различни фактори, включително грешки в кода, липса на адекватни проверки за сигурност по време на разработка или неспазване на най-добри практики при програмирането, използване на остарял/неактуализиран софтуер неправилна конфигурация, зависимости от трети страни и др. [11]

Предизвикателства свързани с уязвимостите на софтуера са предизвикани от бързият темп на разработка, сложността на системите, недостатъчно тестване, и недостиг на квалифицирани специалисти. Управлението на уязвимостите в софтуера изисква цялостен подход, който включва не само технически стратегии, но и ангажираност на цялата организация за поддържане на високи стандарти за сигурност на информацията.

- Стратегии за справяне с уязвимостите на софтуера:

- Редовни одити и оценки на кода;
- Прилагане на строги процеси за разработка;
- Автоматизиране на тестовете за сигурност;
- Бързо прилагане на пачове;
- Управление на конфигурацията.

1.1.6.3 Човешки фактор[21]

Въпреки наличието на напреднали технологии и строги протоколи, човешките грешки или недоразумения могат да доведат до сериозни нарушения на сигурността. Подходящото управление на човешкия фактор е ключово за защитата на информационните активи на организацията.

Основни предизвикателства свързани с човешкия фактор са:

- **Липса на осведоменост и обучение** - много нарушения на сигурността произтичат от липсата на достатъчно обучение и осведоменост на служителите относно рисковете и най-добрите практики;
- **Грешки при обработката на данни** - неправилно управление на данните, включително грешно изпращане на конфиденциална информация на неправилни лица или неправилно съхранение и изтриване на информация, което може да доведе до изтичане на данни;
- **Фишинг и социално инженерство** - служителите често стават жертва на атаки чрез социално инженерство, при които се манипулират да предоставят конфиденциална информация;
- **Небрежност и пренебрегване на политики за сигурност** - случаи, когато служителите умишлено или по небрежност не спазват установените политики за сигурност;
- **Вътрешни заплахи** - служители, които умишлено злоупотребяват с достъпа си до корпоративни системи за неправомерни действия или за лична изгода.

Ефективните мерки за намаляване на рисковете свързани с човешкия фактор са:

- Редовно обучение и повишаване на осведомеността;
- Създаване на култура на сигурност;
- Прилагане на политики и процедури;
- Многослойна защита (Defense in depth);
- Мониторинг и одит;
- Психологическа подкрепа и мотивация.

Управлението на човешкия фактор изисква цялостен и непрекъснат подход, който обхваща технологии, процедури и организационна култура. Това е компонент за защита на информационните активи и предотвратяване на кибератаки. [12]

1.2 Стандарти за информационна сигурност

1.2.1 Стандартизация

Стандартизацията е дейност за определяне на предписания за общо и повтарящо се прилагане, отнасящи се за действителни или евентуални проблеми, чрез които се постига оптимален ред в дадена съвкупност от обстоятелства.

Дейността по стандартизация включва процесите на разработване, одобряване, издаване и прилагане на стандартите, като се спазват общопризнатите основни принципи и правила за работа на стандартизацията. Стандартите се разработват и публикуват в интерес на обществото и представляват мощно средство за информация и взаимно разбиране между партньори. [13] Основна терминология в стандартизацията е посочена в **Приложение 1.**

1.2.2 Стандарт

Стандартите са документи, разработени с консенсус на основата на обединяване на резултатите от науката, технологиите и производствения опит. Стандартите са общопризнати правила и норми и може да включват подробни технически спецификации (характеристики и изисквания към продуктите), процедури за производство, методи за изпитване и оценяване на съответствието. Когато се прилагат стандарти, се постига по-добра ефективност при производството на продуктите и подобряване на услугите и се удовлетворяват в по-голяма степен очакванията на потребителите и клиентите. При разработване и обсъждане им участват заинтересованите от стандартизацията страни. Стандартите се разработват, преработват, изменят, коригират или отменят в зависимост от новостите в развитието на науката и технологиите. За да се отговори на потребностите на обществото и пазара, непрекъснато расте необходимостта от разработване на стандарти. [14]

Стандартите се разработват при спазването на **принципите на стандартизацията** и правилата за работа по национална стандартизация:

- доброволно участие на всички заинтересувани;
- съгласие по отношение на техническото съдържание на стандартите;
- прозрачност;
- взаимосвързаност;
- отразяване на достигнатото ниво на науката и технологиите;
- отразяване на обществените интереси;
- даване на приоритет на европейските и международните стандарти.

1.2.2.1 <u>Цел на стандартите</u>

- повишават безопасността на продуктите;
- служат за подобряване на качеството;
- осигуряват стабилни характеристики на продуктите, процесите и услугите;

- подпомагат пригодността за употреба на продуктите по предназначение;
- служат като база при оценяване на съответствието;
- водят до икономии при производството;
- подпомагат законодателството при създаването и изпълнението на нормативните актове;
- позволяват на производителите да спазват европейското законодателство;
- служат при договаряне по отношение на технически изисквания и предписания;
- подпомагат конкурентоспособността на производителите;
- подпомагат премахването на техническите пречки в търговията;
- спомагат за поддържането на екологичното равновесие;
- подпомагат опазването на околната среда;
- отразяват научните изследвания и развитието на технологиите;
- подпомагат взаимното разбирателство между партньори.

Стандартите се класифицират като Международно признати стандарти, Европейските стандарти и хармонизирани стандарти. При сертификация по определен стандарт се извършва се оценяване на съответствието съгласно неговите парадигми и изисквания. Тази терминология е описана в **Приложение 1.**

1.2.3 Стандарти за информационна сигурност

Стандартите за информационна сигурност са критично важни в днешния свързан и цифровизиран свят. Те определят практики и методологии за защита на информационни активи от неоторизиран достъп, използване, разкриване, нарушаване, изменение или унищожаване. Най-известният и широко прилаган международен стандарт в тази област е ISO/IEC 27000 серията, разработена от Международната организация по стандартизация (ISO) и Международната електротехническа комисия (IEC). [15]

Освен известните ISO/IEC 27000 серия стандарти, има и други международни и национални стандарти, които акцентират върху различни аспекти на информационната сигурност. Те помагат на организациите да защитават своите информационни системи и данни в специфични контексти или технологични сфери. [16]

- **NIST** Стандарти (National Institute of Standards and Technology, САЩ)
    - NIST SP 800-53 - Стандарт за управление на риска и защита на информационни системи и организации, широко прилаган в правителствените структури на САЩ и препоръчан за частния сектор.

- NIST SP 800-171 - Стандарт, специализиран за защита на контролирана несекретна информация в нефедерални информационни системи и организации.

- **PCI DSS** (Payment Card Industry Data Security Standard) - специализиран стандарт за защита на данни на карти, изискващ от всички организации, които приемат, обработват, съхраняват или предават информация за кредитни карти, да спазват определени мерки за сигурност.
- **GDPR** (General Data Protection Regulation, ЕС) не е технически стандарт, но поставя строги изисквания за защита на личните данни в страните от Европейския съюз. Включва принципи за сигурност на данните, които трябва да бъдат интегрирани в информационните системи на организациите.
- **HIPAA** (Health Insurance Portability and Accountability Act, САЩ) HIPAA Security Rule - регулация, която поставя стандарти за защита на медицинска информация, като изисква адекватни административни, физически и технически средства за защита на здравните данни.
- **ISO/IEC 15408** (Common Criteria) - международен стандарт за оценка на сигурността на информационните технологии, предоставящ обща структура за оценка на сигурността на продуктите и системите.
- **FISMA** - Федерален Закон за Управление на Информационната Сигурност (Federal Information Security Management Act) е закон, приет от правителството на САЩ през 2002 година.

1.2.3.1 ISO/IEC 27000

Серията ISO/IEC 27000 е глобално призната и широко приложима, като служи като основен ресурс за всички организации, стремящи се да управляват информационната сигурност по структуриран и ефективен начин.

Семейството на стандарти ISO/IEC 27000 е разработено с цел да предостави най-добри практики и насоки за управление на информационната сигурност в различни типове организации. Тези стандарти са известни като Серията за управление на информационната сигурност. Серията ISO/IEC 27000 включва различни стандарти, които покриват всички аспекти на информационната сигурност, включително риск мениджмънт, мерки за сигурност, управление на инциденти и много други.

Основни стандарти в серията ISO/IEC 27000 са:

- ISO/IEC 27000 - действа като въведение и общ преглед на цялата серия и включва речник с терминология, използвана във всички стандарти от семейството;
- ISO/IEC 27001 - основният стандарт, който определя изискванията за управление на информационната сигурност. Той включва разработването и внедряването на една всеобхватна система за управление на информационната сигурност (СУСИ);

- ISO/IEC 27002 - стандарт, който предоставя насоки за най-добри практики в управлението на информационната сигурност, включително контролите, които следва да се прилагат в рамките на СУСИ;
- ISO/IEC 27003 - Този стандарт дава насоки за прилагане на СУСИ, обяснявайки процесите и етапите на внедряване на системата;
- ISO/IEC 27004 - стандарт, който се фокусира върху мониторинга и измерването на ефективността на СУСИ;
- ISO/IEC 27005 - Този стандарт предоставя насоки за управление на риска в контекста на информационната сигурност;
- ISO/IEC 27017 - Насочен към облачната сигурност, този стандарт предоставя насоки за управление на информационната сигурност в облачни услуги;
- ISO/IEC 27018 - Стандарт за защита на личните данни в облачната среда
- ISO/IEC 27032 - Насоки за киберсигурност, които покриват различни аспекти на сигурността на интернет взаимодействията и информационната инфраструктура.

Семейството на стандарти ISO/IEC 27000 обхваща и други специфични стандарти, които разширяват обхвата и приложимостта на информационната сигурност в специфични контексти или сценарии.

Ключови стандарти, които са част от тази серия:

- ISO/IEC 27014 - насоки за управление на информационната сигурност, които фокусират върху управленските аспекти и усъвършенстването на управленските процеси във връзка с информационната сигурност;
- ISO/IEC 27019 - този стандарт е специално разработен за информационната сигурност в енергийния сектор, предоставяйки насоки за енергийни компании за защита на информационната инфраструктура;
- ISO/IEC 27031 - стандарт за устойчивост на ИКТ услуги при бедствия. Той дава насоки за подготовка и възстановяване на ИКТ способности, което поддържа бизнес устойчивост;
- ISO/IEC 27033 - поредица от стандарти, посветени на сигурността на мрежите, които дават подробни насоки за сигурно проектиране, внедряване и управление на мрежова сигурност;
- ISO/IEC 27035 - този стандарт описва принципите на управление на инциденти свързани с информационната сигурност, подпомагайки организациите в отговора на инциденти и управление на кризи;
- ISO/IEC 27036 - Серия от стандарти, свързани със сигурността на деловите взаимоотношения, като дава насоки за безопасност при аутосорсинг и други форми на делови отношения;
- ISO/IEC 27037 - Стандарт, който урежда процесите за идентификация, събиране, придобиване и защита на информация, която може да бъде

използвана като доказателство;

- ISO/IEC 27701 - Нов добавен стандарт към серията, който дава насоки за управление на лични данни и може да се използва като разширение на ISO/IEC 27001 и ISO/IEC 27002 за управление на конфиденциалността.

Тези стандарти са разработени, за да предоставят цялостна рамка за управление на информационната сигурност, която е приложима в разнообразни индустрии и технологични среди. Прилагането на стандартите от серията ISO/IEC 27000 помага на организациите да подобрят сигурността си, да спазват регулаторни и законови изисквания и да укрепят доверието на клиентите и партньорите в своята способност да управляват информационни рискове и защитават ценни данни.

1.2.3.2 NIST стандарти за информационна сигурност

NIST (National Institute of Standards and Technology) е агенция на правителството на САЩ, която работи в областта на науката за измерванията и стандартите. Основан през 1901 година, NIST има за цел да подпомогне индустрията, науката и икономиката чрез разработването на технологии, метрики и стандарти. NIST е широко признат със своята работа в областта на киберсигурността. Той разработва ръководства, стандарти и технически насоки за подобряване на сигурността на частния и публичния сектор. Примери за такива стандарти включват NIST Cybersecurity Framework и NIST Special Publication 800 серията, които помагат на организациите да управляват и намаляват рисковете за сигурността.

NIST Cybersecurity Framework (CSF) [15] е ръководство, което предоставя обща структура за управление на киберсигурността в организациите, независимо от техния размер или сектор. Рамката е проектирана да бъде гъвкава и да помага организациите да разбират, управляват и намаляват рисковете свързани с киберсигурността, докато защитават бизнес операциите си.

Основните Елементи на NIST Cybersecurity Framework са:

- **Framework Core** - ядрото на CSF се състои от пет основни функции, които са разделени на категории, под категории и информационни справочници. Петте функции са:
    - Identify (Идентифициране) - Разработване на организационно разбиране за управление на рискове в киберсигурността;
    - Protect (Защита) - Прилагане на подходящи защити за осигуряване на доставките на критични услуги;
    - Detect (Откриване) - разработване и внедряване на подходящи активности за идентифициране на настъпването на инцидент в киберсигурността;
    - Respond (Реагиране) - разработване и прилагане на подходящи действия при открит инцидент в киберсигурността;

- Recover (Възстановяване) - разработване и прилагане на подходящи дейности за възстановяване на нормалната функционалност след инцидент в киберсигурността.

- **Нива на внедряване** - тези "нива" помагат на организациите да оценят тяхното текущо ниво на управление на рискове в киберсигурността и степента на интеграция на практики в киберсигурността в техните операционни рискове и нужди. Това включва четири нива, от "Partial" (Частично) до "Adaptive" (Адаптивно).
- **Профили** - профилите представляват персонализираната конфигурация на стойностите от ядрото на рамката, които отговарят на специфични бизнес нужди и изисквания. Те помагат на организациите да установят или подобрят кибер защита си в съответствие с техните конкретни изисквания.

NIST Special Publication 800 серията представлява комплекс от документи, които предоставят подробни насоки, стандарти и рекомендации за управление на информационна сигурност, киберсигурност и защита на лични данни. Тези публикации са разработени за подпомагане на федерални агенции, организации и други заинтересовани страни в оптимизирането на техните информационни технологии и управлението на рискове.

Основни характеристики на **NIST SP 800** серията са: [15]

- **Разнообразие на теми** - серията покрива широк спектър от теми, включително криптография, управление на идентификация и достъп, рисков мениджмънт, облачни технологии, управление на инциденти, и много други. Всяка публикация се фокусира върху конкретен аспект на информационната сигурност или киберсигурност.
- **Подробни насоки** - документите предоставят изчерпателни насоки и методологии за внедряване на контроли за сигурност, оценка на риска, и други критични процедури. Тези насоки са приложими както в правителствения сектор, така и в частния сектор.
- **Обновления и Ревизии** - публикациите се актуализират регулярно, за да отразяват нововъзникващите технологии и заплахи. Това гарантира, че насоките остават релевантни и ефективни срещу съвременните киберпредизвикателства.

Основни Документи от NIST SP 800 Серията са:

- **NIST SP 800-53** "Контроли за Сигурност и Поверителност за Федерални Информационни Системи и Организации" - документ, който предоставя рамка за защитни контроли, които могат да бъдат приложени за защита на информационни системи и организации;
- **NIST SP 800-171** "Защита на Контролирана Некласифицирана Информация в Нефедерални Системи и Организации" - насоки за защита на контролирана, но несекретна информация в системи извън федералното правителство;

- **NIST SP 800-61** "Ръководство за Реагиране при Компютърни Инциденти в Сигурността" - ръководство за реагиране при компютърни инциденти в сигурността, което предоставя стъпки за ефективно реагиране и възстановяване;
- **NIST SP 800-30** "Ръководство за Провеждане на Оценки на Риск" - ръководство за провеждане на оценки на риска, което помага организациите да идентифицират, оценят и управляват информационни рискове.

NIST SP 800 серията е важен ресурс за всеки професионалист в областта на информационната сигурност и киберсигурността. Предоставяйки детайлни и проверени насоки, тези документи помагат на организациите да разработят, внедрят и поддържат сигурни информационни системи. Те също така играят ключова роля в подпомагането на организации да се съобразяват със законови и регулаторни изисквания, като предоставят стандартизирани подходи за сигурност, които могат да бъдат приложени в различни индустрии.

Серията NIST SP 800 е ключов ресурс за насоки и стандарти в областта на информационната сигурност и киберсигурността, оказвайки значително влияние върху развитието на политики и практики за сигурност в различни организации по света. Други ключови документи са:

- **NIST SP 800-37** "Ръководство за прилагане на Рамката за Управление на Риска към Федералните Информационни Системи" - Този документ описва Рамка за Управление на Риска, която интегрира процеси за сигурност и оценка на риска в жизнения цикъл на системата. Тя помага на агенциите да приемат интегриран подход към управление на риска;
- **NIST SP 800-34** "Ръководство за Планиране на Аварийни Мерки за Федерални Информационни Системи" - Ръководство за изготвяне на планове за аварийни ситуации, което предоставя насоки за възстановяване на функциите на ИТ системите след сериозен инцидент;
- **NIST SP 800-88** "Насоки за Санитарна Обработка на Медии" - Насоки за унищожаване на данни, които обсъждат методите и процесите за правилно унищожаване на информацията, за да се предотврати нейното нежелано възстановяване;
- **NIST SP 800-144** "Насоки за Сигурност и Поверителност в Публичното Облачно Изчисляване" - Предоставя насоки за сигурност и поверителност при използването на обществени облачни услуги, като обръща внимание на нуждите за управление на информационната сигурност в облачната среда.

*1.2.3.3 **FISMA*** [80]

Федерален Закон за Управление на Информационната Сигурност (Federal Information Security Management Act) е закон, приет от правителството на САЩ през 2002 година. Той има за цел да подобри сигурността на информационните системи и данните във федералните агенции. FISMA налага изисквания за

федералните агенции да разработват, документират и прилагат програми за управление на информационната сигурност.

Основни аспекти на FISMA:

- **Управление на риска** - FISMA изисква от федералните агенции да разработят цялостна политика за управление на риска, която да включва мерки за оценка, мониторинг и намаляване на рисковете за информационната сигурност;
- **Инвентаризация на активи** - Агенциите трябва да поддържат актуализиран инвентар на всички информационни системи, използвани от агенцията, както и да класифицират тези системи в зависимост от степента на риск за сигурността;
- **Оценка на сигурността** - FISMA налага редовни оценки на сигурността за всички информационни системи, за да се гарантира, че мерките за сигурност са адекватни и ефективно изпълнявани;
- **Сертификация и акредитация** - всички информационни системи трябва да преминат през процес на сертификация и акредитация, за да се увери, че са достатъчно сигурни за операциите, за които се използват;
- **Мерки за сигурност** - FISMA изисква агенциите да внедряват подходящи мерки за сигурност, които могат да включват физически, административни и технически контроли;
- **Отчетност и документация** - агенциите трябва редовно да докладват за статуса на тяхната информационна сигурност и за мерките, взети за подобряването ѝ, към Департамента на националната сигурност и други регулаторни органи.

FISMA подобрява сигурността на информацията във федералните агенции чрез въвеждането на структуриран подход за оценка, мониторинг и подобряване на мерките за сигурност. Този закон също така подпомага за уеднаквяване на практиките за сигурност в различните агенции и помага на САЩ да се защити от информационни заплахи и атаки. FISMA е стълб в усилията на федералното правителство да осигури цялостна защита на критичната инфраструктура и федералните информационни системи.

FISMA е въведена през 2002 година като част от E-Government Act. Целта на този закон е да модернизира управлението на информационната технология във федералните агенции, като подобри сигурността на цифровите активи и сведе до минимум рисковете от кибератаки. През годините, FISMA е била актуализирана и рафинирана, за да отразява променящите се технологични среди и заплахи.

Основни Компоненти на FISMA:

- Оценка на риска - федералните агенции трябва да провеждат подробни оценки на риска, за да идентифицират потенциалните уязвимости в техните информационни системи и да разработят стратегии за тяхното намаляване;
- Политики за сигурност - агенциите са задължени да разработват и поддържат

политики, които да гарантират сигурността на информационните системи и данните;

- Обучение по сигурност - FISMA изисква редовно обучение по сигурност за всички служители и подизпълнители, които имат достъп до федерална информация и системи.
- Инцидентен отговор - Агенциите трябва да разработят и прилагат планове за отговор на инциденти, които да обхващат действията при различни видове кибератаки или нарушения на сигурността.
- Годишни прегледи - FISMA изисква редовни годишни прегледи на политиките и практиките за сигурност, за да се гарантира, че те са актуални и ефективни.

Въпреки че FISMA е направила значителни стъпки към подобряване на информационната сигурност във федералните агенции, тя не е без критики. Някои критици твърдят, че законът е твърде бюрократичен и фокусиран повече на съответствие, отколкото на реалната сигурност. Също така, бързото развитие на технологиите изисква непрекъснато актуализиране и преразглеждане на насоките, за да се справи ефективно с новите заплахи.

FISMA продължава да бъде важен инструмент за управление на информационната сигурност във федералното правителство на САЩ. Редовните актуализации и реформи са от съществено значение за поддържане на ефективността на закона в защитата на информационните ресурси на нацията в динамичната киберсигурност среда.

1.2.3.4 GDPR

Общ регламент за защита на данните (General Data Protection Regulation) е регулация на Европейския съюз, която влезе в сила на 25 май 2018 година. Този регламент се прилага директно във всички държави-членки на ЕС и цели да унифицира и укрепи защитата на личните данни на гражданите в ЕС, както и да гарантира свободното движение на тези данни в рамките на Европейския съюз.

Основни аспекти на GDPR:

- Широк Обхват - GDPR се прилага за всяка организация, независимо от нейното местонахождение, стига да обработва лични данни на лица в ЕС. Това включва организации извън ЕС, които предлагат стоки или услуги на граждани на ЕС или наблюдават тяхното поведение.
- Строги Изисквания за Съгласие - съгласието трябва да бъде ясно и дадено свободно с изрично потвърждаващо действие. То трябва да бъде лесно да се оттегли, колкото е лесно да се даде.
- Права на Субектите на Данни - GDPR укрепва правата на индивидите, като предоставя по-голяма контрола върху техните лични данни. Това включва правото на достъп, правото на изтриване („право да бъдеш забравен“), правото на ограничаване на обработката, правото на данните в машинно четим формат и правото на възражение.

- Задължения за Организациите - организациите трябва да въведат мерки, които съответстват на принципите на „защита на данните чрез дизайн“ и „защита на данните по подразбиране“. Това включва поддържането на подробни записи на дейностите по обработка на данни, провеждането на оценки на въздействието върху защитата на данните и прилагането на подходящи технически и организационни мерки.
- Длъжностни Лица за Защита на Данните - определени организации трябва да назначат Длъжностно Лице по Защита на Данните (DPO), което наблюдава съответствието с GDPR, обучава персонала и извършва редовни проверки.
- Задължения при Нарушения на Сигурността - организациите трябва да уведомят съответния надзорен орган за някои видове нарушения на сигурността в срок до 72 часа след откриването им, ако има вероятност нарушението да представлява риск за правата и свободите на физическите лица.
- Трансгранична Обработка и Одити - GDPR урежда трансграничната обработка на данни и установява координационни механизми и одити, за да се гарантира, че правилата се прилагат еднакво в целия ЕС.
- GDPR е една от най-строгите и всеобхватни регулации за защита на данните в света. Тя слага фокус върху прозрачността, отговорността и правата на индивидите, което гарантира, че личните данни се обработват безопасно и законно. Несъответствието с GDPR може да доведе до значителни финансови санкции, достигащи до 4% от глобалния годишен оборот на организацията или 20 милиона евро, в зависимост от коя сума е по-голяма.

Регламентът GDPR (Общ регламент за защита на данните) има за цел да засили и унифицира защитата на личните данни за всички индивиди в Европейския съюз, а също така регулира износа на лични данни извън ЕС. Той поставя нови изисквания за организациите, които събират, съхраняват или обработват лични данни, и предлага по-строг контрол за субектите на данните. Ето още ключови аспекти и въздействия на GDPR:

Допълнителни аспекти на GDPR

- Оценки на въздействието върху защитата на данните (DPIA) - GDPR изисква организациите да провеждат DPIA за операции по обработка, които вероятно представляват висок риск за правата и свободите на индивидите. Това помага да се идентифицират и минимизират рисковете от обработката на данни.
- Защита на данните от най-ранен етап (Data Protection by Design): Организациите трябва да вградят мерки за защита на данните в технологичните си системи и процеси от самото начало, а не като допълнителен елемент.
- Управление на съгласие - съгласието трябва да бъде ясно, конкретно, информирано и давано чрез активно действие. Субектите на данните трябва да имат възможността лесно да оттеглят своето съгласие по всяко време.

- Правото на преносимост на данните - този аспект позволява на субектите на данните да получат и прехвърлят своите данни от една организация в друга по безпрепятствен и сигурен начин.
- Въведение на концепцията за съгласуван авторитет - при трансгранична обработка на данни, организациите се отчитат пред един водещ регулаторен орган в ЕС, което улеснява управлението на съответствието.

Въздействие на GDPR:

- Укрепване на доверието - Подобряването на защитата на данните укрепва доверието между потребителите и организациите, тъй като клиентите знаят, че тяхната информация се обработва прозрачно и сигурно.
- Глобални изисквания - GDPR засяга не само компаниите, базирани в ЕС, но и всички организации в световен мащаб, които обработват данни на граждани на ЕС, което прави регламента глобален стандарт за защита на данните.
- Санкции - Неспазването на GDPR може да доведе до значителни финансови глоби, което налага строга финансова отговорност и подтиква компаниите да вземат на сериозно изискванията за защита на данните.

GDPR е значителна стъпка напред в правната рамка за защита на личните данни и установява нов стандарт за прозрачност, отчетност и безопасност в обработката на лични данни.

1.3 Системи за управление на сигурността на информацията

Системите за управление на сигурността на информацията представляват систематичен подход за управление на чувствителната информация на организацията, като се гарантира нейната сигурност чрез прилагане на подходящи технически и организационни мерки. Целта на СУСИ е да защити информацията от различни заплахи и да осигури продължаването на бизнес процесите, минимизиране на риска от загуби и максимизиране на възвращаемостта на инвестициите и възможностите за бизнес. [17]

1.3.1 Основни елементи

Основни елементи на СУСИ са:

- **Оценка на риска** - провеждането на оценка на риска е фундаментална стъпка в СУСИ. Тя включва идентифициране на активи, оценка на заплахи и уязвимости, които засягат тези активи, и оценка на потенциалните последствия от компрометирането на информацията;
- **Политики за сигурност** - разработването на подходящи политики за сигурност, които определят стандартите и процедурите за управление на информацията. Тези политики трябва редовно да се преразглеждат и актуализират, за да останат в крак с променящите се технологии и бизнес условия;
- **Физическа и логическа сигурност** - включва мерки като контрол на достъпа

до сгради и помещения, както и информационни системи, за да се гарантира, че само упълномощени лица имат достъп до чувствителна информация;

- **Управление на инциденти** - разработване на процедури за реагиране при инциденти, които включват идентифициране, докладване, разследване и възстановяване при нарушения на сигурността;
- **Обучение и съзнание** - редовно обучение на служителите относно политиките и процедурите за сигурност, както и повишаване на осведомеността относно потенциалните киберзаплахи и начините за тяхното предотвратяване;
- **Непрекъснат мониторинг и подобрение** - непрекъснато мониторинг на ефективността на СУСИ и въвеждане на подобрения, където е необходимо, за да се справи с новите или променящи се рискове.

Системите за управление на сигурността на информацията (СУСИ) са набор от политики, процедури и мерки, които една организация прилага, за да защити своята чувствителна информация. Те осигуряват рамка за идентифициране, анализ, управление и непрекъснато подобряване на сигурността на информационните активи. СУСИ предпазват конфиденциалната информация от неоторизиран достъп, използване, разкриване, промяна и унищожаване. Много индустрии имат специфични законови изисквания за сигурността на данните и СУСИ гарантират на организациите спазването на тези изисквания. Клиентите и партньорите имат по-голямо доверие в организации, които са демонстрирали ангажираност към сигурността на информацията. СУСИ спомагат да се предотвратят финансови загуби, прекъсвания на бизнеса и увреждане на репутацията, причинени от кибератаки и други инциденти. [18]

1.3.2 Разработка и внедряване

СУСИ се разработва конкретно за всяка компания или организация, отразявайки нейната специфика. Внедряването на система за управление на сигурността на информацията е значително начинание, изискващо ангажираност на всички нива в организацията и строга методология за планиране, изпълнение, мониторинг и непрекъснато подобрение. Основните стъпки, които се следват при внедряването на СУСИ са:

1. Определяне на обхвата и целите

Определя се обхвата на СУСИ, като се избира кои процеси, информация, технологии и географски локации ще бъдат включени. Ясното дефиниране на целите на системата помага за ориентация на проекта и измерване на неговия успех.

2. Ангажиране на Ръководството

За успеха на СУСИ е критично да има ангажираността и подкрепата на висшето ръководство. Те трябва да разбират ползите от СУСИ и да предоставят необходимите ресурси.

3. Оценка на риска

Провежда се оценка на риска за идентифициране на потенциалните заплахи за информационните активи и се определят уязвимостите, които могат да бъдат експлоатирани. Оценява се вероятността и потенциалните последствия от тези рискове.

4. Разработване на политики и процедури

Създават се подробни политики и процедури за управление на информационната сигурност, които да отразяват резултатите от оценката на риска и стратегията на организацията за справяне с тези рискове.

5. Прилагане на контроли

Прилагат се избраните контроли и решения за сигурност, които да помогнат за намаляване на идентифицираните рискове до приемливо ниво. Това може да включва технически мерки, както и организационни изменения.

6. Обучение и съзнателност

Организират се обучения за всички служители, включващи правилата и процедурите на СУСИ. Развива се култура на сигурност в рамките на организацията.

7. Мониторинг и преглед

Регулярно се наблюдава и преглежда ефективността на СУСИ. Това включва проследяване на инциденти, провеждане на вътрешни одити и събиране на обратна връзка от служителите.

8. Подобрения

На базата на събраната информация от мониторинга и прегледите, се идентифицират нуждите за подобрения в системата. Планират се и се реализират мерките за постоянно подобряване на системата за управление на сигурността.

9. Сертификация

Организациите могат да изберат да се сертифицират по ISO/IEC 27001, което може да увеличи доверието на клиентите и другите заинтересовани страни в управлението на информационната сигурност в организацията.

Внедряването на СУСИ е процес, който изисква време, ресурси и постоянство, но предоставя значими дългосрочни ползи за сигурността и устойчивостта на организацията.

1.3.3 Видове СУСИ [38]

Системите за управление на сигурността на информацията (СУСИ) могат да варират значително в зависимост от специфичните нужди, размера и характера на дадена организация, както и от отрасловите стандарти и регулации, които се прилагат. Основни вида СУСИ, които са разработени за различни приложения и среди:

- ISO/IEC 27001 базиран СУСИ

Това е най-широко разпространеният международен стандарт за СУСИ, който предоставя рамка за управление на информационната сигурност във всякакви видове

организации. Той изисква определяне на рискове, имплементиране на подходящи контроли за сигурност и редовен мониторинг и преразглеждане на ефективността на тези контроли.

- Отраслово-специфични СУСИ

Различни отрасли имат специфични изисквания за сигурност, което води до разработването на отраслово-специфични системи за управление на сигурността:

  - PCI DSS за финансовата индустрия, особено за организации, които обработват платежна информация;
  - HIPAA в здравеопазването за защита на защитената здравна информация (PHI);
  - FISMA за американските федерални агенции, за да отговори на изискванията на федералното законодателство за управление на информационната сигурност.

- Облачни и Интернет на нещата (IoT) СУСИ

С нарастването на облачните услуги и IoT устройствата, са разработени специализирани системи за управление на сигурността, които се справят с уникалните предизвикателства на тези среди. Те включват контроли за защита на данни в облака и управление на идентификациите и достъпа в множество устройства и платформи.

- Военни и правителствени СУСИ

Тези системи са разработени с много високи стандарти за сигурност, за да защитават класифицирана и високо секретна информация. Те често използват много сложни и строго контролирани технически и физически мерки за сигурност.

- СУСИ за малък и среден бизнес (МСП)

Специално адаптирани системи за управление на сигурността, които са разработени с оглед на ограничените ресурси и нужди на малки и средни предприятия. Тези системи обикновено са по-прости и струват по-малко, но предоставят основни контроли и защити.

- Интегрирани СУСИ

Тези системи се интегрират с други системи за управление, като системи за управление на качеството (ISO 9001) или системи за управление на околната среда (ISO 14001), за да предоставят всеобхватен подход за управление на рисковете и управление в организацията.

Всяка от тези системи трябва да бъде избрана и адаптирана според специфичните нужди и контекста на организацията. Изборът на подходящ тип СУСИ е критичен за осигуряване на ефективността и устойчивостта на организационните мерки за сигурност.

1.3.4 Архитектура и управление на информационната сигурност

Архитектурата на информационната сигурност в една организация (Enterprise information security architecture - EISA) е практиката на прилагане на цялостен и строг метод за описване на текуща и/или бъдеща структура и поведение на процесите за сигурност, системите за информационна сигурност, персонала и организационните подразделения в организацията, по такъв начин, че те да се приведат в съответствие с основните цели и стратегическите насоки на организацията. Въпреки че, EISA често се асоциира стриктно с технологиите за информационна сигурност, все пак тя има по-широк смисъл и обхват и се отнася до сигурни практики за оптимизация на бизнеса дотолкова, доколкото засяга архитектурата за сигурност на бизнеса, управлението му както и архитектурата на процесите за сигурност.

Основната цел на създаването на архитектура за информационна сигурност на организацията е да се гарантира, че бизнес стратегията и ИКТ-сигурността са съгласувани (не си противоречат). При това условие, архитектурата на информационната сигурност в предприятието и организацията осигурява проследимост на процесите в посока отгоре-надолу: от бизнес стратегията до използваните основни технологии.

В последните години, развитието на високите технологии и най-вече на ИКТ налагат нов подход при изграждане на архитектурата на съвременните предприятия и организации: ориентирана към услугите архитектура. При този подход, архитектурата на организацията е съставна и се изгражда от ориентирани към услугите: бизнес архитектура, информационна архитектура и архитектура на използваната базова технология (на английски BIT - Business architecture, Information architecture and Technology architecture). С добавянето на четвъртия елемент – архитектурата на сигурността (Security architecture) архитектурата на съвременните предприятия става популярна под абревиатурата BITS. [19]

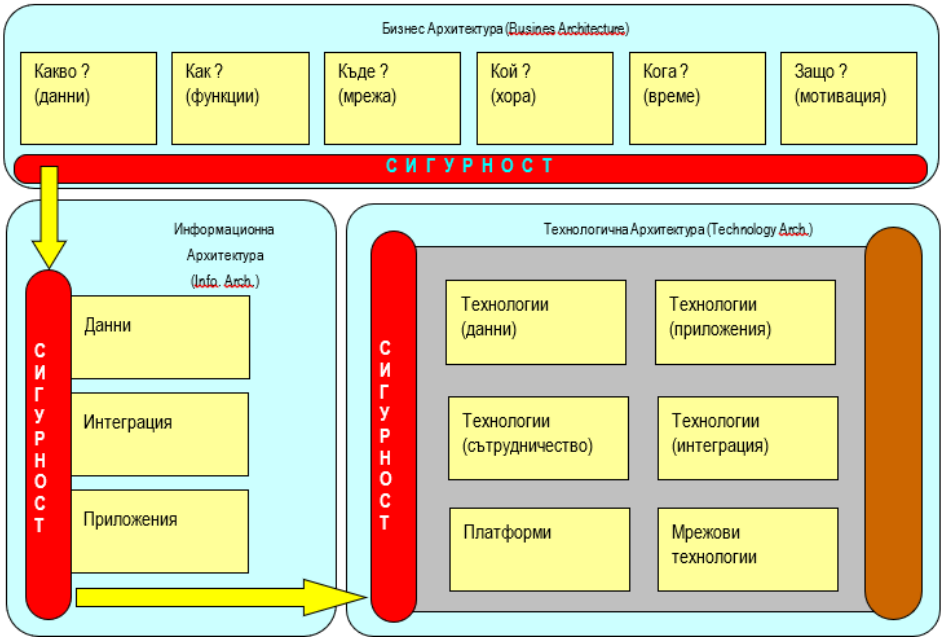
Архитектурната рамка на сигурността е само част от общата рамка на организацията. В максимално опростен вид, една концептуална абстракция от най-високо ниво на архитектурата на сигурността, интегрирана в общата архитектурна рамка на организацията е показана на фигурата.

Интегрирането на сигурността в съставната архитектура на организацията, от своя страна, налага промени и нови изисквания, свързани с аспекти като:

- въвеждане и използване на бизнес пътни карти,
- съобразяване със законодателни и правни изисквания,
- въвеждане и използване на технологични пътни карти,
- следене и съобразяване с тенденциите в промишлеността,
- следене на тенденциите на риска,
- анализ на перспективите (визия за развитие).

Основните цели на архитектурата на сигурността са [20]:

- Осигуряване на структура, съгласуваност и консолидация/свързаност;
- Осигуряване на възможност за съгласуване между бизнеса и сигурността;
- Дефиниране на подход отгоре-надолу, започвайки с бизнес стратегия;
- Осигуряване на увереност, че всички модели и реализации/приложения могат да бъдат проследени обратно към бизнес стратегията, специфичните изисквания на бизнеса и ключовите принципи;
- Осигуряване на възможности за абстракция, така че усложняващи фактори, като географски и технологични специфики, да могат да бъдат отстранявани и възстановявани на различни нива на детайлност, само когато е необходимо;
- Установяване на общ, ясен и недвусмислен "език" за информационна сигурност в рамките на организацията.



Фигура 2 Архитектурата на сигурността

1.3.5 Други аспекти на СУСИ

В обсега на концепцията за система за управление на информационна сигурност попадат и следните аспекти:

- управление на процеси, свързани с ръководство и стратегически насоки на политиките по информационната сигурност;
- непрекъснатост на бизнес процесите;
- контрол над процесите по управление на инциденти и промени [21];
- планиране на възстановяването след бедствие;
- съобразяване със закони и регулации;

- изграждане на култура на информационната сигурност;
- въвеждане и използване на стандарти.

1.4 Софтуерни системи и приложения за информационна сигурност

Системите за управление на информационната сигурност разчитат на разнообразен набор от софтуерни инструменти, за да осигурят ефективна защита във всички етапи от жизнения цикъл на многообразните информационни масиви. [22]

Програмните продукти могат да бъдат класифицирани в следните функционални категории:

- SIEM системи (Security Information and Event Management) - Системи за управление на информация за сигурността и събитията;
- Софтуер за управление на идентификационни данни и достъп (Identity and Access Management - IAM);
- Антивирусен и антималуер софтуер;
- Софтуер за криптиране;
- GRC Платформи (Governance, Risk Management, and Compliance), Платформи за управление, управление на риска и съответствие";
- Софтуер за управление на уязвимости;
- Софтуер за анализ на потока от данни (Data Loss Prevention - DLP);
- Софтуер за резервно копиране и възстановяване;
- Облачна сигурност (Cloud Security);
- Софтуери за мрежова сигурност;
- Софтуер за управление на инциденти.

Всяка категория програмни продукти има специфична функционалност и множество компании разработчици, предлагащи съответните конвенционални решения. [41]

1.4.1 Конвенционален софтуер свързан със СУСИ

В различните аспекти на Системите за управление на сигурността на информацията се предлагат от множество доставчици конвенционални софтуерни продукти с кореспондираща функционалност:

- Управление, управление на риска и съответствие GRC (Governance, Risk Management, and Compliance) - Тези системи осигуряват централизиран подход към управлението на управленските процеси, риск мениджмънта и спазването на нормативната уредба. Примери: RSA Archer; MetricStream; ServiceNow GRC.
- Софтуер за криптиране - инструменти за криптиране на данни в покой и по време на трансфер. Примери: Symantec Encryption; VeraCrypt; BitLocker.

- Антивирусен и антималуер софтуер - Тези инструменти защитават системите от зловреден софтуер и атаки. Примери: Avast Antivirus; SET NOD32 Antiviru; Trend Micro Antiviru; Kaspersky; Norton; McAfee и много други.
- Софтуер за управление на идентификационни данни и достъп (Identity and Access Management - IAM) - Системи, които управляват идентичностите на потребителите и контролират техния достъп до ресурси. Примери: Okta; Microsoft Azure Active Directory; IBM Security Identity Manager.
- Системи за управление на сигурността на информацията и събития SIEM (Security Information and Event Management) - осигуряват събиране, анализ и отговор на сигурностни събития в реално време. Примери: Splunk; IBM QRadar; LogRhythm.
- Софтуер за управление на уязвимости - този тип софтуер идентифицира, класифицира и управлява уязвимостите в системите. Той помага на организациите да приоритизират и тстраняват уязвими точки преди те да бъдат използвани от атакуващите. Примери: Qualys; Tenable Nessus; Rapid7.
- Софтуер за анализ на потока от данни (Data Loss Prevention - DLP) - Системите DLP помагат на организациите да предотвратяват нежеланото изтичане или използване на чувствителна информация. Symantec DLP; McAfee Total Protection for Data Loss Prevention; Digital Guardian.
- Софтуер за резервно копиране и възстановяване - продукти за възстановяване след събития, които могат да доведат до загуба на данни, като например хардуерни повреди, софтуерни проблеми или кибератаки. Примери: Nakivo; Veeam, Acronis True Image; Veritas Backup Exec.
- Мрежови инструменти - включват файруол, системи за предотвратяване на проникванията (IPS), и виртуални частни мрежи (VPN). Примери: Cisco ASA; Fortinet FortiGate; Palo Alto Networks Firewall.
- Облачна сигурност (Cloud Security) - инструменти и стратегии за защита на данни, приложения и инфраструктура, разположени в облака. Примери: Amazon Web Services (AWS) Security; Microsoft Azure Security; Google Cloud Security.
- Обучение и осъзнаване на сигурността - софтуерни платформи, които предоставят обучение и тестове за осведоменост относно киберсигурността на служителите. Примери: KnowBe4; Proofpoint Security Awareness Training; SANS Securing The Human.
- Софтуер за управление на пачове - автоматизирано управление на процеса на инсталиране на софтуерни пачове за отстраняване на уязвимости. Примери: Microsoft SCCM; WSUS; Puppet.
- Софтуер за анализ на заплахи - събиране и анализ на информация за най-новите заплахи, за да се подобрят защитните мерки. Threat Intelligence Platforms (TIPs) от различни доставчици.

- Софтуер за управление на инциденти - управление на целия жизнен цикъл на един инцидент, от откриването до разрешаването. Примери: ServiceNow Security Operations; IBM Security Incident Response Platform.

1.4.2 Софтуер за управление на стандарти по информационна сигурност.

Този тип софтуер помага на организациите да създават, управляват и поддържат Системите за управление на сигурността на информацията (СУСИ). Сравнителен анализ е показан в Таблица 1.

- ISMS.online [23]

Тази платформа предлага изчерпателен набор от инструменти за управление на всички аспекти на съответствието с ISO 27001, включително управление на риска, управление на активи и виртуален коуч. Цели да опрости процеса на съответствие и може да намали времето за сертификация с предварително изградени инструменти и политики.

- Compleye [24]

Този инструмент е специално проектиран за стартиращи и нарастващи компании, предоставяйки опростена, всичко-в-едно платформа за постигане на сертификация по ISO 27001. Включва над 30 шаблона за политики, готови за одит, и функции като управление на инциденти и доставчици.

- Vanta [25]

Vanta се фокусира върху автоматизирането на съответствието, предлагайки функции като непрекъснато наблюдение и автоматично събиране на доказателства. Насочена е към предоставяне на лесен път за управление не само на ISO 27001, но и на други стандарти като SOC 2 и GDPR

- Scytale [26]

Известен със своите възможности за автоматизация, Scytale е специално проектиран за компании, предлагащи софтуер като услуга (SaaS), и помага за опростяване на усилията за съответствие с функции като автоматично събиране на доказателства, управление на одити и непрекъснат мониторинг.

- Apptega [27]

Съсредоточен върху опростяването на процеса на съответствие, Apptega предлага функции за оценка на риска, управление на одити и създаване на политики, заедно с изчерпателно табло за мониторинг на съответствието в реално време.

- AuditBoard [28]

Известен със своите силни функции за управление на одити, AuditBoard автоматизира процеса на одит от началото до края, улеснява управлението на документацията и следенето на съответствието. Той също така предоставя възможности за докладване и анализ.

- Secureframe [29]

Цели да осигури на организациите инструменти за непрекъснат мониторинг и актуализации в реално време, гарантиращи ефективно управление на сигурността, поверителността и съответствието.

Горепосочените системи са най-популярните софтуери в изследваната област, които могат да бъдат разглеждани като представителна извадка. Те са фокусирани върху процесите по сертификация, поддръжка и одитиране на стандартите по информационна сигурност и свързаната с тях документация. Основни функции са:

- Управление на съответствието
- Управление на риска
- Автоматизация на задължения по сигурността
- Управление на достъпа и уязвимостите
- Интеграции
- Образователни ресурси и подкрепа за клиентите

С оглед извършените анализи в Глава 1 и еволюцията на описаните предизвикателства този обхват на системите не е достатъчен. За да има максимална ефективност е необходимо всички работни процеси в една компания да бъдат цифрово индексирани и управлявани от единен софтуер, предмет на настоящата теза, който да бъде моделиран съобразно въведената в организацията СУСИ.

1.5 Основни изводи към Глава 1

- ☞ Въз основа на направения анализ на сигурността на информацията, стандартите за информационна сигурност и системите за управление на сигурността на информацията се налага извода, че е необходим комплексен подход за справяне с описаните прогресиращи предизвикателства.
- ☞ От изследването на видовете и функционалния обхват на софтуерните приложения, свързани със СУСИ се идентифицира сегментацията на продуктите. Системите за цялостно управление на СУСИ са предимно в аспекти сертификация, ре сертификация и поддържане на необходимите записи и шаблони за целите на одитния процес. Липсват цялостни решения които да управляват и контролират всички работни процеси и информационни потоци в инфраструктурата и суперструктурата на организацията. Платформения подход за изграждане на адаптивна система, моделираща и автоматизираща стандартизирани системи за управление на сигурността на информацията е иновативно, генерализирано решение на третираната проблематика.
- ☞ С цел да се гарантира ефективност, полезност и надеждност на платформата е необходимо да се разработи модел, който се базира на цялостен мониторинг, анализ и управление на документната матрица, работните процеси и информационните потоци и активи на организацията.

Таблица 1 Сравнителен анализ на софтуера за управление на стандарти и Платформата

Функционалност/Процес	ISMS.online	Compleye	Vanta	Scytale	Apptega	AuditBoard	Secureframe	Платформа
Управление на съответствието с ISO 27001	X		X	X	X	X	X	X
Шаблони	X	X	X	X	X	X	X	X
Управление на съответствието по други стандарти			X			X	X	X
Автоматизация на одитен процес	X	X	X	X	X	X	X	X
Управление на риска	X		X	X	X	X	X	X
Автоматизирано събиране на записи						X	X	X
Непрекъснат мониторинг						X		X
Управление на процеси от СУСИ	X		X	X			X	X
Управление на документация по СУСИ	X	X	X		X	X		X
Възможност за моделиране на всички бизнес процеси на организацията								X
Възможност за моделиране на СУСИ			X	X			X	
Цялостно управление на бизнес процесите и мониторинг на информационната сигурност съобразно СУСИ								X

2. ГЛАВА 2. МОДЕЛИРАНЕ НА ПЛАТФОРМА ЗА УПРАВЛЕНИЕ И АВТОМАТИЗАЦИЯ НА СТАНДАРТИЗИРАНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА.

В съвременното развито информационно общество, характеризиращо се с бързо нарастваща цифровизация на процесите и ежедневно генериране на големи обеми информация, управлението на информационната сигурност е ключово условие за успех, свързано със значителни рискове. Системите за управление на информационната сигурност осигуряват необходимите механизми за защита на информационните активи и гарантиране сигурността на всички заинтересовани страни. Международните стандарти определят ясни изисквания за създаване, внедряване, експлоатация, наблюдение, преглед, поддръжка и постоянно подобряване на документираните СУСИ в контекста на общите бизнес рискове на организацията. Моделите, описани в тези стандарти, са универсални и подходящи за всяка организация, независимо от нейния размер, вид и сфера на дейност. [30]

Предизвикателствата пред платформа за автоматизация и управление на системи за управление на информационната сигурност са да моделира, дигитализира, регистрира, управлява, съхранява и контролира работните процеси и цялата свързана с тях информация и документация в реално време. Необходима е платформа, тъй като функционирането на СУСИ на организациите се влияе от техните нужди и цели, изисквания за сигурност, използваните процеси, размера и структурата на организацията, както и от изключително динамичното движение на заплахите за сигурността и технологиите. Следователно се очаква системите за управление на СУСИ да се променят гъвкаво и адаптивно с течение на времето. Платформата, както и международните стандарти обхващат всички видове организации (търговски предприятия, държавни агенции, организации с нестопанска цел и т.н.). [38]

Целите на изследването са да се идентифицира ефективен набор от характеристики, атрибути и функции за моделиране на оптимална и ефективна технология за управление на информационната сигурност.

2.1 Методология

Методологията за изследване и моделиране на автоматизирана стандартизирана платформа за управление на сигурността на информацията включва следните ключови стъпки: [4]

- **Анализ на процесите**

Необходимо е да се изследват и анализират стандартизираните работни процеси, които системата да автоматизира и кореспондиращите с тях информационните потоци.

- **Определяне на изискванията**

За определяне на функционалните и нефункционалните изисквания е необходимо да се извърши:

  - Изследване и анализ на потребителските групи;
  - Изследване и анализ на стандартите за информационна сигурност;
  - Изследване и анализ на данните.

Изследването и анализа на данните се извършва в аспекти източници, ползватели структура и атрибути.

- **Определяне на общите характеристики на платформата**

Изследване и анализ на добрите практики за потребителско поведение, продуктивност, сигурност и администрация на информационните системи.

Прилагането на тази методология осигурява създаването на модел с устойчива и ефективна архитектура, която може да се мащабира и адаптира към променящите се бизнес нужди и технологични изисквания. [31]

2.1.1 Методология за анализ на процесите и моделиране

Реализацията на софтуерни платформи с нарастваща сложност изисква прилагането на общи стандарти и ефективни методологии за проектиране и разработка. От появата си през 1997 г. до сега Унифицираният език за моделиране – UML™ – се превърна фактически в стандартен „графичен език за визуализиране, специфициране, конструиране и документиране на елементите на една софтуерно-интензивна система“.

Сред предимствата на UML подход са:

- Плавен преход между отделните етапи при моделирането на платформата – от формулирането на изискванията до крайната реализация, чрез използване на междинни модели за анализ и проектиране на архитектурата и поведението на системата, които позволяват всяко изискване да бъде адресирано на подходящото ниво на абстракция;
- Възможност за ефикасно разширяване на съществуващи модели с цел включване на допълнителни функционални изисквания в една бързо променяща се работна среда – проектът може да расте запазвайки ефективна и ясна архитектура;
- Стандартен графичен език за изразяване и дискусия на идеи, изисквания и проектантски решения, който улеснява комуникацията;
- Един UML-базиран процес за разработка позволява да се настрои количеството и качеството на проектната документация според изискванията на конкретния проект (време, обем, бюджет, нужда от бъдещо разширяване).

UML моделирането е основно средство в процеса на анализа и проектирането на платформата. С негова помощ се постигнат няколко основни цели:

- формално описание на системата и нейните компоненти (подсистеми);
- описание на начина на внедряване, на работата и на функционалността;
- провеждане на експерименти с модела (симулация) и база за взимане на решения за оптимизиране на системата.

Business Process Model and Notation (BPMN) е другият стандарт, който се използва за визуално моделиране на бизнес процеси под формата на диаграма – Business Process Diagram (BPD). BPMN надгражда Unified Modeling Language (UML), като целта е да се разшири техническата насоченост на описанието в UML, създавайки универсален език за описание на бизнес процеси, който е еднакво четим и удобен за бизнес потребителите (мениджъри, бизнес анализатори и др.) и в същото време да дава възможност за описание на сложна семантика на бизнес процесите.

Поради спецификата на платформата и широкия набор от функционалности, която трябва да реализира, използването на неформалния метод би довело до създаване на описания с твърде голям обем, чието систематично интерпретиране би било сериозно затруднение. Подобна сложна система е много по-подходяща за описание чрез диаграми и модели на данните, отколкото с текстово описание на изискванията. По тази причина най-подходящият подход към дейността е използването на полуформален подход, чрез комбинирането на документ със спецификация на изискванията, с модел от UML диаграми, представящи систематично изискванията към архитектурата на системата и отделните потребителски случаи (use cases).

2.1.2 Методология за определение на изискванията - спецификация на потребителските случаи

Потребителските случаи (use case) се смятат за стандартна нотация при изготвянето на изискванията в обектно-ориентирано моделиране. Потребителските случаи на употреба осигуряват комуникацията между заинтересованите страни. Разглеждат се три различни нива на абстракция на изискванията (бизнес, потребителски и системни) и това как потребителските случаи могат да бъдат определящ фактор при разработването на детайлните изисквания за проектиране на платформата.

Изискванията към платформата, определят нейното функционално поведение, както и типовете информация, до която трябва да се осигури достъп, как тя се трансформира и организира. Определянето на изискванията дават възможност да се уточни ясно целта, насоката и да се изяснят очакванията от информационните цели. Целта е те да се трансформират в детайлни, пълни и подлежащи на тестване модели, на базата на които да бъде моделирана система, максимално отговаряща на нуждите.

- **Бизнес изисквания**

Бизнес изискванията представят цели на високо равнище, които следва да се реализират чрез внедряването на системата. Те идентифицират първичните ползи, които системата ще донесе на потребителите. Бизнес изискванията представляват най-високото ниво абстракция във веригата на изискванията. Те описват целите, възможностите и основните потребителски типове, които дават обобщена представа, за това как би следвало да функционира системата.

- **Потребителски изисквания**

Потребителските изисквания описват задачите и действията, които даден потребител трябва да може да извършва с помощта на платформата. Тези изисквания се уточняват с потребителските групи, които на практика използват системата. Съобразно тези потребители се описват не само задачите, които е нужно да се извършват в системата, но и нефункционалните ѝ характеристики, които са важни за доброто приемане и лесната работа със системата. Потребителските изисквания следва да са в синхрон с бизнес изискванията. Те могат да бъдат уточнени най-пълноценно посредством описанието на потребителските сценарии. Фокусират се върху конкретните нужди при използване на системата и съответно са доста по-значими от традиционният подход за извличане на изисквания посредством директно питане на потребителите какво биха искали да прави системата.

- **Детайлни системни изисквания**

Те представляват системните изисквания на много детайлно ниво, което подпомага пълното, детайлно специфициране на изискванията, позволяващо използването им при изграждане на компонентите от разработчиците. Системните изисквания съответстват на потребителските и бизнес изисквания и съдържат точни и ясни критерии, които са основа за верификация.

2.1.3 Методология за определяне на общите характеристики на платформата

Поради спецификата на поставените цели и изучаваната материя се използват евристични техники: [32]

- Подход най-добри практики;
- Проучване и анализ на академични източници;
- Техника SCAMPER;
- Метод Делфи - постигане на добре обмислено решение - чрез съгласие между експертите.

При подхода най-добрите практики се идентифицират общи характеристики на софтуерна платформа в редица ключови аспекти, като: гъвкава архитектура; потребителско преживяване (UX/UI); производителност и мащабируемост; автоматизация и др.

SCAMPER е техниката за креативно мислене, която помага за генериране на нови идеи, решаване на проблеми и подобряване на продукти, процеси или услуги. Тя

се основава на седем стратегии за творческо разсъждение, които могат да бъдат приложени към всяка концепция. SCAMPER е акроним, в който всяка буква представлява различен подход за иновация:

- S (Substitute) – Заместване.
- C (Combine) – Комбиниране.
- A (Adapt) – Адаптиране.
- M (Modify/Magnify) - Промяна или уголемяване.
- P (Put to Another Use) – Прилагане за друга употреба.
- E (Eliminate) – Премахване или намаляване.
- R (Reverse/Rearrange) – Обратен ред или пренареждане.

Методът Делфи (Delphi Method) е структуриран процес за събиране и синтезиране на мненията на експерти, използван за прогнозиране, вземане на решения и намиране на оптимални решения в иновативни ситуации. Той се използва широко в бизнеса, науката и управлението за събиране на обективни експертни мнения и предвиждане на бъдещи тенденции.

2.2 Анализ на процесите

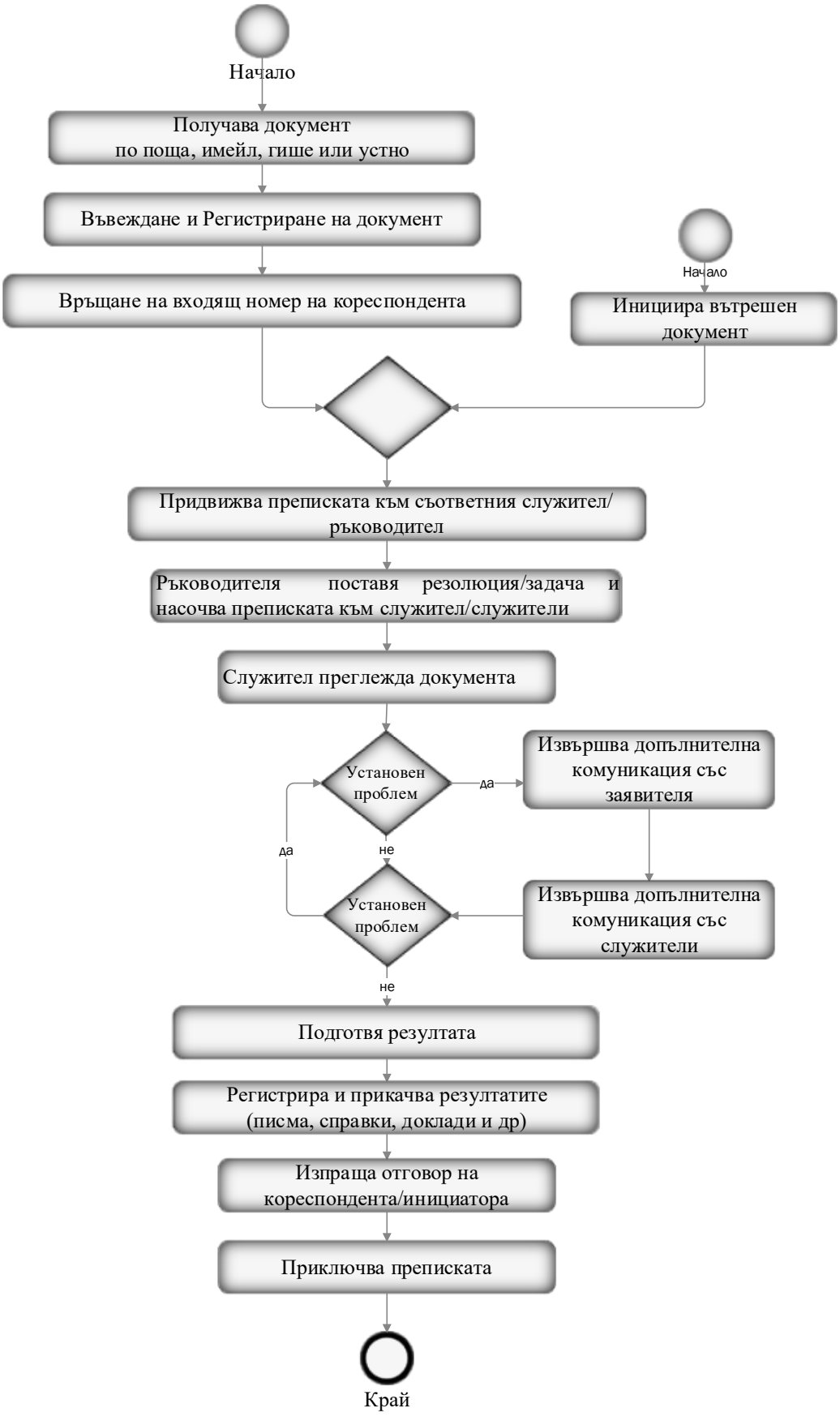
Платформата обхваща всички информационни единици - документи (хартиени и електронни), аудио и видео комуникации, системни, програмни и комуникационни логове. Нейната основна цел е да мониторира входящите, изходящите и вътрешните информационни потоци и да ги управлява, съобразно моделираните в нея работни процеси и стандартизирани форми. За това е необходимо да се изследват и анализират **стандартизираните работни процеси**, в обхвата на платформата и кореспондиращите с тях информационните потоци.

2.2.1 Изпълнение на бизнес процеси ИБП/Документооборот

Документооборота обхваща регистрацията и движението на информационните единици от съставянето им до предаването им в архива или унищожаването им. Той е съвкупност от взаимно пресичащи се маршрути на документите в документираните процедури по международните стандарти. Документирането на процедурите по международните стандарти се извършва чрез деловодната функционалност на Платформата.

Документооборотът се изпълнява текущо при официалното съставяне на документите, като се осигурява коректното спазване на всички стъпки от работните процеси: съответно коректното попълване на кореспондиращата документация; мониторинг на работните процеси и контрол по решенията; установяване на несъответствия, корекция, коригиращи и превантивни действия; преглед от ръководството; външен одит на системата за управление с цел верифициране на съответствието ѝ със стандарта.

Чрез документооборота се моделират всички бизнес процеси и се регистрират параметрите в различните етапи и елементи на тяхното изпълнение.



Фигура 3 Процес Документооборот

Ръководителят на организацията утвърждава политиката за управление в съответната област и плана за приложението ѝ с посочени отговорници за всяка дейност, а така също и изискванията на Платформата към служителите в организацията, свързани с документирането на процедурите по съответните международни стандарти.

Към всеки регистриран документ се задават срокове за изпълнение, които платформата контролира и за които информира по различни начини (e-mail, SMS, звуково и визуално) за различни контролирани събития, аспекти и рискове, просрочени срокове и задачи за изпълнение, съгласно изискванията на документираните процедури по съответните международни стандарти.

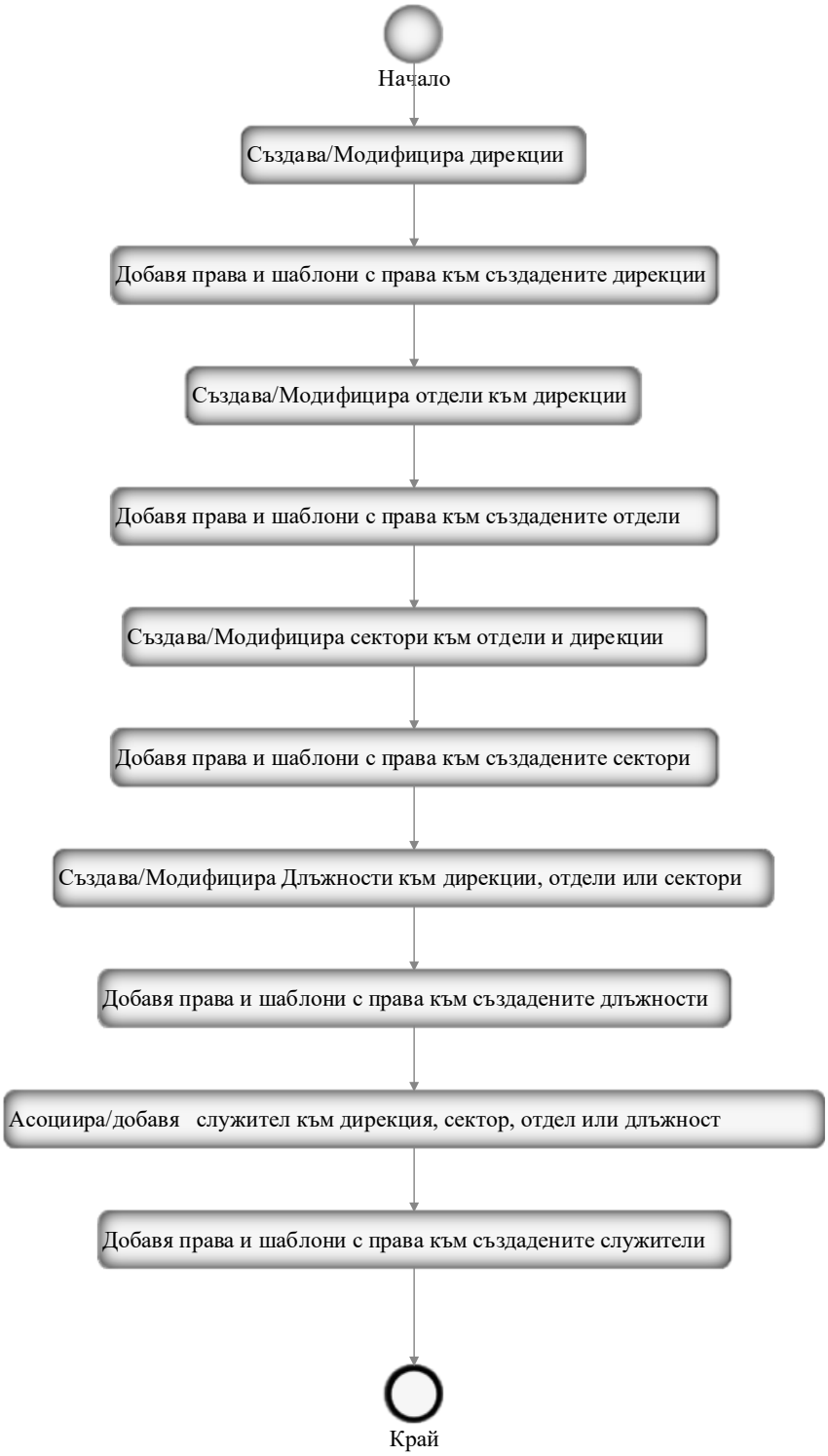
2.2.2 Процеси по администрация на платформата

Платформата е необходимо да предоставя интерфейси за изграждане на конкретното клиентско решение, съобразно внедрената в клиентската организация СУСИ. Обучен потребител, със съответстващи права на достъп за конструктор, чрез екраните на модула въвежда параметри на индивидуалната инсталация както следва:

- Регистрационни индекси;
- Общи данни, административни данни;
- Документообороти Маршрути - (точки, възли и права на достъп) в зависимост от организационната йерархия, международно признатите стандарти въведени в клиентската организация и оперативните процедури в тях;
- Модел на организационната йерархия;
- Специализирани изгледи в зависимост от международно признатите стандарти въведени в клиентската организация;
- Форми, бланки, регистри, формуляри, изискуеми от международно признатите стандарти въведени в клиентската организация за оперативното им управление.

Административният модул изгражда индивидуалното решение за всяка клиентска организация, отговарящо точно на нейните нуждите и въведените в нея стандарти чрез съществуващи, предварително дефинирани форми, регистри, процеси, блокове и набори от средства. При администрацията на платформата упълномощен служител или администратор конфигурира Организационната структура, потребителите и потребителските права и роли.

Работните процеси се развиват между служителите на организацията, които се дефинират, чрез организационната структура. Тя е скелета, определящ параметризацията на платформата. Организационната структура е основен елемент от системата за управление на сигурността на информацията.



Фигура 4 Създаване и управление на организационна структура

Организационната структура е начинът, по който една организация разпределя своите ресурси, задачи, отговорности и взаимоотношения между служителите и отделите. Тя осигурява яснота относно йерархията, комуникационните канали и процесите в организацията.

Правата на достъп и ролите на потребителите се определят от мястото им в организационната структура. Към всеки потребител могат да се добавят и допълнителни права свързани с конкретна функционалност на Платформата.

Фигура 5 Процес Регистрация на потребител

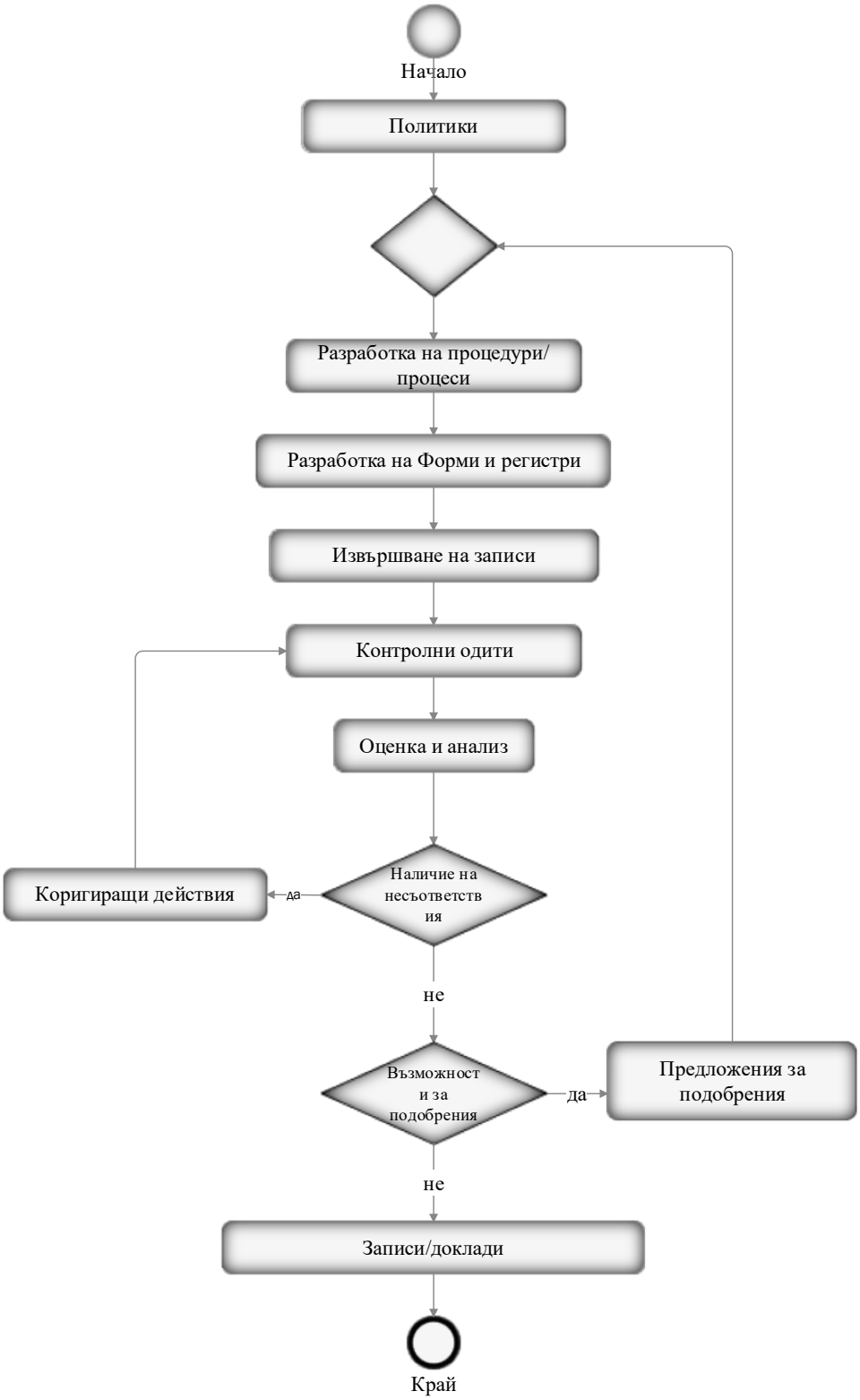
2.2.3 Дефиниране и управление на бизнес процеси

Процеса реализира дефинирането и изпълнението на сложни автоматизирани работни процеси с множество стъпки (етапи на обработка) и различни типове задачи и срокове за изпълнение от различни участници в организационната структура. Определя се и проследяването и управлението на отделните инстанции на процеса, включително изчисляване на база на данни от документа на маршрута, по който документа да бъде насочван при изпълнението на процеса, потребителите които следва да го обработват на различните стъпки, както и условия при което задачите в дадена стъпка могат да се считат за приключени, за да се премине към следваща стъпка от обработката.

Работните процеси и стандартизирани форми се моделират в платформата, съобразно политиките, процедурите и шаблоните на СУСИ. Всички записи, свързани с елементите на СУСИ се формализират във платформата и се извършват само чрез нея.

Фигура 6 Процес по създаване и промяна на дефиниция на автоматизиран процес

2.2.4 Управление на СУСИ



Фигура 7 Управление на СУСИ - генеричен процес

Управлението на системите за управление на информационната сигурност по международно признати стандарти се базират на дефинирането на ефективни политики за сигурност и съответстващите процеси и процедури, които осигуряват техното изпълнение. Управленския анализ и оценка се извършват върху данните генерирани от записите, извършвани в съответните регистри и форми, които са интегрални части от процедурите и СУСИ. Записите се извършват текущо в документната матрица на организацията при изпълнение на работните процеси и се обследват при контролните одити на СУСИ. В зависимост от резултатите от оценката и анализите се предприемат коригиращи действия при необходимост и се дефинират предложения за подобрения на СУСИ като цяло.

Управлението на СУСИ е генеричен процес, който обхваща дефинирането, развитието и подобрението на системата като цяло.

2.2.5 Мониторинг и контрол

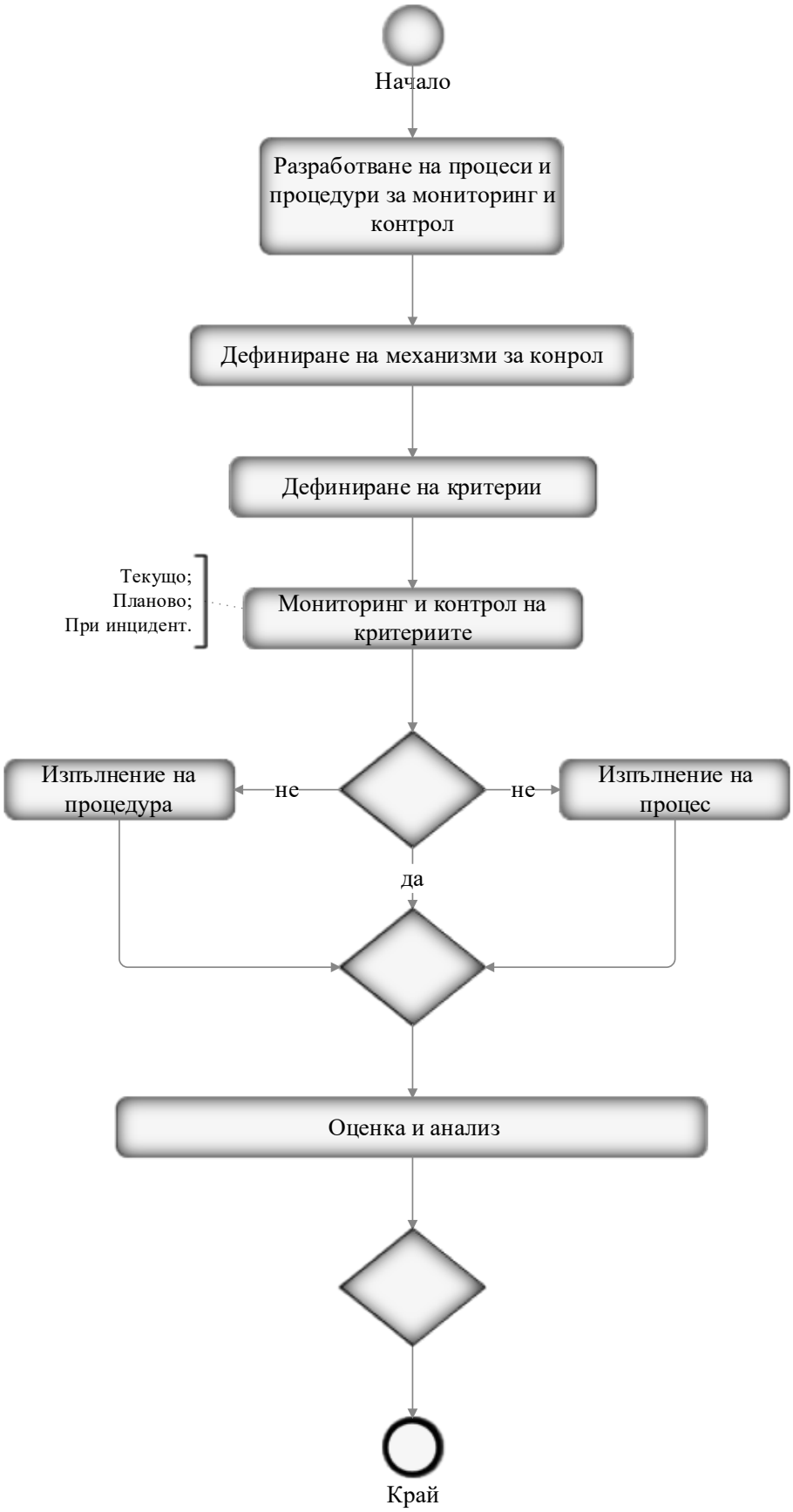
Мониторинга и контрола на СУСИ се извършва по три направления върху нейните елементи:

- Текущо;
- Планово (планирани одити);
- При инцидент.

Общия процес обхваща всички информационни единици - документи (хартиени и електронни), аудио и видео комуникации, системни, програмни и комуникационни логове. [30]

Всеки механизъм за контрол от системата от контроли на стандартите, съобразно които е изградена СУСИ се асоциират с един или няколко предварително дефинирани критерия. Критерия е формализиран запис с определени параметри на регистрираната информация, за който е определен честота и начин на проверка.

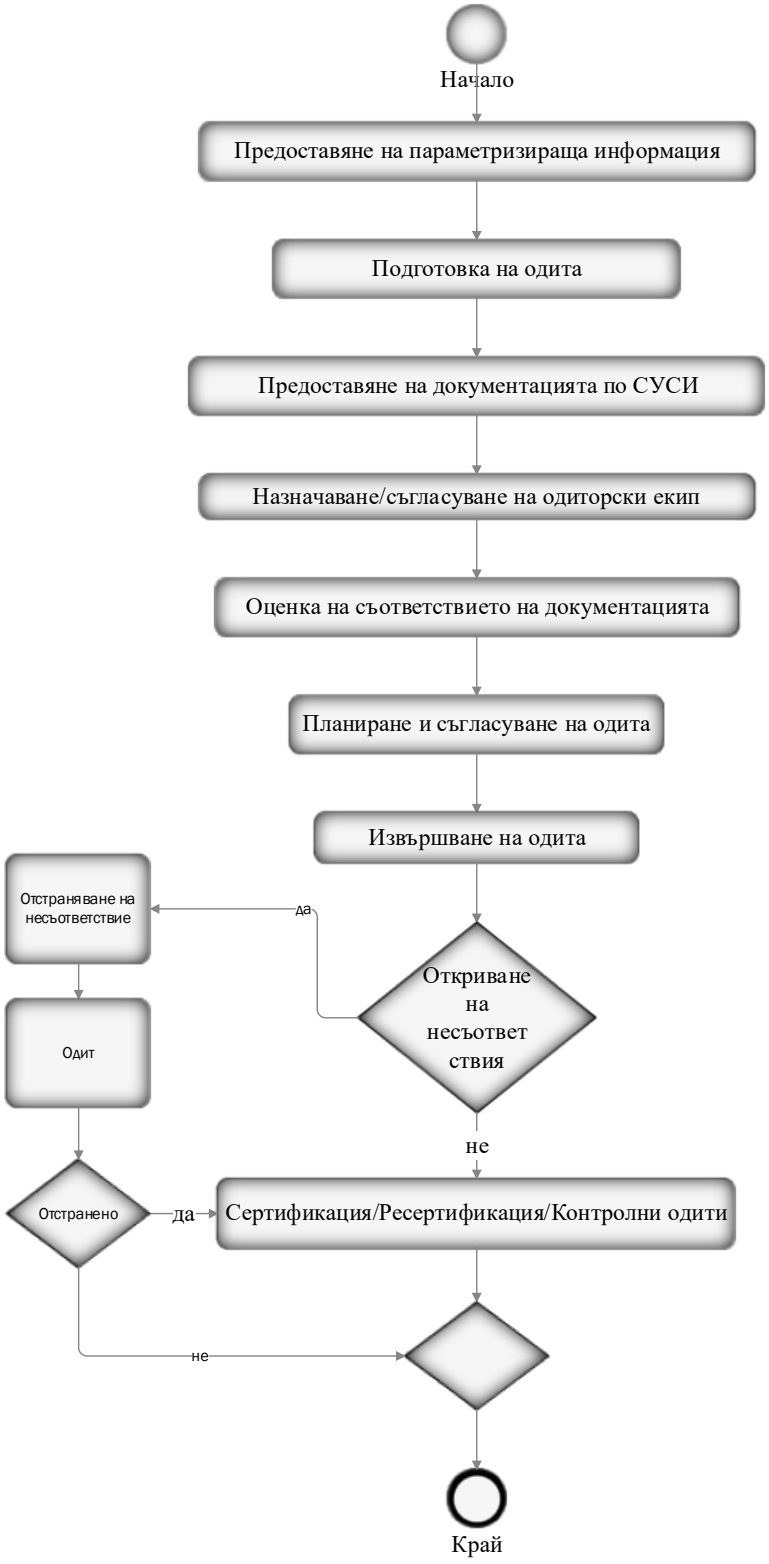
В зависимост от резултата при контрола на критерия се дефинират тригери на възможни действия, формализирани в процеси и процедури или се отчита неговото изпълнение. Процеса се повтаря циклично в зависимост от слоя в който се изпълнява. [30]



Фигура 8 Мониторинг и контрол

2.2.6 Одит

Одитния процес при СУСИ се изпълнява при сертификация и ре сертификация на системата, контролни и вътрешни одити.



Фигура 9 Одитен процес

2.2.6.1 Начало

За да стартира процесът по сертификация е необходимо организацията да предостави на сертифициращата организация детайлна информация относно: предмет на дейност; брой на работните площадки; брой на служителите; стандарт, спрямо който ще се сертифицира системата за управление.

Тази информация се предоставя чрез попълването на специализиран формуляр - **данни за сертификация**. Въз основа на детайлите за организацията, сертифициращата организация определя продължителността на всеки одит, както и необходимата квалификация и компетентност на одиторския екип, който ще участва в него.

2.2.6.2 Подготовка за извършване на одит

Ако има съмнения/притеснения относно готовността на системата за управление, може да бъде извършен **предварителен одит,** преди започването на сертификационния процес, за да бъде уточнена готовността на организацията за сертификация. Тези одити не са задължителни за сертификацията.

Сертификационният процес започва с предоставянето на сертифициращата организация на документацията на СУСИ на клиента. Предоставената документация трябва да бъде в такъв обем и обхват, че да позволи да бъде направена реална оценка на съответствието на документираната СУСИ с изискванията на правилата и съответния стандарт/и, по които е разработена. На този етап от процеса сертифициращата организация назначава одитор/одиторски екип с подходяща квалификация, които да извършат одита.

Водещият одитор или друг член на одиторския екип оценява съответствието на документацията на клиента с изискванията на правилата и стандарта и изготвя доклад от прегледа на документите. Прегледът на документите на системата за управление на клиента може да се извърши и на площадката на клиента по време на Етап 1 на сертификационния одит.

На базата на документираната СУСИ водещият одитор подготвя план за извършването на одита на площадката на клиента.

2.2.6.3 Извършване на одит на площадката на клиента

Одиторът/одиторският екип извършват одита на площадката съгласно одобрения план за одита. Сертификационните одити се извършват на 2 етапа. Целта на Етап 1 на одита е да се оцени общата готовност за сертификация. Този одит се провежда на площадката на клиента. Планът за Етап 2 на сертификационния одит се изготвя след провеждането на Етап 1 на базата на получените резултати от одита. По време на одита одиторският екип прави проверка на изпълнението на всички изисквания на правилата и стандарта, с цел да оценят системата за управление на качеството. Одиторите записват всички наблюдения. Ако по време на одита се установят отклонения от изискванията на правилата и стандарта, клиентът се информира за това и се съгласуват последващи действия.

В случай, че се установят значими недостатъци на системата за управление, се взема решение за последващите действия (прекратяване на одита, извършване на последващо посещение), което се съгласува с органа по сертификация. При нормално протичане на одита водещият одитор представя наблюденията от одита по време на закриващата среща. Одиторският екип обобщава наблюденията си и документира препоръката си в писмен доклад, който се предоставя на органа по сертификация и клиента.

2.2.6.4 Сертификация

След извършването на одита, на базата на предоставения доклад от водещия одитор, както и всички други записи, изискващи се за одита, схемният мениджър взема решение за сертификация. Всички решения за сертификация са обект на контрол от страна на Надзорния съвет на органа по сертификация. При положително решение, след заплащане на дължимата по договора сума за извършване на сертификационния одит, клиентът получава сертификат, който покрива одитирания обхват на дейността му.

Този сертификат е валиден за три години, освен ако този период не е ограничен по изискване на клиента или промени в правилата или стандартите. Ако не може да бъде взето положително решение за сертификация, органът по сертификация уведомява писмено клиента за мотивите за отрицателното решение. Ако не бъде постигнато съгласие, се използва арбитър съгласно правилата за сертификация.

2.2.6.5 Поддържане на валидността на сертификата

За поддържането на **валидността на сертификата**, по време на 3-годишния период на сертификация, сертифициращата организация провежда два ***контролни одита*** – по един годишно. Целта на тези одити е да се установи дали се спазват изискванията за сертификация, дали може да бъде доказана ефективността на СУСИ и дали има доказателства за непрекъснато подобряване. При положително становище на одиторския екип, в резултат от наблюденията от одита, схемният мениджър взема решение за продължаване на валидността на сертификата.

Ако по време на одита са констатирани несъответствия, трябва да бъдат съгласувани адекватни коригиращи действия, които да се изпълнят от клиента. В случай на значими недостатъци в системата за управление (искания за коригиращи действия от първа категория) органът по сертификация изисква извършването на последващо посещение за проверка на място на изпълнените коригиращи действия, което се заплаща от клиента.

Всички последващи одити се планират спрямо датата на последния ден на сертификационния одит. Всички контролни и ре сертификационни одити трябва да бъдат извършени в рамките на тримесечен период преди горната дата на съответната година.

2.3 Определение на изискванията

Съгласно описаната методология, за определяне на функционалните и нефункционалните изисквания е извършено:

- Изследване и анализ на потребителските групи;
- Изследване и анализ на стандартите за информационна сигурност;
- Изследване и анализ на данните.

Изискванията се представят с UML диаграми на случаите на употреба (Use Case Diagram).

2.3.1 Изследване и анализ на потребителските групи

Потребителите на платформа за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията може да обособим в следните големи групи:

- **Ползватели**

Компании и организации внедрили Система за управление на информационната сигурност, сертифицирана по международно признат стандарт.

Това са ползватели от всички сектори на икономиката, изпълняващи дейност във всички раздели на класификатора на икономическите дейности, включително държавни и общински организации.

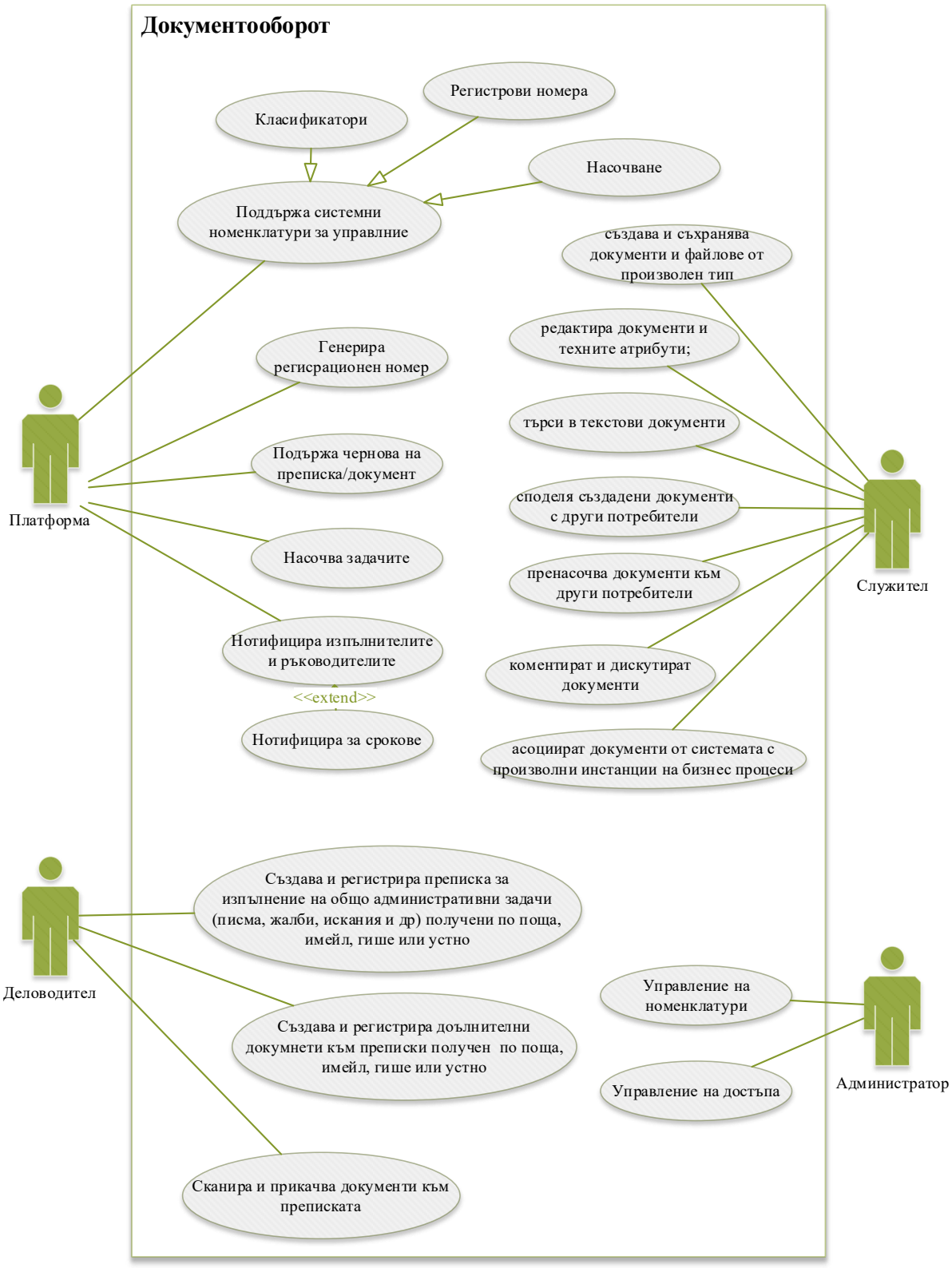
- **Сертификационни организации;**

Основен бизнес партньор в средата на автоматизация и управление на международно признати стандарти са сертифициращите организации. Те извършват одити при сертифицирането на СУСИ и контролни одити за потвърждаване на съответствието. Функционалните нужди на одиторските организации, свързани с информационното осигуряване и електронното взаимодействие с организациите въвели СУСИ са обособени пряко от процеса по сертификация и неговата същност.

2.3.1.1 Потребителски изисквания на ползвателите

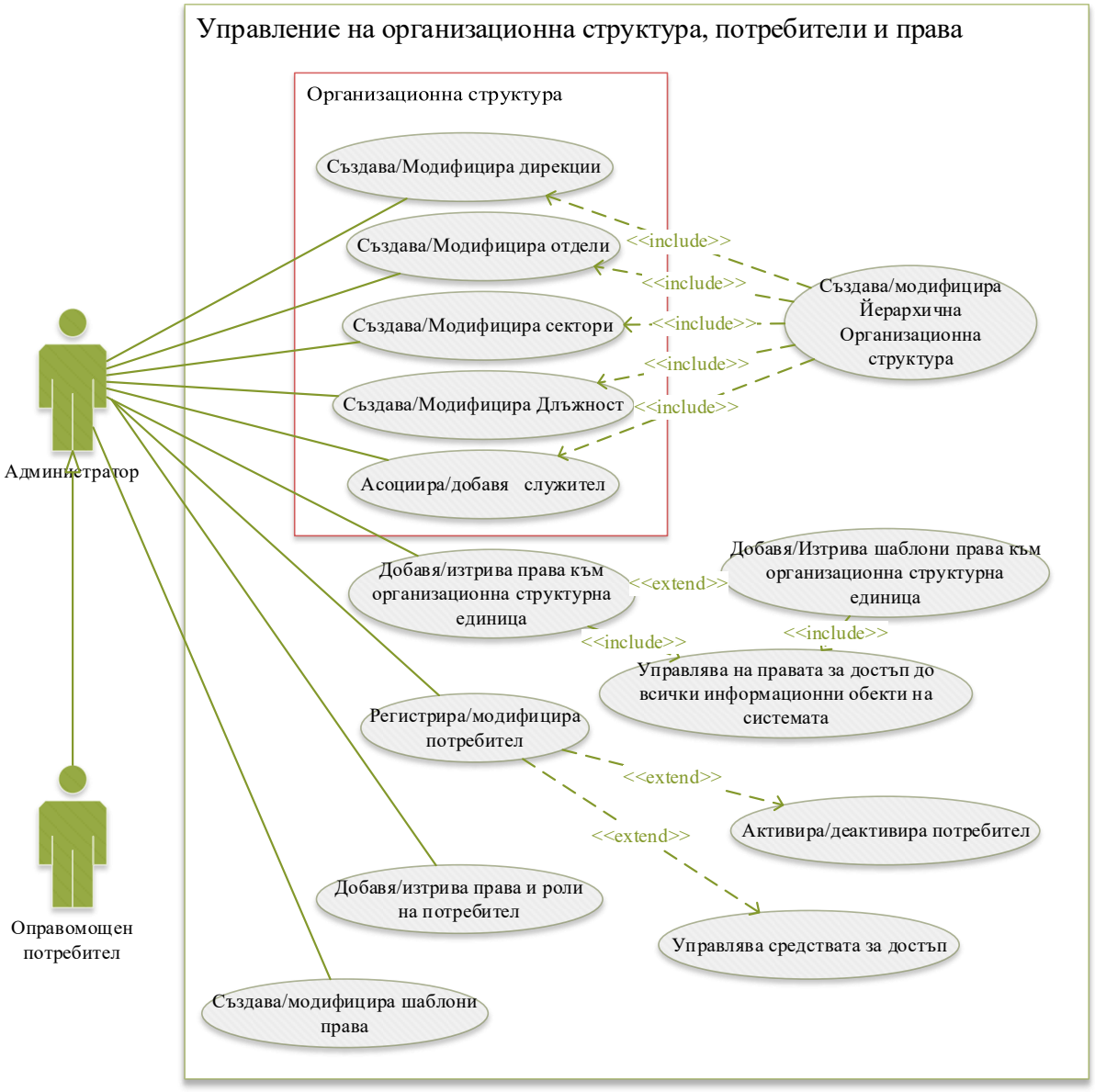
Изискванията на тази потребителска група се определят от оперативните процеси описани в т. 2.2 и от изискванията на международно признатите стандарти, които ще бъдат представени в т. 2.3.2.

2.3.1.1.1 Изисквания Документооборот

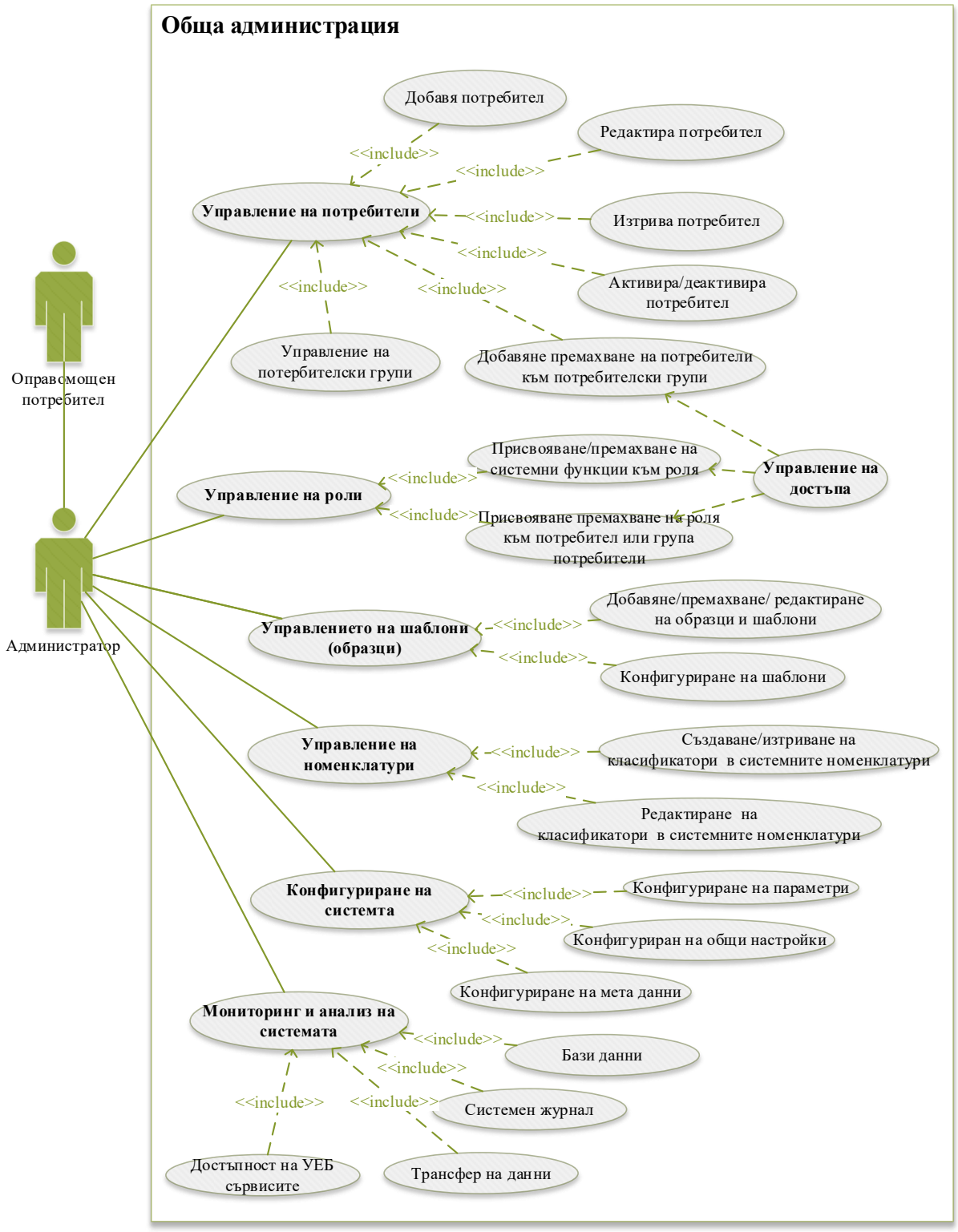


Фигура 10 Документооборот диаграма на потребителските случаи

2.3.1.1.2 Изисквания - Администрация



Фигура 11 Администрация - диаграма на потребителските случаи



Фигура 12 Обща администрация

2.3.1.1.3 Изисквания - Дефиниране и управление на бизнес процеси

Фигура 13 Дефиниране и управление на бизнес процеси диаграма на потребителските случаи.

2.3.1.1.4 Изисквания за актуалност и промяна на документите и управление на записите

Управлението на актуалността и промяната на документи и управлението на записите по международно признати стандарти са свързани с аспектите и практиките по тази тематика описани в **Приложение 4.**

2.3.1.2 Потребителски изисквания на Сертификационни (одитиращи) организации

Интернационалния Регистър на сертифицираните одитори (IRCA) е най-големият международен орган за сертификация в света за одитори на системи за управление.

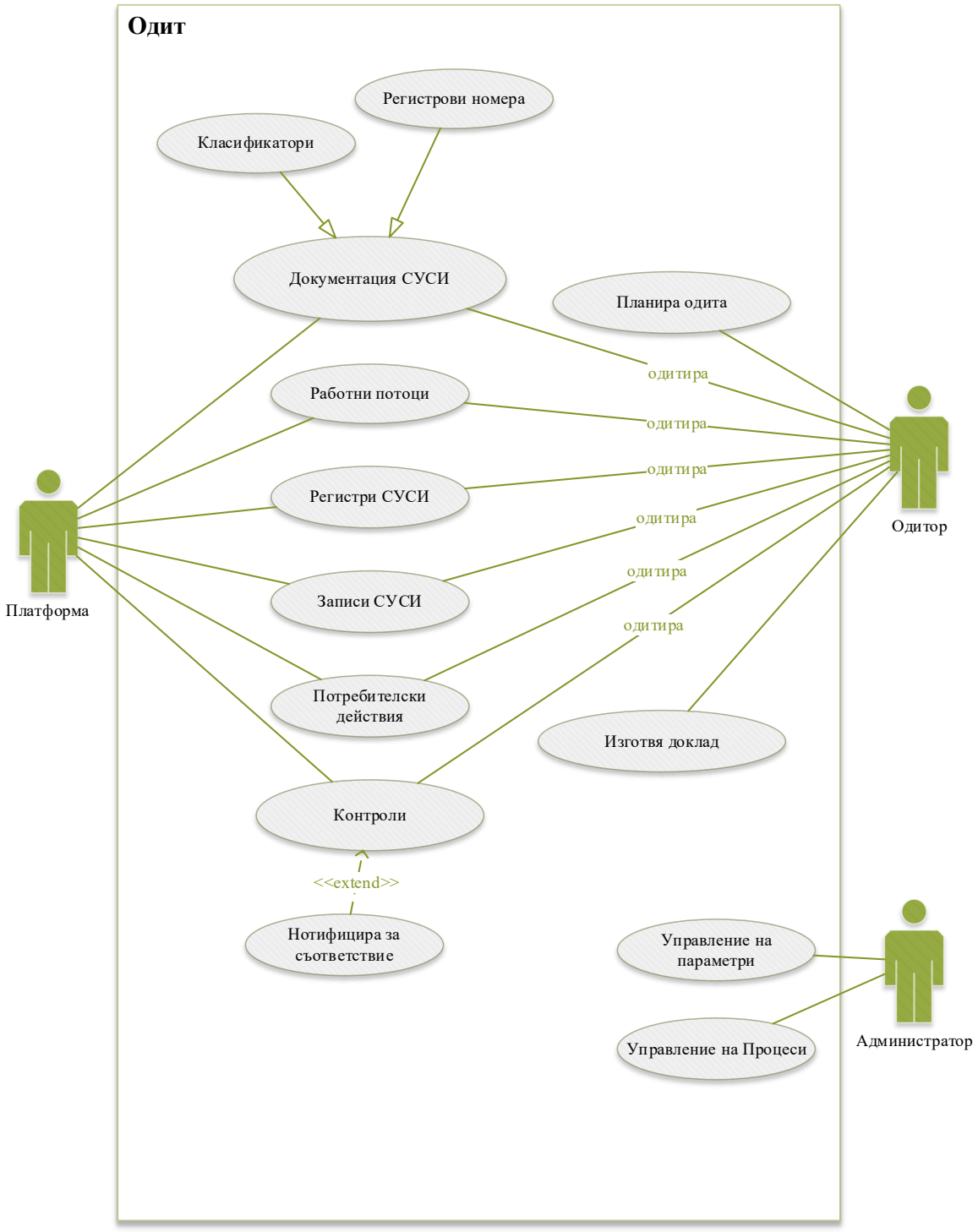
IRCA осигурява две основни услуги:

1. Сертифициране на одитори на системи за управление;
2. Одобрения на организации за обучение и сертифициране на техните курсове за одитори обучение.

Сертифициращите компании с различен обхват са представени в Приложение 2.

Платформа за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията с функционалност, покриваща специфичните изисквания на системите за управление по международно признатите стандарти подпомага одиторските организации при извършване на сертификационни и контролни одити.

Функционалните нужди на одиторските организации, свързани с информационното осигуряване и електронното взаимодействие с организациите въвели международно признати стандарти се генерират от одиторския процес.



Фигура 14 Одитиране - диаграма на потребителските случаи

2.3.1.3 ***Общи изисквания на потребителските групи***

Платформата за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията трябва да моделира създадените в компанията по международните стандарти оперативни процедури и процесни карти, като осигурява информационно коректното спазване на всички стъпки от работните

процеси, съответно коректното попълване на кореспондиращата документация, мониторинга на оперативната дейност и контрола по решенията.

Платформата трябва да поддържа в електронен вариант всички образци на документи, които се използват в компанията – молби, заповеди, договори, протоколи, отчети, документи по качеството и др.

Системата трябва да автоматизира процедурите за реализация на цялостния процес, посредством предварително дефинирани електронни маршрути за всички типове документи и обекти. Маршрутите трябва да бъдат дефинирани, следвайки съподчинеността на оптималните организационни структури и екипа. Документите автоматично преминават през различни участници в процеса, гарантирайки единни обективни стандарти и правила, които отговарят на различните типове дейност. По този начин се реализира комуникация между различните участници в процеса и се гарантира качествения порядък на изпълнение.

Платформата трябва да осигури проследяване и контрол на действията по задачите при условията на времеви ограничения и процеси, като доставя на отдели и крайни потребители детайлна информация относно текущия статус на всяка една от задачите, нейните стъпки, ангажираните лица и свързаните с това задължения.

Платформата трябва да събира и цифровизира неструктурираните данни от външната за дружеството среда и заедно с вътрешните информационни потоци да ги организира в стройна, структурирана информационна база.

Процеса на извличане на данни от структурна база и публикуването им в различни отчети, справки и форми за анализи, контрол и информираност е в основата на изходната функционалност, необходими на одиторските организации за сертификационни и контролни одити. Необходимо е да има средства за пълнотекстово търсене на всички обекти намиращи се в базата данни. Пълнотекстовото индексиране, позволяващо търсене на ключови думи или фрази и в прикрепени документи, които са създадени с офис приложения. Търсенето се извършва на различните езици и трябва да е независимо от операционната система и от файловата структура.

Като част от всеки документ в информационната система се включва под форма, визуализираща целия път на документа - кой кога е дал отношение по него, какъв е срокът за отговор на всяка стъпка, как е отговорила всяка инстанция. Необходимо е да се проследява кои лица следва да отговорят по този документ и в какъв срок. Всеки потребител със съответни права трябва да може да види тази информация или съответна част от нея. [5], [33], [34]

2.3.1.3.1 Изисквания на потребителя

Базирането на системите върху клиент-сървър платформа инсталирана на централен сървър с функционалност за поддръжка на мобилни потребители дава възможност за широк достъп до информация, независимо от комуникационните алтернативи. От гледна точка на потребителя на системата съществена нейна характеристика е нейната **готовност (availability)**, което характеризира достъп по всяко време, от всички възможни точки, при всякакво натоварване. Гарантиране на

обслужването се характеризира с **отказоустойчивост,** който критерии е важен за функционалността на система за синхронно изследване и анализ на фокус група**.** [35]

Потребителят поставя и други изисквания към системата. Тя трябва да бъде **информативна**, да му носи необходимата информация, за да реализира безгрешно услугата.

От гледна точка на потребителите, като извършващи анализи от различно естество, платформата трябва да осигурява: разширяемост, лекота на надграждането и обновяването, връзка със съществуващите системи, сигурност на функционалността и конфиденциалност на потребителските данни.

Съществен и особено важен критерии за оценка на информационното съдържание при интегриране на множество самостоятелно създавани модули е **информационното единство**. Това означава единство в описанието на информационните масиви, както по форма, така и по съдържание.

Изискванията при проектирането на платформата за администрация, автоматизация и управление на системи за управление на сигурността на информацията са свързани с основните цели, които трябва да се постигнат при нейното реализиране:

- Да задоволят нуждите на потребителя – за администрация, автоматизация и управление на системи за управление на сигурността на информацията;
- Да са максимално удобни за обслужване;
- Да осигурят оптимална организационна структура за комуникация в реално време и управление на съдържанието.

При изследването на платформата трябва да се вземат в предвид следните основни акценти:

Осигуряване на интуитивен диалог с потребителя

Степента на ***интуитивност*** се определя от еднозначното и ясно структуриране на диалога потребител-система.

Навигация

Навигацията се изразява в безпроблемното търсене в съдържанието и използване на функционалността чрез менюта и други навигационни елементи.

Дизайн

Трябва да се използва единен дизайн, с балансирано съотношението текст – дизайн елементи и добро качество на графичните елементи.

Бързина

Приемливо бърз достъп до търсената информацията и функционалност.

Съдържание

Достъпна очакваната информация и функционалност. [36] [37]

2.3.1.3.2 Изисквания, свързани с организацията на информационната система

Ядрото на концепцията за предоставяне на електронна информация и функционалност, отнасяща се до платформената суперструктура и инфраструктура се състои от:

- Оптимална организационна структура и алгоритми за гъвкаво управление на информацията;
- Отговорности към съдържанието на информацията и функционалност в системата между различните потребители;
- Обезпечаване на качество и контрол.

Възможност за непрекъснати подобрения

Непрекъснатото усъвършенстване е постоянна цел. Важността на този принцип е значителен поради динамиката на областта и на решенията на информационните технологии, комуникациите и техническите възможности. Непрекъснатите подобрения на системата трябва да следват и даже да изпреварват световните най-добри практики.

Процесен подход

Желаният резултат се постига по-ефикасно, когато свързаните източници и дейности са управлявани като един процес. Вътрешните връзки между различните нива и типове мениджъри и редактори на съдържание се разглеждат като процес в съответните краткосрочни и *дългосрочни параметри и тенденции.*

Системен подход към управление

Определянето, разбирането и управляването на система от вътрешно-свързани процеси за дадена цел допринася за ефективността на организационната среда в платформата за администрация, автоматизация и управление на системи за управление на сигурността на информацията. [38]

2.3.1.3.3 Изисквания, свързани с обслужване на системата

Идентификация и дефиниция на правата на потребителя в платформата и последващото изготвяне на оптимална организационна структура за управление на съдържанието и функционалността е ключова предпоставка за осигуряване на качеството. Затова различните информационни класове трябва да бъдат идентифицирани и подходящо съобразени с потенциалните потребители на различни нива.

Осигуряване на хомогенна информационна среда

Сърцевината на системата за управление на сигурността на информацията трябва да бъдат предварително дефинирани модели за въвеждане на информацията в информационните раздели/класове на модулите за управление на информационното съдържание и функционалност. Те трябва да се използват за въвеждане/редактиране на информацията в системата и да следват стриктно всички дефинирани стандарти за информационните раздели/класове, за интеграция на обектите за синхронно

поведение при запис и т.н. Предварително дефинираните форми също трябва да са в съответствие с общите и технически изисквания на системата. Те описват точния начин на действие във всички работни процеси, които се отнасят до управление, верификация, въвеждане, администриране, мониторинг и контролиране на информация. Процедурите гарантират точност на информацията, стабилитет, издръжливост и съответственост на информационните потоци; единно действие на редакторите от различните стадии на процеса; подходящо контролиране и управление.[38]

2.3.2 Изследване и анализ на стандартите за информационна сигурност

Международно признати стандарти за сигурност на информацията се определят от следните основни групи характеристики: [39] [40]

- Съдържание на стандарта - име, цел, политики, обхват, изисквания, условия, определения, вид и област на приложимост.
- Инфраструктура - процедури, процеси, документи, контроли, регистри, срокове, инструменти и функционални алгоритми.
- Суперструктура (външна среда) - кореспонденти, клиенти, доставчици, партньори и институции, свързани стандарти, възможни възможности за интеграция, одити, и т.н.
- Ресурси - организационна структура и персонал, активи, инструменти и материали, необходими за планиране, поддържане и контрол на стандартните механизми.

„Сигурността на информацията се постига посредством внедряване на подходящ набор от механизми за контрол, в това число политики, правила, процеси, процедури, организационни структури и функции на софтуера и хардуера. За да изпълни тези специфични за сигурността и бизнеса си цели, организацията би трябвало да определя, прилага, наблюдава, преразглежда и подобрява тези механизми за контрол, където е необходимо. СУСИ както тази, специфицирана в стандартите, носи цялостен, координиран поглед върху рисковете за сигурността на информацията на организацията, за да определи и приложи обширен набор от механизми за контрол на сигурността на информацията в рамките на цялостната рамка на една съгласувана система за управление.“ [41]

2.3.2.1 Механизми за контрол

Механизмите за контрол, касаещи информационната сигурност се разпределят най-общо в четири категории:

- Организационни;
- Човешки ресурси;
- Физически;

- Технологични

Съгласно стандарта БДС ISO/IEC 27002:2022 всеки механизъм за контрол е свързан с пет атрибута както следва

1) Тип на механизма за контрол

- превантивен - механизъм за контрол, който е предназначен да предотврати възникването на инцидент, свързан със сигурността на информацията;
- откриващ - механизмът за контрол действащ при възникване на инцидент, свързан със сигурността на информацията;
- коригиращ - механизмът за контрол, действащ след като инцидентът, свързан със сигурността на информацията вече се е случил

2) Свойства за сигурност на информацията

Свойствата за сигурност на информацията са атрибут за визията на механизмите за контрол от гледна точка на това, на коя характеристика на информацията ще допринесе за запазването на този механизъм за контрол. Стойностите на атрибутите се състоят от:

- поверителност/конфиденциалност (confidentiality),
- цялостност/интегритет (integrity)
- и наличност (availability).

3) Концепции за киберсигурност

Концепциите за киберсигурност са атрибут за визията на механизмите за контрол от гледна точка на практикуващия по отношение им с концепциите за киберсигурност, определени в рамката за киберсигурността, описана в ISO/IEC TS 27110. Стойностите на атрибутите се състоят от:

- идентифициране (identify);
- защита (protect);
- откриване (detect);
- реагиране (respond);
- възстановяване (recover).

4) Оперативни възможности

Оперативните възможности са атрибут за визията на механизмите за контрол от гледна точка на практикуващия по отношение на възможностите за сигурност на информацията. Стойностите на атрибутите се състоят от:

- Ръководене (Governance);
- Управление на активи (Asset_management);
- Защита на информацията (Information_protection);
- Сигурност на човешките ресурси (Human_resource_security);
- Физическа сигурност (Physical_security);

- Сигурност на система и мрежа (System_and_network_security);
- Сигурност на приложенията (Application_security);
- Сигурна конфигурация (Secure_configuration);
- Управление на идентичността и достъпа (Identity_and_access_management);
- Управление на заплахи и уязвимости (Threat_and_vulnerability_management);
- Непрекъснатост (Continuity);
- Сигурност при взаимоотношения с доставчици (Supplier_relationships_security);
- Законност и съответствие (Legal_and_compliance);
- Управление на събития свързани със сигурността на информацията (Information_security_event_management);
- Осигуряване на сигурност на информацията (Information_security_assurance).

5) Домейни за сигурност

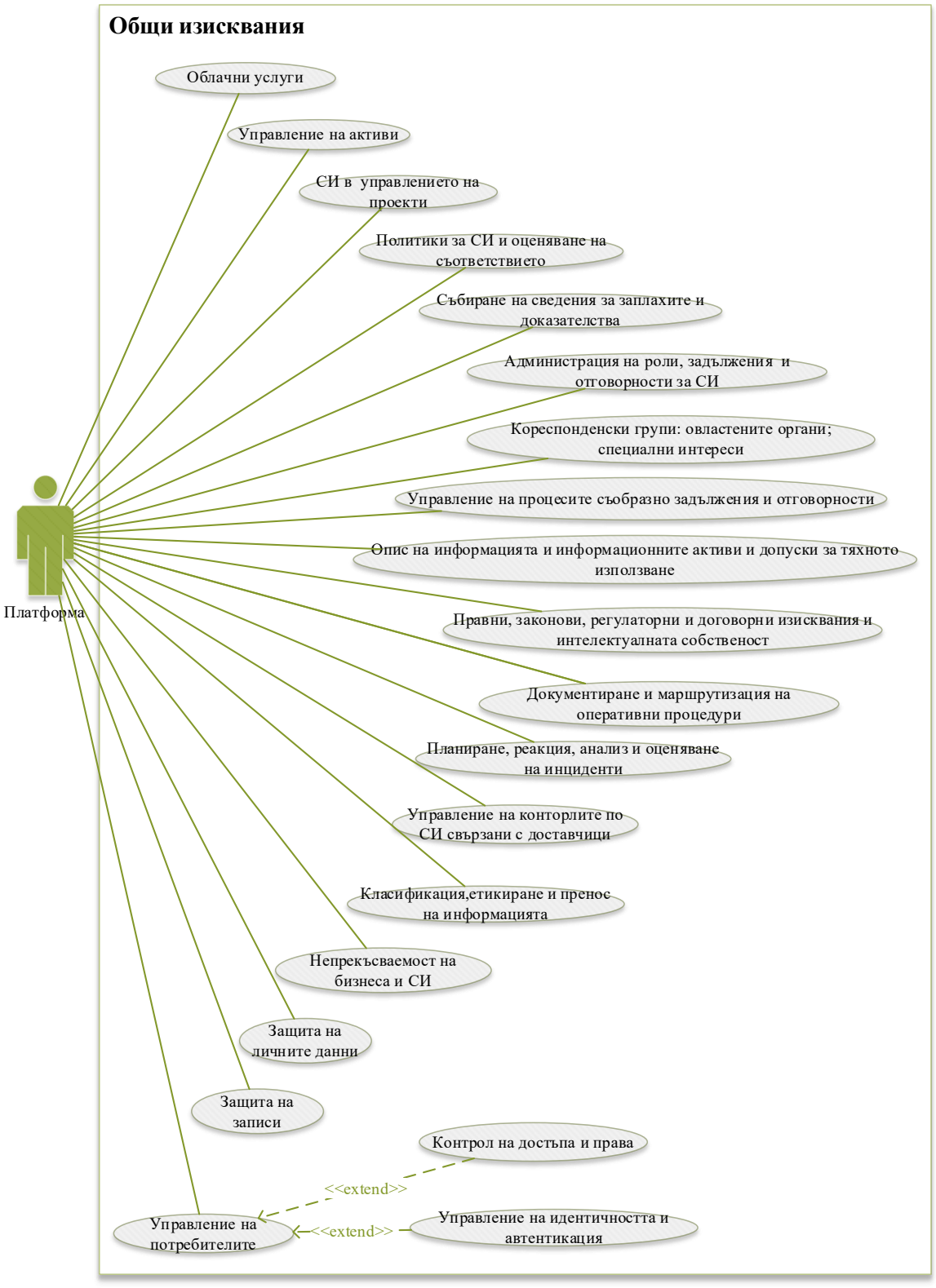
Домейните за сигурност са атрибут за визията на механизмите за контрол от гледна точка на четири домейна за сигурност на информацията. Стойностите на атрибутите се състоят от:

- Ръководене и екосистема (Governance and Ecosystem) включва:
    - ръководене на сигурността на информационната система и управление на риска (Information System Security Governance & Risk Management);
    - Управление на киберсигурността на екосистемата (Ecosystem cybersecurity management) (включително вътрешни и външни заинтересовани страни);
- Защита (Protection) включва:
    - архитектура за ИТ сигурност (IT Security Architecture);
    - администриране на ИТ сигурност (IT Security Administration);
    - управление на идентичността и достъпа (Identity and access management);
    - поддържане на ИТ сигурността (IT Security Maintenance);
    - физическа и екологична а сигурност (Physical and environmental security);
- Откриване (Defence) включва:
    - откриване (Defence);
    - управление на инциденти свързани с компютърната сигурност (Computer Security Incident Management);
- Устойчивост (Resilience) включва:
    - непрекъснатост на операциите (Continuity of operations);

- управление на кризи (Crisis management).

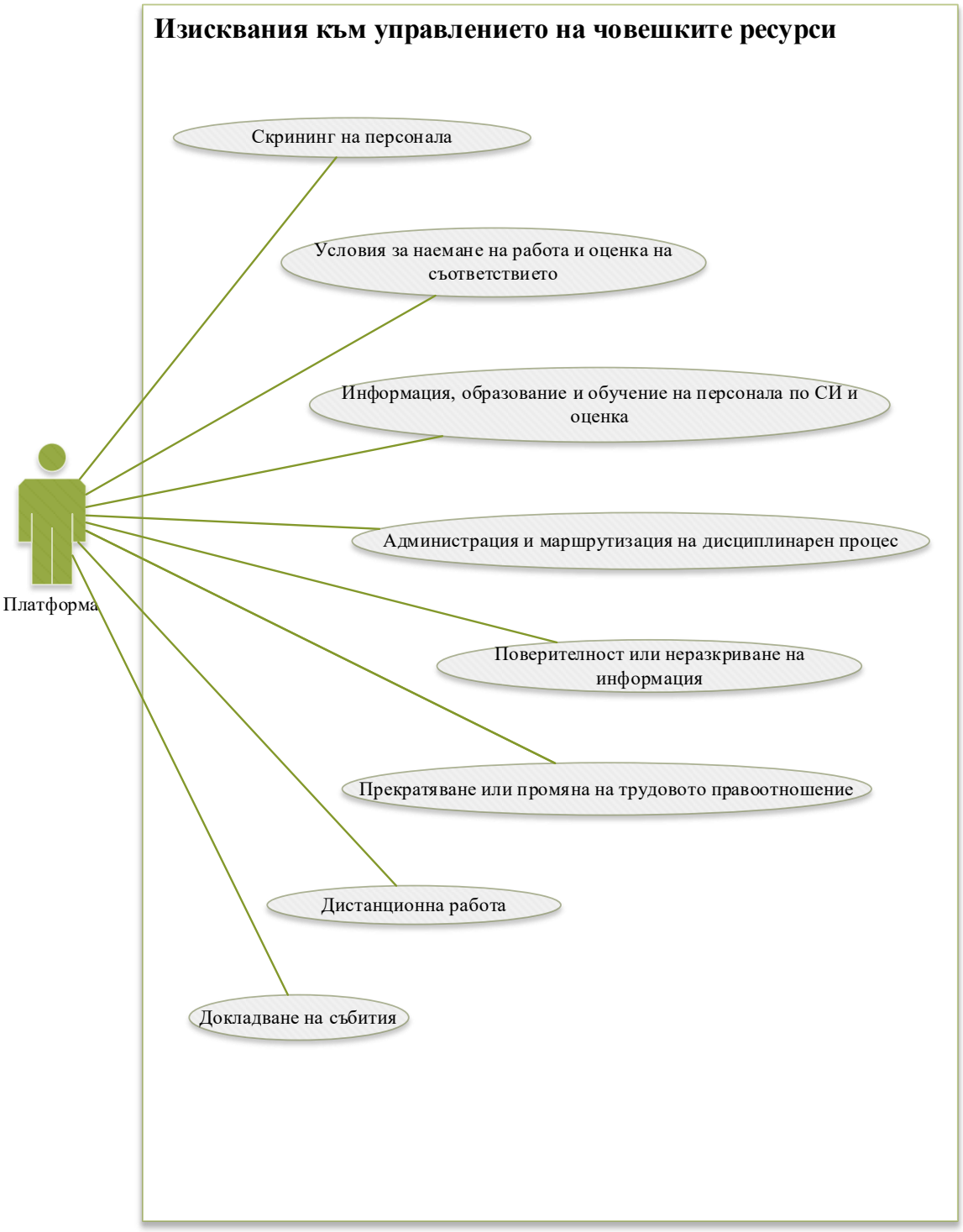
2.3.2.2 Изисквания на стандартите

2.3.2.2.1 Общи изисквания



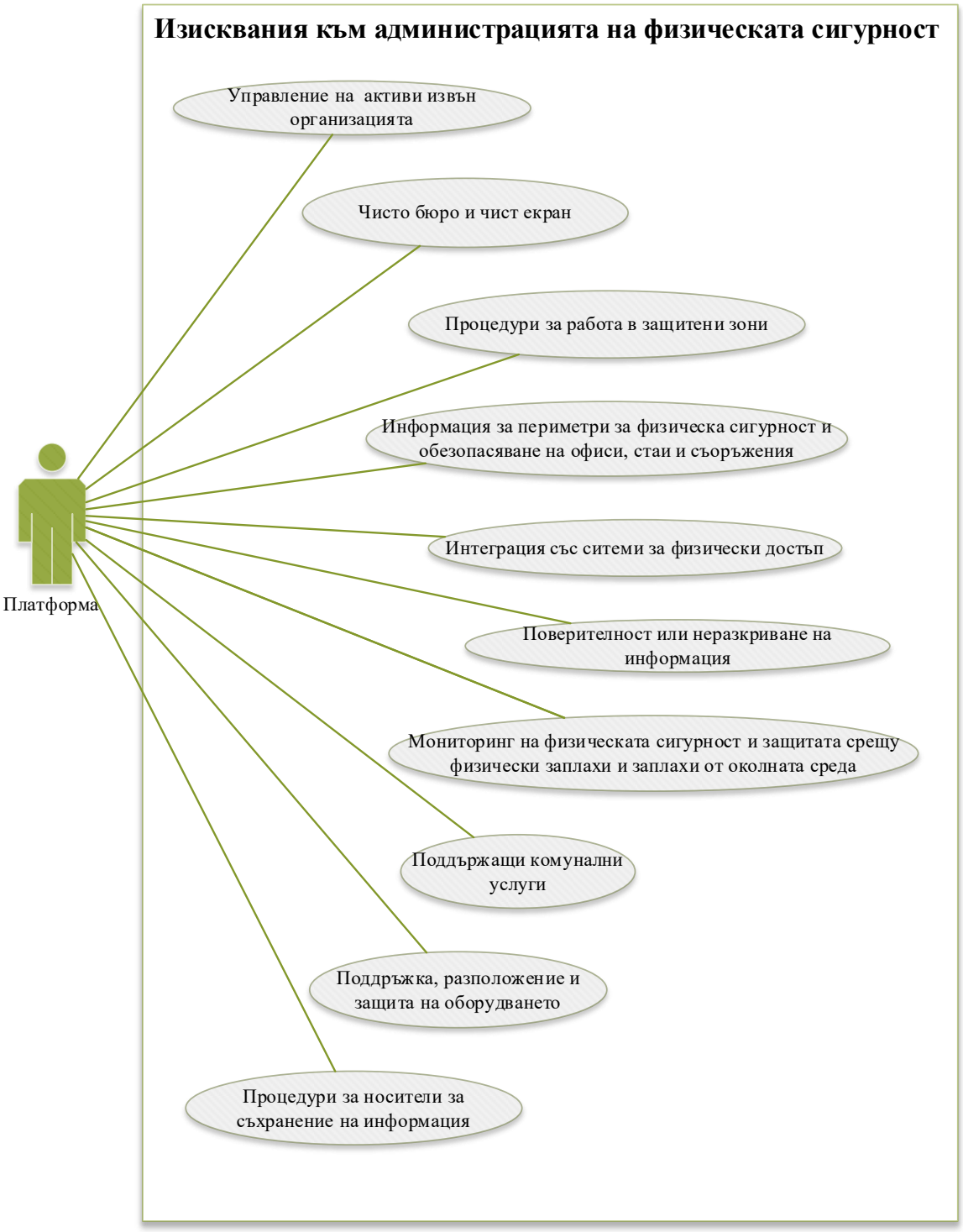
Фигура 15 Общи изисквания към модела произхождащи от стандартите за СИ

2.3.2.2.2 Изисквания към управлението на човешките ресурси



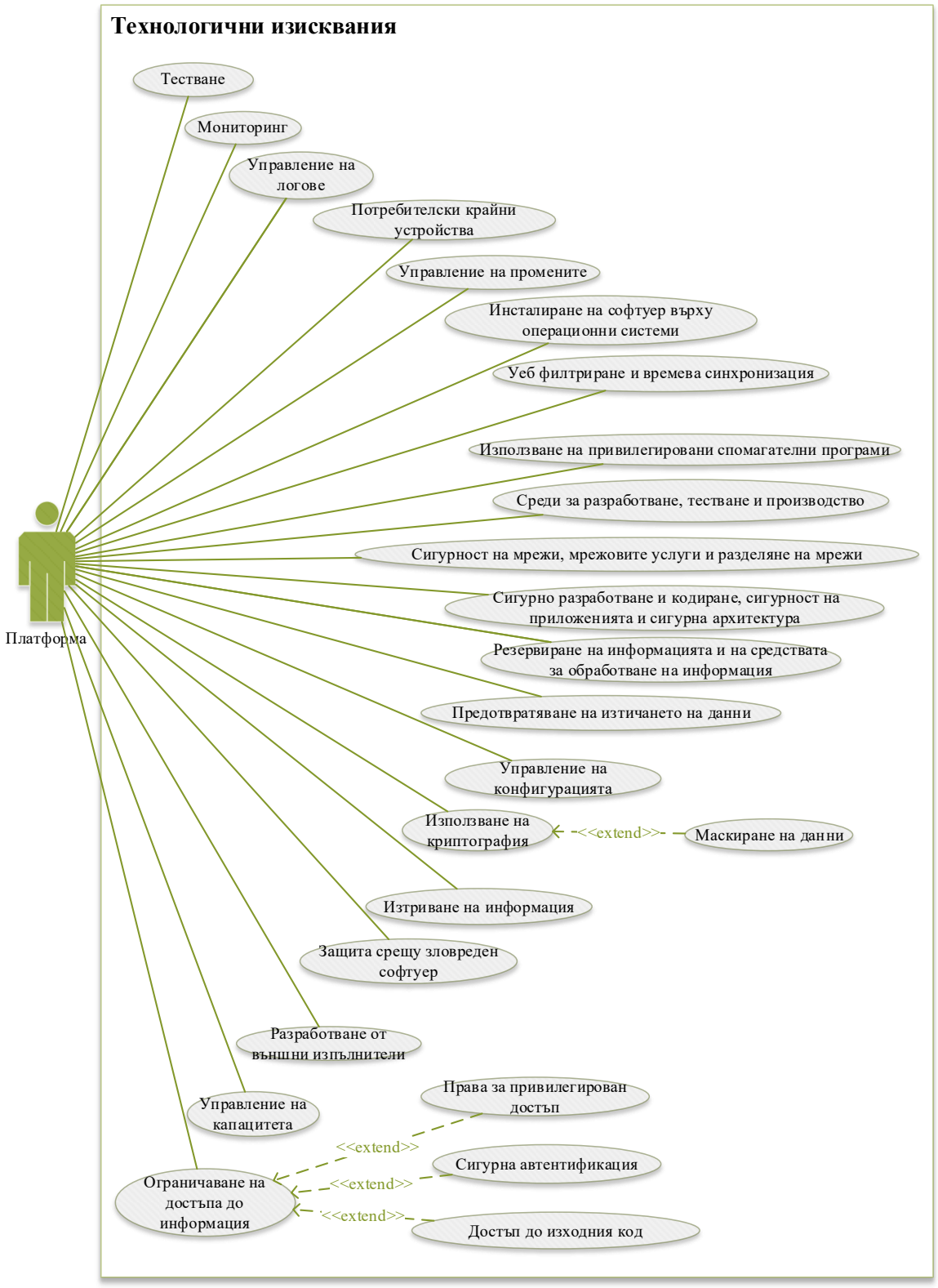
Фигура 16 Изисквания към управлението на човешките ресурси произхождащи от стандартите за СИ

2.3.2.2.3 Изисквания към физическата сигурност



Фигура 17 Изисквания към администрацията на физическата сигурност, произхождащи от стандартите за СИ

2.3.2.2.4 Технологични изисквания



Фигура 18 Технологични изисквания произхождащи от стандартите за СИ

2.3.3 Изследване и анализ на данните

Платформа за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията СУСИ, оперира с две основни групи данни, като следва:

2.3.3.1 Данни свързани със стандартите за информационна сигурност

Регистрираните, управляваните и анализираните данни, свързани със стандартите за сигурност определящи СУСИ се дефинират и генерират от механизмите за контрол. Изследвани са съобразно групите механизми и е идентифициран техния формат и тип. Резултата е показан в **Приложение 3.**

2.3.3.2 Данни свързани с функционалните изисквания за Платформата

Изследвани са данни свързани с функционалните изисквания за Платформата като са групирани в категории Документалистика и архивистика, Администриране и Комуникация. Резултата е показан в **Приложение 3.**

2.4 Общи характеристики на платформата

Определянето на общите характеристики на платформата за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията е извършено съгласно методологията описана в т. 2.3.1. Характеристиките са класифицирани в 4 групи както следва: [32]

2.4.1 Системна и приложна архитектура

Платформата е интегрирана информационно-оперативна система за управление на СУСИ в компании и организации, която създава, цифровизира, регистрира, управлява, контролира и съхранява фирмената инфраструктура. Системата **моделира и автоматизира бизнес логиката и бизнес процесите в използващата я организация.** [42]

2.4.1.1 Хетерогенна архитектура

Концептуално модела е софтуерна отворена платформа за управление на предприятието с многослойна, хетерогенна, клиент-сървър, сървис ориентирана архитектура (СОА), базирана върху компонентна технология, която позволява изграждането на персонализирани “Business on Demand” решения с използване на съществуващи съставни блокове. Всяка адаптация на платформата представлява необходимия оптимален за клиентската организация набор от функции и под функции на системните модули. [43]

Предимството на модулната архитектура е съответната автономност на модулите. Възможно е да се добавят, променят, развиват и премахват модули, съобразно динамиката на Бизнес средата. Позволява етапност в разработката и внедряването на различните функционални части и възможност за приоритизиране на изпълнението, съобразно решенията на мениджмънта на организацията.

2.4.1.2 Интегрируемост

Важно изискване към платформата е **интегрируемост,** постижима основно чрез установяване на стандартни интерфейси между модулите на интегрираната система. Такава характеристика на системата предполага възможности за**:** [44], [45]

Еднократно въвеждане на данните – данните свързани с различните информационни класове се въвеждат в системата там където възникват и се използват навсякъде, където са необходими. Това води до оптимизиране на работните процеси, минимизиране на оперативната работа и респективно до минимизиране на риска от информационни грешки.

Проследяване на дейностите – възможност за наблюдение на работните процеси, персонализация на операциите – респективно на отговорностите за целите на контрола по решенията. Актуалното състояние на всеки модул трябва да бъде достъпно за всички останали логически свързани модули. Платформата трябва да осигурява запис на всички системни приложни транзакции, да идентифицира и записва всяка промяна в данните, както за потребителските така и за системните елементи, да поддържа и отпечатва справки за всички промени, показвайки миналата и текуща ситуация. Всички справочни записи трябва да носят информация за потребител, дата и време когато са направени. [46]

Унифициране на клиентското работно място – потребителите използват различните информационни класове и системна функционалност чрез унифицирани интерфейси и инструментариум, съответно унифицирани съобразно възможните вариации на изпълняваните операции. Системата трябва да използва общ стил за всички потребителски интерфейси (екрани и справки) в аспекти употреба и представяне.

Системна прозрачност – хармонизирана архитектура на програмните решения, недвусмислено описание на програмните класове, параметри и функции, алгоритъм за проследяване и трасиране в реално време. Системната прозрачност осигурява възможност за интеграция с външни системи, разработка и внедряване на нови функционалности и усвояване на нови иновационни решения. Текущото състояние на всеки системен модул трябва да бъде видимо за всички останали логически свързани модули.

Висока скорост на извличане на информация – функционално изискване към структурата на базата данни на платформата за осигуряване на информационен обмен и респективно висока степен на информационно потребление. Базата от данни трябва да бъде обновявана незабавно след като входящите данни се потвърдят и приемат. Трябва да бъде осигурена подходящо **висока скорост на обработка на информацията и кратко време за отговор на системата,** гарантирано с висока **производителност (performance)**.

Взаимодействията между отделните модули в системата и интеграциите с външни информационни системи трябва да бъдат реализирани и описани под формата на уеб услуги. За всеки от отделните модули на платформата е необходимо да се

внедрят и опишат интерфейси за приложно програмиране (API), които са налични за интегриране на нови модули и други системи. [47]

2.4.1.3 Гъвкавост

Платформата е с презумпцията, да отразява адекватно околната и вътрешно-организационната среда, да е в състояние да реагира своевременно на промените във функционалността и структурата на потребителя. Платформата трябва да може да отразява възможни промени в резултат на постоянно променящата се регулаторна, бизнес и технологична среда. Основното изискване е необходимостта информационната система да бъде разработена като гъвкава и лесно адаптируема, отчитаща възможностите за законодателни, административни, структурни или организационни промени, водещи до промени в работните процеси. [48]

2.4.1.4 Адаптивност

Входът и изходът е необходимо да са параметризирани, което да дава възможност да бъдат настройвани в зависимост от конкретните условия и изисквания на клиентската компания. При извеждане на информация се използват филтри, в които се задават критериите, по които потребителят би искал да бъде сортирана информацията. Бизнес процесите и услугите трябва да бъдат проектирани възможно най-независимо за по-лесно надграждане, разширяване и поддръжка. Платформата трябва да бъде максимално параметризирана и да позволява настройка и промяна на параметри през сервизен (администраторски) потребителски интерфейс. [49]

2.4.1.5 Максимален обхват на участниците

Необходимо е автоматизиране на работата с партньори и основни кореспонденти на базата на използване на уеб-базирани технологии. Потребителите на системата да могат при строго контролиран достъп да работят в реално време с части от системата открити и интерпретирани с подходящ за тях интерфейс, съобразно потребителските групи. Всяко тяхно действие автоматично се регистрира, а стартираните от тях процеси.) следват стандартно заложени процедури. [50]

2.4.1.6 Интуитивен потребителски интерфейс

Потребителският интерфейс трябва да е интуитивен за потребителските групи и да не е необходимо те да бъдат компютърни специалисти или да преминават специални курсове на обучение. Тази функционалност гарантира безпроблемното възприемане на платформата в различните потребителски звена. Потребителите могат да концентрират усилията си към изпълнение на преките си задължения и функции.

2.4.1.7 Достъп

Концепцията на СУСИ се базира на строго контролиран достъп до обекти и функции. Платформата трябва да дава възможност за фино контролиране на правата на достъп и действие на всички потребители до обектите на всички нива – област (домейн), сървър, база, справка, документ и дори поле.

2.4.1.8 Комуникативност

Платформата трябва да осигури оптимална организационна структура за комуникация в реално време и реализиране на единна комуникационна среда.

2.4.1.9 Скалируемост

Архитектурата на Платформата и всички софтуерни компоненти (система и приложение) трябва да гарантират надеждност, наличност, поддръжка, както и недискриминационна инсталация (без различни условия за инсталация във физическа и виртуална среда). Системата трябва да предоставя възможности за разширяване, резервиране и балансиране на натоварването между множество екземпляри на сървъри с една и съща роля. [51]

2.4.2 Управление на работните процес и контрол на решенията

2.4.2.1 Управление на работните процес

Платформата трябва да предоставя необходимата инфраструктура за автоматизиране на работните процеси в организацията. Тя гарантира, че работата намира извършителя, вместо, както често се случва, обратното. На автоматизираното работно място на всеки служител пристигат документи, изискващи определено действие. Те носят своята история в предишни инстанции, както и връзки с различни обекти, до които може да се стигне по всяко време. Платформата автоматизира процедурите за изпълнение на целия процес, чрез предварително дефинирани електронни маршрути, шаблони и процедури за всички видове документи и обекти. Маршрутите трябва да се определят, като се съобразяват оптималните организационни структури, изискванията на различните стандарти за сигурност и на екипа. Документите автоматично преминават през различни участници в процеса, осигурявайки единни обективни стандарти и правила, които съответстват на различните видове дейности за всички участници. По този начин се осъществява комуникация между тях и се гарантира качествен ред на изпълнение.

Неструктурираната входна информация се въвежда в платформата чрез различните функционални модули на подсистемите и се трансформира в определени модели и форми, изградени според изискванията на фирмата клиент, световните практики и различните стандарти за сигурност. По този начин процесите на категоризиране, достъп, анализ, управление и споделяне на информация са оптимизирани.

Платформата създава и управлява шаблони - стандартни документи за употреба. За целта се използват два различни метода, всеки от които активно намира своето приложение. Един от начините е да се създават шаблони с помощта на вътрешни системни формуляри. Подходящ е за прости документи с фиксиран формат и необходимост да се работи само в среда на платформа. Другият метод позволява създаване на сложни документи, създадени от друго приложение (Word, Excel, Open Office и др.). [32]

2.4.2.2 Контрол на решенията

Всеки документ и всяко действие или бездействие при необходима реакция се регистрира от платформата. Така голяма част от базата за вземане на решения: пакет от документи, справки от друга система, становища на колеги, становища на експерти и т.н. е налична за всяка инстанция. Взетото решение се регистрира и всеки мениджър може да следи състоянието на своите приоритетни, текущи или просрочени задачи, свързани със системата за управление на информационната сигурност на компанията. Платформата осигурява проследяване и контрол на действията по задачите в условията на времеви ограничения и процеси, като предоставя на отделите и крайните потребители подробна информация за текущото състояние на всяка от задачите, нейните стъпки, участващите лица и свързаните с тях задължения.

2.4.3 Администрация

Платформата трябва да предоставя профил за потребителско администриране и достъп. За системна администрация е необходимо да се предвиди използването на административен панел, с който системните администратори да управляват, назначават, отнемат роли и права на потребители. Трябва да има и административен интерфейс, чрез който да се конфигурира.

По отношение на системните записи в приложните сървъри, които поддържат критични дейности като сървъри на системна инфраструктура, сървъри на мрежова инфраструктура, съоръжения за сигурност, мрежово оборудване и администраторски работни станции, платформата трябва автоматично да записва всички събития, които са свързани с удостоверяване на потребителя, управление на акаунти, права за достъп, промени в правилата за сигурност и работа на информационни и комуникационни системи.

За всяко от събитията трябва да се регистрира астрономическото време, когато събитието се е случило, като се гарантира, че информацията се архивира за определен период. Записите в регистъра не трябва да се изтриват или променят и всяко изтриване или промяна трябва да представлява нов запис. Астрономическото време за удостоверяване на настъпването на факти с правно или техническо значение се отчита с точност до година, дата, час, минута, секунда и при необходимост до милисекунди, изписано в съответствие със стандарт БДС ISO 8601:2006.

Платформата трябва да осигури функционалност за текущо наблюдение, анализ и контрол на изпълнението на бизнес процесите. Трябва да се използват системи за пълнотекстово търсене, за да се предотврати използването на пълно текстови индекси в RDBMS. Всеки обект в системата трябва да има уникален идентификатор. [32]

2.4.4 Използваемост, продуктивност и сигурност

- Функционалностите на потребителския интерфейс на Платформата трябва да са независими от интернет браузърите и устройствата, използвани от

потребителите, при условие че последните са версии в процес на поддръжка от съответните производители.

- Екранните форми на Платформата трябва да използват персонализирани бутони с еднакъв размер и лесни за разбиране текстове в същия стил. Всички текстови елементи на потребителския интерфейс трябва да бъдат визуализирани с шрифтове, които са подходящи за показване на екрана и осигуряват максимална съвместимост и еднакво възпроизвеждане при различни клиентски операционни системи и браузъри.
- Полетата, опциите на менюто и командните бутони, които не са специално разрешени за влезлия потребител, не трябва да са достъпни за този потребител.
- Платформата трябва да поддържа прекъсване на потребителски сесии при липса на активност. За големи йерархични категоризации трябва да е възможно навигиране по нива или чрез отложено зареждане.
- Платформата трябва да може да съхранява и едновременно да показва данни и съдържание, които са въведени/генерирани на различни езици.
- Всички софтуерни компоненти на Платформата, използваните софтуерни библиотеки и комплекти за разработка, сървърите за приложения и сървърите за управление на бази данни, елементите на потребителския интерфейс, програмно-приложните интерфейси, уеб услугите и др. трябва да се поддържат стандартно и да бъдат изрично конфигурирани да отговарят на минимум Unicode 5.2 стандарт при съхраняване и обработка на текстови данни, съответно трябва да се използва само UTF-8 кодиране на текстови данни.
- Във формите за въвеждане трябва да се реализира валидиране на въведените от потребителите данни на ниво "поле" (in-line validation). Валидацията трябва да се извършва в реално време на сървъра, като при успешна валидация данните от съответното поле следва да бъдат запазени от сървъра.
- Трябва да се разработи контекстуална помощна информация за всички процеси, екрани и електронни формуляри, включително ясни инструкции за попълване и обяснения за спецификата на попълване на различни групи полета или отделни полета;
- Разработеното решение трябва да осигури проследимост на действията на всеки потребител (одит), както и версия на предишното състояние на данните, които потребителят е променил в резултат на действията си (системен журнал). Трябва да бъде изграден модул за проследимост на действията и събитията в Платформата (добавяне, изтриване, промяна, четене).
- Системата трябва да поддържа на ниво приложение скоростно ограничаване и throttling на заявки от един и същи клиентски адрес както към страниците с уеб съдържание, така и по отношение на заявките към програмните интерфейси на приложенията.
- Платформените модули и интерфейси трябва да бъдат проектирани и да

използват разпределени кохерентни кеш системи в случаите, когато това би подобрило производителността и скалируемостта чрез запазване на заявки към СУБД или сървърни файлови системи.

- При показване на екрани платформата трябва да осигурява висока производителност и минимално време за реакция – средното време за заявка трябва да е по-малко от 1 секунда, с максимум 1 секунда стандартно отклонение за 95% от заявките, без включително мрежово време закъснение при транспортиране на пакети между клиента и сървъра.
- Не трябва да се разрешава публично съхраняване на пароли на администратори, вътрешни и външни потребители и акаунти за достъп до системи. Всички пароли трябва да бъдат защитени с подходящи сигурни алгоритми за съхранение на пароли и където е възможно, трябва да се използва прозрачно криптиране на данните в покой.
- При внедряването на всички уеб услуги трябва да се използва само HTTPS протокол със задължително приложение на минимум TLS 1.2. Програмният код трябва да включва методи за автоматична проверка на въведените данни и потребителски действия за защита от кибератаки.
- Платформата трябва да осигури ежедневно архивиране на данните, съхранявани извън инфраструктурата на системата. [32]

2.4.5 База данни

- Трябва да се следват най-добрите практики за проектиране и оперативна съвместимост на бази данни (релационни или нерелационни (NoSQL)):
- Дизайнът на схемата на базата данни трябва да бъде с максимално ниво на нормализиране;
- Базата данни трябва да може да работи в клъстер;
- Имената на таблиците и колоните трябва да следват унифицирана конвенция;
- Индексите трябва да се създават върху конкретни колони, така че да се оптимизират най-често използваните заявки;
- Връзките между таблиците трябва да се дефинират с помощта на външен ключ;
- Трябва да се използват транзакции с подходящо ниво на изолация;
- Заявките трябва да бъдат ограничени до броя на записите, които връщат;
- Когато се използват слоеве на абстракция между приложението и базата данни, броят на излишните заявки трябва да бъде сведен до минимум;
- Когато се използва нерелационна база данни, трябва да се използват по-бързи и компактни комуникационни протоколи. [32]

2.5 Основни изводи и резултати към Глава 2

- Извършен е анализ на стандартизираните работни процеси, които да бъдат включени в модела на Платформата, подлежащи на автоматизация и съответните, кореспондиращите с тях информационните потоци.
- Определени са функционалните и нефункционалните изисквания към Платформата след направен анализ на данните, на потребителските групи и на стандартите за информационна сигурност
- Изследвани са добрите практики за потребителско поведение, продуктивност, сигурност и администрация на информационните системи и са идентифицирани общите характеристики на Платформата.

3. ГЛАВА 3. МОДЕЛ НА ПЛАТФОРМА ЗА МОДЕЛИРАНЕ И АВТОМАТИЗАЦИЯ НА СТАНДАРТИЗИРАНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА.

3.1 Концепция

Платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията е съвременна, иновативна, интегрирана информационно-оперативна система, която моделира, дигитализира, регистрира, управлява, съхранява и контролира работните процеси и свързаната с тях информация и документация, в съответствие с различни международно признати стандарти за информационна сигурност. [52]

Модела се базира на мониторинг, анализ и управление на документната матрица, работните процеси и на информационните потоци и активи на организацията. Платформата обхваща всички информационни единици - документи (хартиени и електронни), аудио и видео комуникации, системни, програмни и комуникационни логове. Мониторира входящите, изходящите и вътрешните информационни потоци и ги управлява, съобразно моделираните в нея работни процеси и стандартизирани форми.

Работните процеси и стандартизираните форми са моделирани, съобразно политиките, процедурите и шаблоните на системите за управление на сигурността на информацията (СУСИ). Всички записи, свързани не само с елементите на СУСИ, а и с оперативните процеси се формализират във платформата и се извършват само чрез нея. Целта е да се използват най-новите технологични постижения, за да се цифровизира, индексира и съживи документната матрица на организацията и да позволи оперативна ефективност на управление на сигурността.

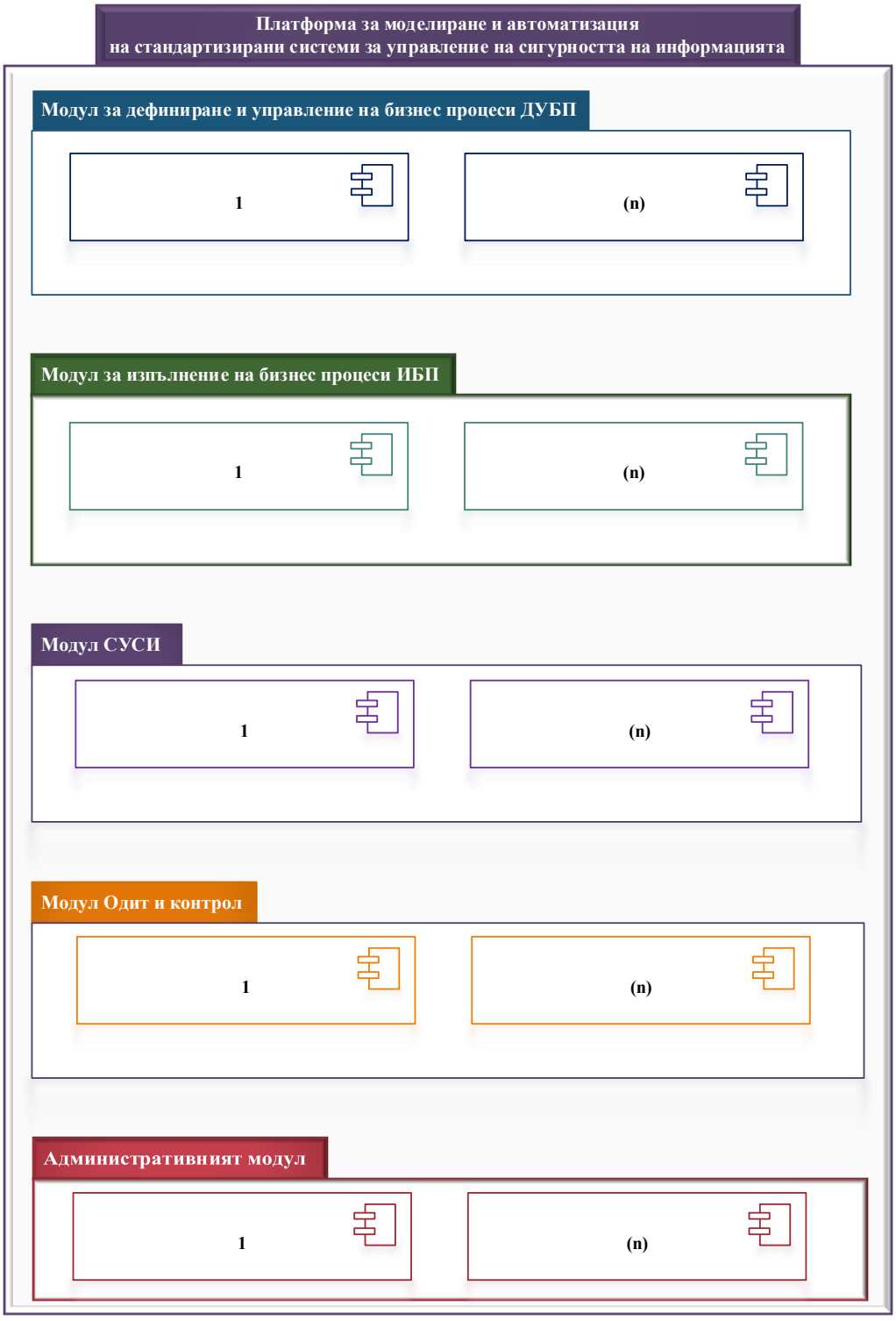
Информационните активи се въвеждат в Платформата като параметризирани обекти. Всеки контрол от системата от контроли на стандартите за информационна сигурност, съобразно които е изградена СУСИ се асоциират с един или няколко предварително дефинирани критерия на платформата.

Всеки критерий е формализиран запис с определени параметри на регистрираната информация и честота и начин на проверка. За всеки критерий се дефинират тригери на действие на платформата, съобразно възможни стойности или събития.

Контролите се прилагат към актив и/или процес в съответствие със СУСИ.

Мисията на платформата е да интегрира всички документи потоци, свързани с работните процеси в клиентската организация. Да свърже множеството приложни софтуерни продукти работещи в сферата на информационната сигурност и масивите от данни в една единна информационно-комуникационна и управленска система. Платформата

обединява информационните сечения и информационните потоци в единно информационно пространство и осигурява интегрирана среда за съхранение, управление и обмен. Това позволява да се следи ефективно движението на информацията, структурирана в отделни типове документни единици, да се моделира СУСИ и да се осъществява надежден контрол. [53]



Фигура 19 Структура на Платформата

Съгласно извършените изследвания и анализи, представени в Глава 2 Платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията се реализира, както е показано на фигурата със следните компоненти (функционални модули):

- Модул за дефиниране и управление на бизнес процеси ДУБП;
- Модул за изпълнение на бизнес процеси ИБП;
- Модул СУСИ;
- Модул Одит и контрол;
- Административният модул;

Модулите са взаимно интегрирани в обща среда на платформата, съобразно концептуалната архитектура, показана във фигура 21.

Платформата моделира йерархичната структура на организацията, с възможност за изменения, като позволява адекватно разпределение на задачите съобразно субординацията на компанията. Системата управлява движението на разнообразни типове документи, като автоматизира всички фази на работните потоци. [54]

3.1.1 Документна матрица

Всяка компания независимо от мащаба си изпълнява своята дейност във вътрешна и външна работна среда. Вътрешната среда се определя от ресурсите на компанията (човешки, материални и нематериални) и от работните процеси в нея, свързани с предмета на дейност. Външната среда са клиентите, доставчиците, партньорите и държавните институции с които компанията работи.

Системите за управление на сигурността на информацията по международно признатите стандарти дефинират, регламентират, управляват, наблюдават, регистрират и архивират вътрешната и външната среда на функциониране, чрез системата от документи на организацията и кореспондиращите масиви от данни.

Документа е запис, чрез който се отразява в неговото развитие всяко действие, норма, събитие, ресурс, отношение, процес и интелектуално производство. Освен че в днешно време документите са електронни и хартиени те могат условно да се класифицират в няколко формални групи.

- *Конвенционални записи* – задължителни за всяка организация:
    - Входящо-изходяща кореспонденция с партньори, клиенти и доставчици;
    - Запитвания, Оферти и Тръжна документация;
    - Договори, анекси, протоколи за изпълнение;
    - Вътрешни заповеди, длъжностни характеристики, правилници и инструкции;
    - Фирмени документи от и за държавната и общинска администрация;

- Първични счетоводни документи и др.

- Специализирани документи - Фирмено ноу-хау:
  - Проектна документация;
  - Проучвания и изследвания;
  - Интелектуална собственост;
  - Дизайн;
  - Информация за клиенти и история на взаимоотношенията;
  - Работни процеси и методики за изпълнение;
  - Маркетингови документи – марка, фирма, реклами, брошури, пазарни анализи;
  - Фирмена практика и специфични решения;
  - Процедури, форми, регистри и др.

Количеството от всички тези записи, наречени документи, дефинират и определят компанията, нейната история, капацитет, качество и конкурентно способност.

Документите сами по себе си не са независими отделни единици. Те са свързани в специфична за всяка фирма **документна мрежа**.

Всеки документ е краен продукт, зад който стои процес от различна сложност и обхват (Пример фигурата по-долу). Всеки документен процес се състои от дейности и етапи и както във всяко производство се нуждае от ресурси и материали. Ресурсите и материалите от своя страна са най-често масиви от данни и други документи, които имат своите процеси и своя жизнен цикъл. Множеството документи и връзките между тях образуват документната мрежа на организацията. За разлика от Интернет мрежата обаче документната мрежа на една компания има дефинирани пътища, връзки и форми (формуляри) и е свързана и индексира и управлява масивите (базите) от данни на организацията.

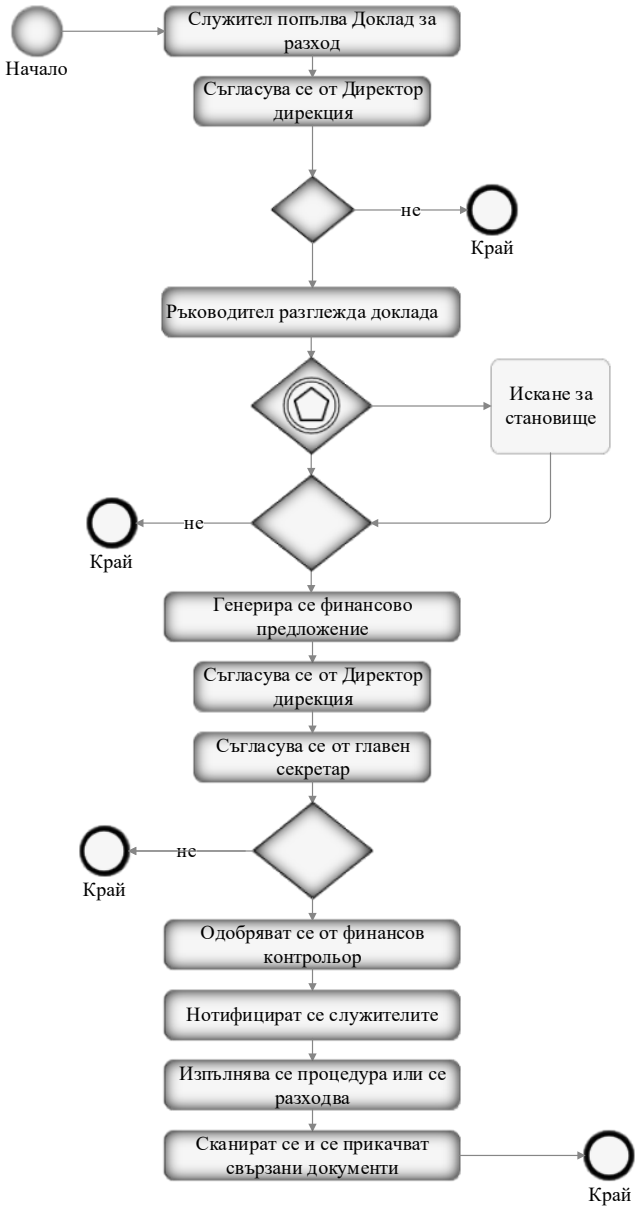
По тази причина системата от фирмени документи се разглежда не като документната мрежа, **а като документна матрица** на компанията. [1]

Документната матрица засяга всеки елемент от вътрешната и външна работна среда на фирмата и е съвсем логично тя да дава възможност за максимален контрол върху организацията.

Фирмената документна матрица е в основата на управлението на всяка система за управление, изградена по международно признати стандарти. Те са базирани на политики, работни процеси, процедури и множество форми за контрола им.

Когато документите на фирмата са на хартиен носител, то те са образно казано мъртви. Почти невъзможно е употреба им от множество потребители едновременно, много трудно се проследяват многобройните връзки, трудно се преизползват решения, трудно се осъществява контрол на тяхна база.

Когато документите се цифровизират, връзките между тях се визуализират и матрицата се облече в подходяща функционалност, то се получава изключително ефективна система за мониторинг, контрол и управление на всички нива и ресурси в компанията.

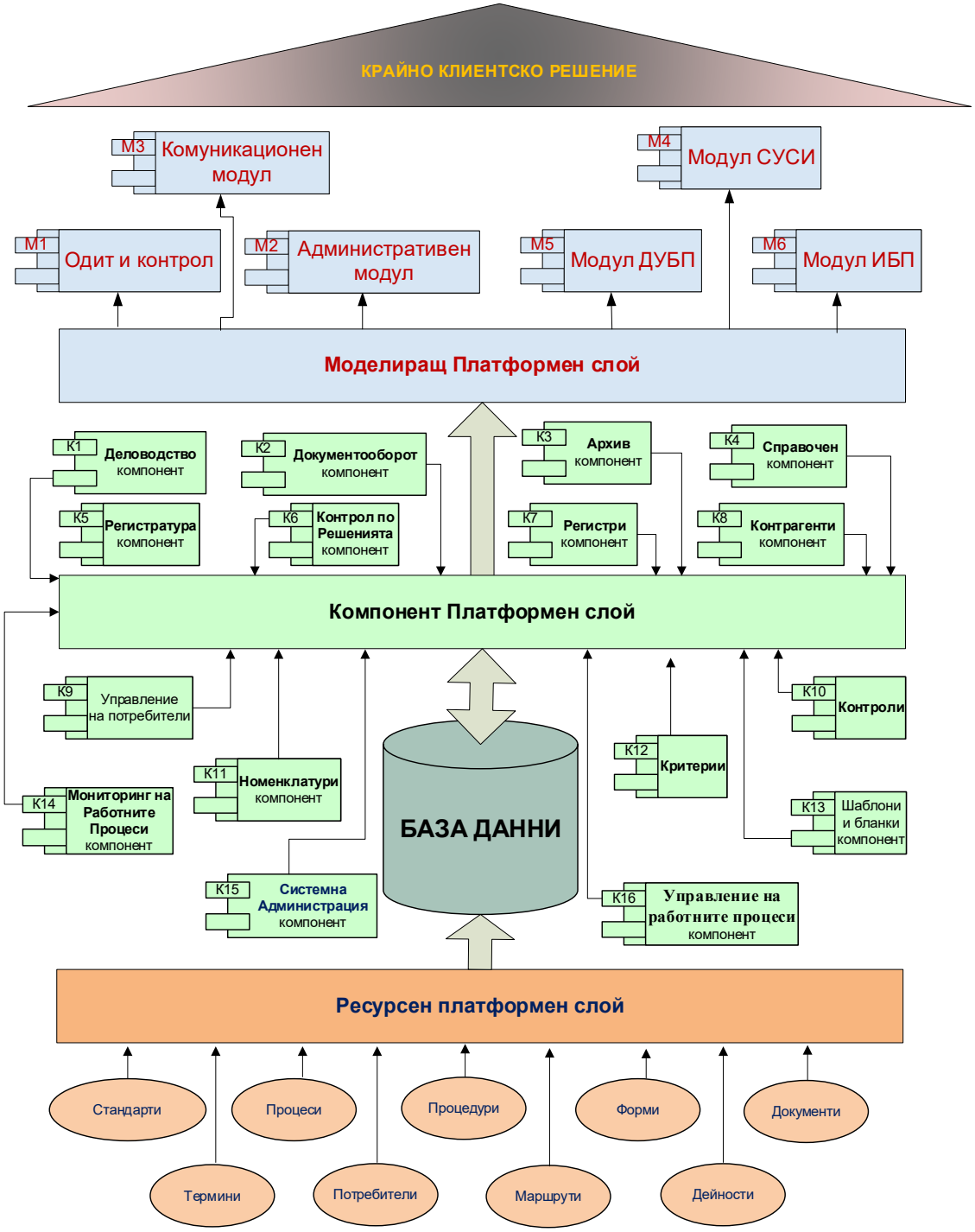


Фигура 20 Процес на заявка за закупуване на материали

3.1.2 Концептуален модел

Платформата използва единна база от данни в която чрез различни интерфейси се въвежда и извежда необходимата информация, съобразно информационните класове. Базовите масиви се управляват чрез изграждане на специализирана логика за всеки от тях – стандарти, термини, процеси, потребители, процедури, маршрути, форми, контролирани процеси, и различни неструктурирани данни. Платформения слой, така наречения мидълуер, реализира логиката и обмена на информация между

интерфейсите за въвеждане на информация и базата от данни. Друг платформен слой, реализира връзката на функционалните модули и базата от данни. Функционалните модули (компоненти) изпълняват определена група от функции, чрез предоставяне на интерфейси за осъществяване на необходимите задачи. Платформата изгражда модулите си в контекста на всяка клиентска организация, като набор от компоненти (функционални модули) както е показано на фигурата. [55], [56]



Фигура 21 Концептуална архитектура на модела

Платформата обхваща всички информационни единици - документи (хартиени и електронни), аудио и видео комуникации, системни, програмни и комуникационни логове. Мониторира входящите, изходящите и вътрешните информационни потоци и ги управлява, съобразно моделираните в нея работни процеси и стандартизирани форми.

Работните процеси и стандартизирани форми се моделират, съобразно политиките, процедурите и шаблоните на СУСИ. Всички записи, свързани с елементите на СУСИ се формализират във платформата и се извършват само чрез нея.

Информационните активи се въвеждат в Платформата като параметризирани обекти.

Всеки контрол от системата от контроли на стандартите, съобразно които е изградена СУСИ се асоциира с един или няколко предварително дефинирани критерия на платформата.

Всеки критерий е формализиран запис с определени параметри на регистрираната информация и честота и начин на проверка.

За всеки критерий се дефинират тригери на действие на платформата, съобразно възможни стойности или събития.

Контролите се прилагат към актив и/или процес в съответствие със СУСИ.

Системата притежава регистрационно-контролна част, в която се въвеждат индекси на организацията и се регистрират в съответствие с тях всички входящо-изходящи и вътрешно оперативни документи (събития). Автоматично се генерират номера на документите съгласно предварително заложен стереотип. Към всеки регистриран документ могат да се задават срокове за изпълнение, които тя контролира. Системата функционира и като комуникатор, като информира по различни начини (е-мейл, SMS, звуково и визуално) за различни контролирани събития, просрочени срокове и задачи за изпълнение. Електронната система моделира създадените в компанията по съответния стандарт оперативни процедури и процесни карти, като осигурява информационно коректното спазване на всички работни процеси, попълване на съответните формуляри и бланки, мониторинг на работните процеси и контрол на решенията. Системата гарантира възможно най-високи нива на сигурност, надеждност и защита на информацията. Осигурена е възможност всеки потребител да се идентифицира не само с потребителско име и парола, а и с частен електронен подпис. Всеки служител/потребител има предварително дефинирани профили, роли, права на достъп и функционалност, съответстваща на длъжностната му характеристика. Системата генерира динамично персонални екрани при влизането на потребителя, като му предоставя интуитивен потребителски интерфейс и навигация. [57]

Модулите на Платформата изграждат моделите, свързани с управление на различи типове международно признати стандарти с богат инструментариум: **типизирани процеси**; **предварително разработени сценарии и постановки**; набор от предварително дефинирани форми; разработени конвенционални регистри;

специализирани регистри; вътрешна комуникационна среда; системи за оценка, контрол и подпомагане на одита; и други. [58], [59]

3.2 Методика за моделиране

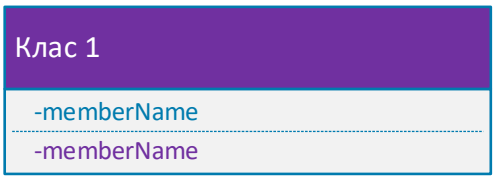
Въз основа на функционални и нефункционални изисквания, бизнес процесите и спецификацията на потребителски случаи, дефинирани в предходната глава след направеното изследване и анализ, се разработи оптимален набор от информационни определители, разпределени в логически информационни класове и подкласове.

Наборът от дескриптори, генериран от извършените изследвания и анализи е декомпозиран на логически информационни класове, в съответствие с тяхната функционална ориентация в описанието на стандартите. Информационните класове се разглеждат като програмни обекти и подобекти. Те се описват чрез своите информационни атрибути, които се наричат информационни идентификатори. Тяхното представяне е унифицирано чрез използване на специфичен технически формат, който определя формата на представяне на стойностите на всеки атрибут на информационните обекти. Техническият формат на информационните класове и техните атрибути се описва от синтаксиса на унифициран език за моделиране (UML).

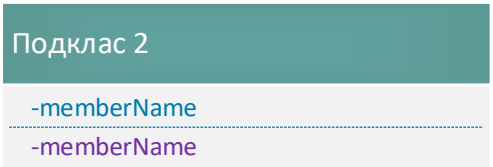
За дизайна на системата са използват UML клас диаграми. които изобразяват структурата на системата чрез моделиране на нейните класове, свойства, операции и връзки между обекти. Клас диаграмата е визуална нотация, използвана за изграждане и визуализиране на обектно-ориентирани системи. Тя е статична структурна диаграма, демонстрираща свойствата на системата, класовете, операциите и връзките между обекти за описание и дизайн на системата. Диаграмите на класове са форма на структурни диаграми, тъй като те определят какво трябва да бъде включено в моделираната система. [60]

Информационните идентификатори са моделирани в 3 нива информационни класове структурирани в модули на платформата:

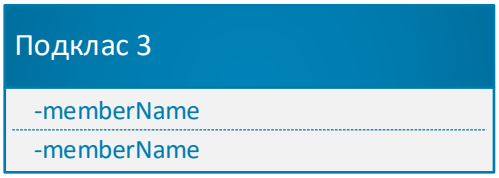
Използваната нотация е:



- този блок означава основен информационен клас;



- този блок означава композитен информационен подклас (включващ подкласове)



- този блок означава информационен подклас

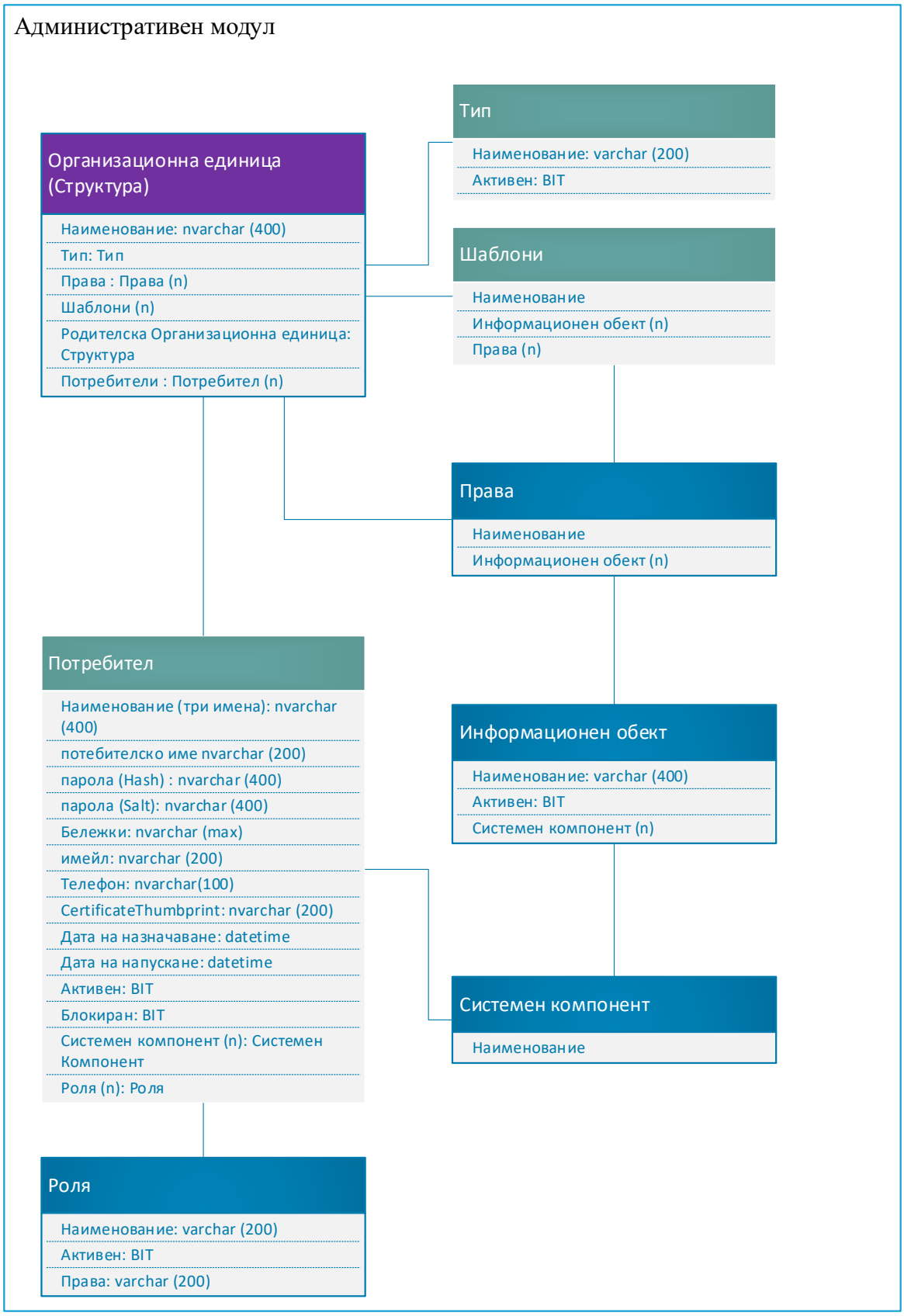
3.3 Модел на платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията.

Модела е изграден съблюдавайки добрите практики и постулати при проектирането. [61]

3.3.1 Административен модул

Административният модул позволява на оторизирани лица с право на достъп да:

- Създават и променят организационна структура от дирекции, отдели и сектори. в йерархичен вид;
- Позволява регистрация на потребители (служители);
- Асоцииране на служител към йерархичната структура на организацията;
- Позволява редактиране, активиране и деактивиране на потребители;
- Позволява управление на средствата за достъп (пароли, ключове, електронни подписи и т.н.) на потребителите;
- Позволява управление на правата на всеки потребител или група такива за достъп до всички информационни обекти на системата;
- Позволява йерархично определяне на права;
- Позволява създаване на шаблони от права както и тяхната йерархична организация;
- Дефинира достъп за четене, запис (промяна) на информационните обекти в системата като цяло, както и до определени техни полета и колекции;



Фигура 22 Административен модул

3.3.1.1 *Организационна единица (Структура)*

Таблица 2 Описание клас Структура

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Организационна единица: () Структура	Организационна единица (Структура) е базов клас на Административния модул, отнасящ се към описване на структурата на организацията и кореспондиращото и моделиране в Платформата.
Атрибут	Наименование: Nvarchar (400)	Наименование на организационната структурна единица.
Атрибут	Тип: Тип	Типът на структурата е предефинирана номенклатура – дирекция, отдел, сектор и длъжност.
клас	Родителска Организационна единица: Структура	Наименование на родителската организационна единица към която принадлежи структурата. (ако има такава)
Подклас	Права (n): Право	Списък от права върху информационните обекти които има организационната единица и всички нейни подструктури. Определят се набор от права за всеки информационен обект от класификатора – Пример: за информационен обект „Регистър на инцидентите“ право на четене, право на регистриране и право на редакция.
Подклас	Шаблони: Шаблон	Шаблоните са набор от права които могат да се прилагат към всеки информационен обект и да се добавят за структурно звено в комплект.
Подклас	Потребители: Потребител (n)	Списък от служители на организацията които са добавени към организационната структура.

3.3.1.2 *Потребител*

Таблица 3 Описание клас Потребител

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Потребител/ Служител: Потребител	Потребител е базов клас на Административния модул, отнасящ се към процеса на регистриране и управление на потребителите на Платформата
Атрибут	потребителско име: nvarchar (200)	Наименование на потребителя -Три имена
Атрибут	парола (Hash): nvarchar (400)	парола (Hash)

Атрибут	парола (Salt): nvarchar (400)	- парола (Salt)
Атрибут	Бележки: nvarchar (max)	Поле за отразяване на бележки за служителя.
Атрибут	Имейл: nvarchar (200)	Имейл адрес на служителя
Атрибут	Certificate Thumbprint : nvarchar (200)	CertificateThumbprint
Атрибут	Дата на назначаване: Date/time	Дата на постъпване на работа на служителя
Атрибут	Дата на напускане: Date/time	Дата на напускане на служителя
Атрибут	Активен: BIT	Двузначно поле за избор с възможности – активен/неактивен
Атрибут	Блокиран: BIT	Двузначно поле за избор с възможности – блокиран/неблокиран
Подклас	Системен компонент (n): Системен Компонент	Модули и компоненти на Платформата до които потребителя има Достъп.
Подклас	Роля (n): Роля	Набор от роли, които могат да бъдат присвоявани на потребителя.

3.3.1.3 Роля

Таблица 4 Описание клас Роля

Описание		
Тип	**Наименование/ Формат**	**Описание**
Подклас	Роля	Роли на потребителя
Атрибут	Уникален идентификатор: nvarchar (200)	Уникален идентификатор на ролята за системата
Атрибут	Наименование: nvarchar (200)	Наименование на ролята
Атрибут	Активна: BIT	Активна / неактивна
Подклас	Права : Права	Права за работа в системата, които съдържа ролята

3.3.1.4 Права

Таблица 5 Описание клас Права

Описание		
Тип	**Наименование/ Формат**	**Описание**
Подклас	Право: Право	Права върху системни компоненти

Атрибут	Уникален идентификатор: nvarchar (200)	Уникален идентификатор на правото за системата
Атрибут	Наименование: nvarchar (200)	Наименование на правото
Подклас	Информационен обект (n): Информационен обект	Права за работа в системата, които съдържа ролята

3.3.1.5 ***Информационен обект***

Таблица 6 Описание клас Информационен обект

Описание		
Тип	**Наименование/ Формат**	**Описание**
Подклас	Информационен обект:	Информационен обект в системата
Атрибут	Уникален идентификатор: nvarchar (200)	Уникален идентификатор на информационния обект за системата
Атрибут	Наименование: nvarchar (200)	Наименование на информационния обект
Атрибут	Активен: BIT	Статус на информационния обект Активен / неактивен
Подклас	Системен компонент: Системен компонент	Системни компоненти от Платформата.

3.3.1.6 ***Номенклатури***

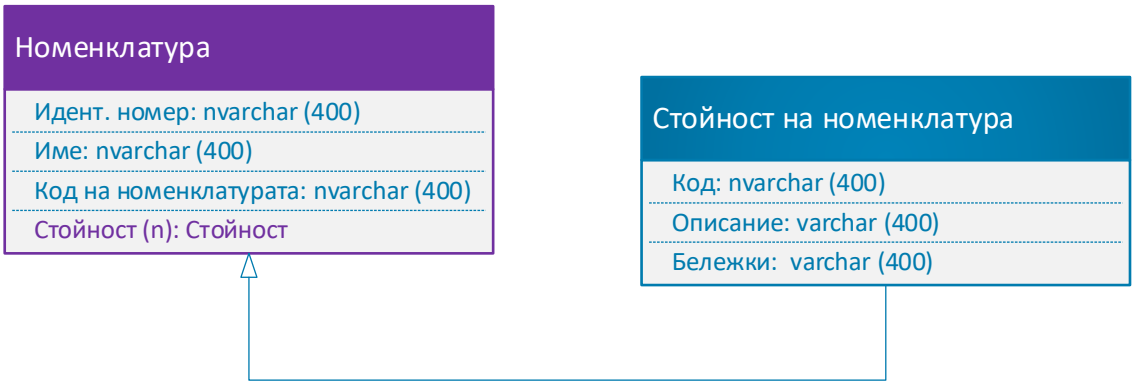


Таблица 7 Описание клас Номенклатури

Описание		
Тип	**Наименование/ Формат**	**Описание**
Подклас	Номенклатура	Номенклатури в системата

Атрибут	Уникален идентификатор: nvarchar (200)	Уникален идентификатор на Номенклатурата за системата
Атрибут	Наименование: nvarchar (200)	Наименование на Номенклатурата
Атрибут	Код: nvarchar (400)	Код на Номенклатурата
Подклас	Стойност (n): nvarchar (400)	Стойности на номенклатурата

3.3.1.7 Стойност на номенклатура

Таблица 8 Описание подклас Стойност на номенклатура

Описание		
Тип	**Наименование/Формат**	**Описание**
Подклас	Стойност на номенклатура	Стойности в номенклатурата
Атрибут	Описание: nvarchar (400)	Описание на номенклатурната стойност
Атрибут	Код: nvarchar (400)	Код на номенклатурната стойност
Атрибут	Бележки: nvarchar (400)	Бележки към номенклатурната стойност.

3.3.2 Модул за изпълнение на бизнес процеси ИБП

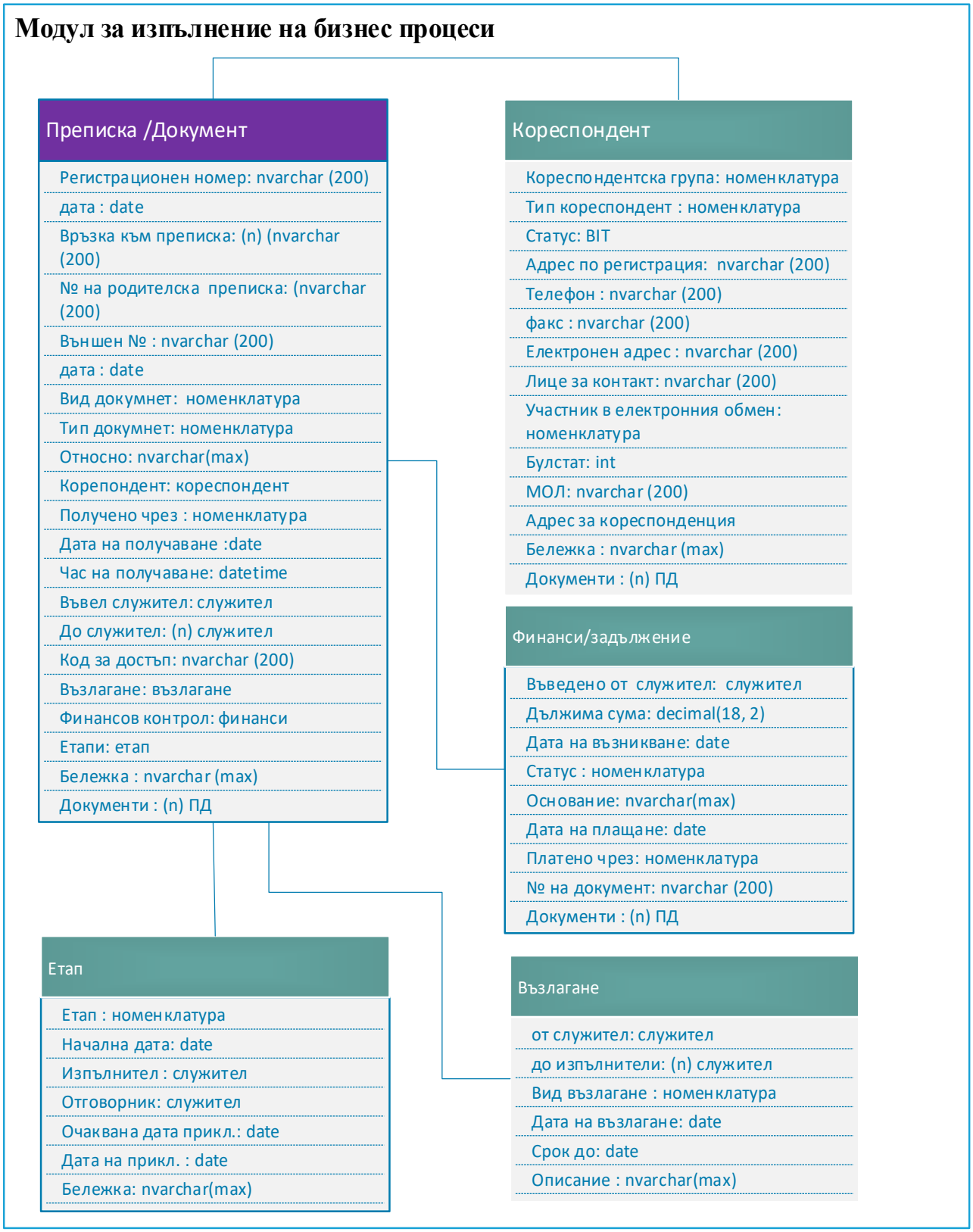
Модула за изпълнение на бизнес процесите позволява стартирането и изпълнението на инстанции на дефинираните бизнес процеси, базирани на правата на потребителите. Той позволява след автентикация и авторизация на потребителите, съобразно правата им да:

- Стартират нови инстанции на процеси;
- Виждат списък с разпределените им процеси;
- Получават нотификация за ново-разпределени към тях инстанции, промяна в статуса на съществуващи такива и за задачи;
- Филтрират, групират и търсят инстанции на процеси по дефинирани критерии;
- Изпълняват стъпки(бизнес операции) в една или няколко инстанции на процеси;

Прилагат се следните типове процеси:

- Цифровизация на всички входящи заявки, получени по традиционни канали;
- Процесите по предлагане на публична услуга за клиент;
- Процесите по предлагане вътрешна услуга за клиент/служител;
- Управление на използването, управлението и отчитането на активите на организацията;

- Управление на персонала чрез йерархичната структура.



Фигура 23 Модул за изпълнение на бизнес процеси

3.3.2.1 Преписка /Документ

Таблица 9 Описание клас Преписка /Документ

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Преписка /Документ	Преписка /Документ
Атрибут	Регистрационен номер: nvarchar (200)	Регистрационен номер автоматично се инкрементира от системата в зависимост от типа на документа
Атрибут	дата : date	дата на регистрация
Атрибут	Връзка към преписка: (n) (nvarchar (200)	Връзки към други преписки – извършва се от служителя
Атрибут	№ на родителска преписка: (nvarchar (200)	№ на родителска преписка под формата на връзка ако има такава – автоматично се задава от системата.
Атрибут	Външен № : nvarchar (200)	Външен № на регистрирания документ ако има такъв
Атрибут	дата : date	дата
Атрибут	Вид документ: номенклатура	Вид документ – номенклатура свързан с вида на АУ и прилежащите документи
Атрибут	Тип документ: номенклатура	Тип документ: входящ, изходящ, вътрешен.
Атрибут	Относно: nvarchar(max)	Относно:
Подклас	Кореспондент: кореспондент	Кореспондент
Атрибут	Получено чрез : номенклатура	Получено чрез
Атрибут	Дата на получаване :date	Дата на получаване
Атрибут	Час на получаване: datetime	Час на получаван
Подклас	Въвел служител: служител	Въвел служител
Подклас	До служител: (n) служител	До служител: (n)
Атрибут	Код за достъп: nvarchar (200)	Код за достъп – автоматично генериран код на достъп, който се изпраща на гражданите за да следят статуса по преписката
Подклас	Възлагане: възлагане	Възлагане
Подклас	Финансов контрол: финанси	Финансов контрол
Подклас	Етапи: етап	Етапи
Атрибут	Бележка : nvarchar (max)	Бележка свободен текст
подклас	Документи : (n) ПД	Документи : (n) ПД

3.3.2.2 ***Кореспондент***

Таблица 10 Описание подклас Кореспондент

Описание		
Тип	**Наименование/ Формат**	**Описание**
подклас	Кореспондент	Кореспондент
Атрибут	Кореспондентска група: номенклатура	Кореспондентска група: номенклатура
Атрибут	Тип кореспондент : номенклатура	Тип кореспондент : номенклатура
Атрибут	Статус: BIT	Статус: активен/неактивен
Атрибут	Адрес по регистрация: nvarchar (200)	Адрес по регистрация/лична карта
Атрибут	Телефон : nvarchar (200)	Телефон
Атрибут	факс : nvarchar (200)	факс
Атрибут	Електронен адрес : nvarchar (200)	Електронен адрес
Атрибут	Лице за контакт: nvarchar (200)	Лице за контакт
Атрибут	Участник в електронния обмен: номенклатура	Участник в електронния обмен: номенклатура – връзка със СЕОС и избор от участниците
Атрибут	Булстат: int	Булстат:
Атрибут	МОЛ: nvarchar (200)	МОЛ материално отговорно лице
Атрибут	Адрес за кореспонденция	Адрес за кореспонденция
Атрибут	Бележка : nvarchar (max)	Бележка : nvarchar (max)
подклас	Документи : (n) ПД	Документи : (n) ПД

3.3.2.3 ***Финанси***

Таблица 11 Описание подклас Финанси

Описание		
Тип	**Наименование/ Формат**	**Описание**
подклас	Финанси/задължение	Финанси/задължение
Подклас	Въведено от служител: служител	Служител въвел задължението

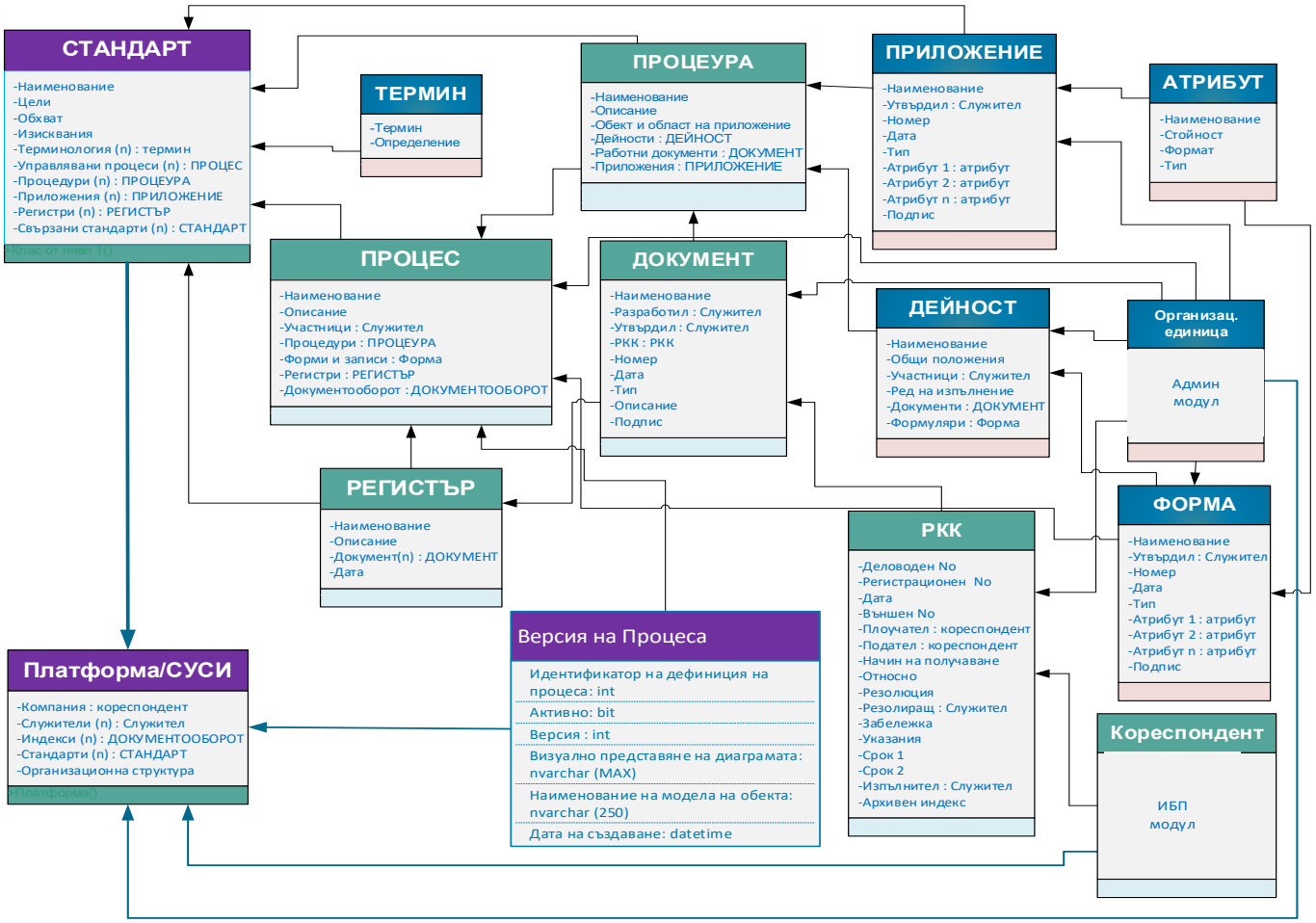
Атрибут	Дължима сума: decimal(18, 2)	Дължима сума в лева
Атрибут	Дата на възникване: date	Дата на възникване
Атрибут	Статус : номенклатура	Статус
Атрибут	Основание: nvarchar(max)	Основание – такса, ценоразпис описание
Атрибут	Дата на плащане: date	Дата на плащане
Атрибут	Платено чрез: номенклатура	Платено чрез:
Атрибут	№ на документ	№ на документ – фактура таксова бележка
подклас	Документи : (n) ПД	Документи : (n)
подклас	Възлагане	Възлагане
Подклас	от служител: служител	от служител
Подклас	до изпълнители: (n) служител	до изпълнители
Атрибут	Вид възлагане : номенклатура	Вид възлагане
Атрибут	Дата на възлагане: date	Дата на възлагане
Атрибут	Срок до: date	Срок за изпълнение
Атрибут	Описание : nvarchar(max)	Описание

3.3.2.4 Етап

Таблица 12 Описание подклас Етап

Описание		
Тип	**Наименование/Формат**	**Описание**
подклас	Етап	Етап
Атрибут	Етап : номенклатура	Етап : номенклатура
Атрибут	Начална дата: date	Начална дата:
Атрибут	Изпълнител : служител	Изпълнител
Подклас	Отговорник: служител	Отговорник
Атрибут	Очаквана дата прикл.: date	Очаквана дата приключване
Атрибут	Дата на прикл. : date	Дата на приключване
Подклас	Бележка: nvarchar(max)	Бележка

3.3.3 Модул СУСИ



Фигура 24 Модул СУСИ [62]

3.3.3.1 ***Платформа за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията СУСИ***

Таблица 13 Описание клас Платформа

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Платформа/СУСИ	Определящ клас за СУСИ
Атрибут	Компания: кореспондент	За да работи платформата за конкретна компания трябва да бъдат въведени данни те за компанията, които са от тип „кореспондент”.
Атрибут	Служители (n): Служител	Цели на международно признатия стандарт, съгласно описанието от неговата документация.
Атрибут	Индекси (n): Маршрут	Информация се структурира и класифицира, чрез стройна регистраторна система от индекси индивидуални за всеки процес и/или организационна структура. Всеки индекс се описва чрез модул ДУБП с информационен клас „Версия на процеса”, като по този начин се осигурява гъвкавост на информационните потоци, електронно моделиране на дейностите и динамичност на процесите.
Атрибут	Стандарти (n) : СТАНДАРТ	Платформата се изгражда чрез добавянето на n на брой основни класове „СТАНДАРТ” в зависимост от броя на стандартите, които компанията използва. Основния клас съдържа всички необходими за конкретния моделиран стандарт под класове с техните определители.
Подклас	Организационна структура: Организационна единица (n)	Дефинира организационната структура, чрез n боя служители

3.3.3.2 ***Клас Стандарт***

Таблица 14 Описание клас Стандарт

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Стандарт	Определящ клас за СУСИ
Атрибут	Наименование: nvarchar (400)	Наименование на международно признатия стандарт.
Атрибут	Цели: nvarchar (400)	Цели на международно признатия стандарт, съгласно описанието от неговата документация.

Атрибут	Обхват: nvarchar (400)	Обхват на международно признатия стандарт, съгласно описанието от неговата документация и дейността на компанията която е внедрила стандарта.
Атрибут	Изисквания: nvarchar (400)	Изисквания на международно признатия стандарт, съгласно описанието от неговата документация. Потребност или очакване, което е формулирано, обикновено се подразбира или е задължително.
Подклас	Терминология (n):	Подклас от общо ниво. n на брой в зависимост от броя на използваните термини в стандарта.
Подклас	Управлявани процеси (n):	Подклас от второ ниво. n на брой в зависимост от броя на управляваните процеси в стандарта. Съвкупност от взаимосвързани или взаимодействащи дейности, които превръщат входните елементи в изходни.
Подклас	Процедури (n):	Подклас от второ/трето ниво. n на брой в зависимост от броя на общите за стандарта процедури. Точно определен начин за осъществяване на дейност или процес.
Подклас	Приложения (n):	Подклас от четвърто ниво. n на брой в зависимост от броя на общите за стандарта приложения.
Подклас	Регистри (n):	Подклас от четвърто ниво. n на брой в зависимост от броя на общите за стандарта регистри.
Подклас	Свързани стандарти (n):	Подклас от общо ниво. n на брой в зависимост от броя на свързаните стандарти.

3.3.3.3 Клас „Термин”

Таблица 15 Описание клас Термин

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Термин	
Атрибут	Термин: nvarchar (200)	Термин съгласно документацията на стандарта
Атрибут	Определение: nvarchar (400)	Определение на термина, съгласно документацията на стандарта

3.3.3.4 *Клас „Регистър”*

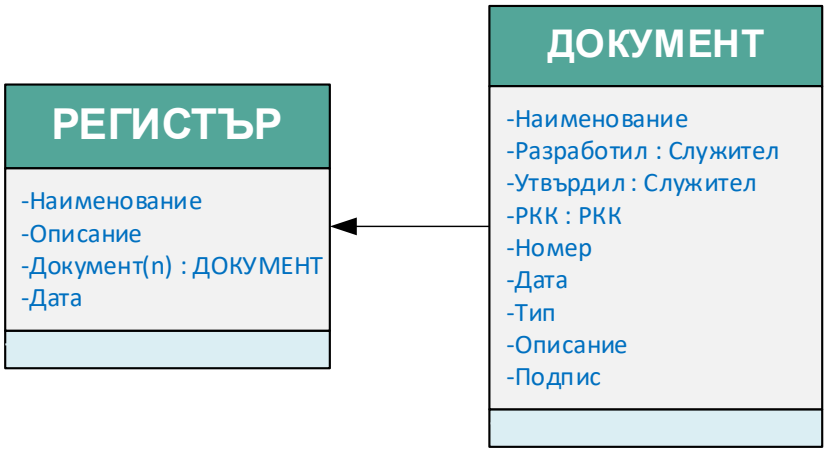


Таблица 16 Описание клас Термин

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Регистър	
Атрибут	Наименование: nvarchar (200)	Наименование на регистъра съгласно изискванията на конкретния стандарт
Атрибут	Описание: nvarchar (400)	Описание на регистъра съгласно документацията на стандарта
Подклас	Документ (n): Документ	Документи регистрирани в регистъра - n на брой – допълват се при развитието на регистъра
Атрибут	Дата: date	Дата на регистрация на документа

3.3.3.5 *Клас „Форма”*

Таблица 17 Описание клас Форма

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Форма	
Атрибут	Наименование: nvarchar (200)	Наименование на формата
Подклас	Утвърдил: Организационна единица	Служител утвърдил формата - Подклас „Организационна единица

Атрибут	Номер nvarchar (200)	Номер на формата
Атрибут	Дата: date	Дата на формата
Атрибут	Тип: nvarchar (200)	Тип на формата - номенклатура
Подклас	Атрибут (n): Атрибут	Чрез атрибутите се описват задължителните компоненти на формата . Чрез набор от атрибути се описва **записа** в стандарта.

3.3.3.6 Клас „Процедура”

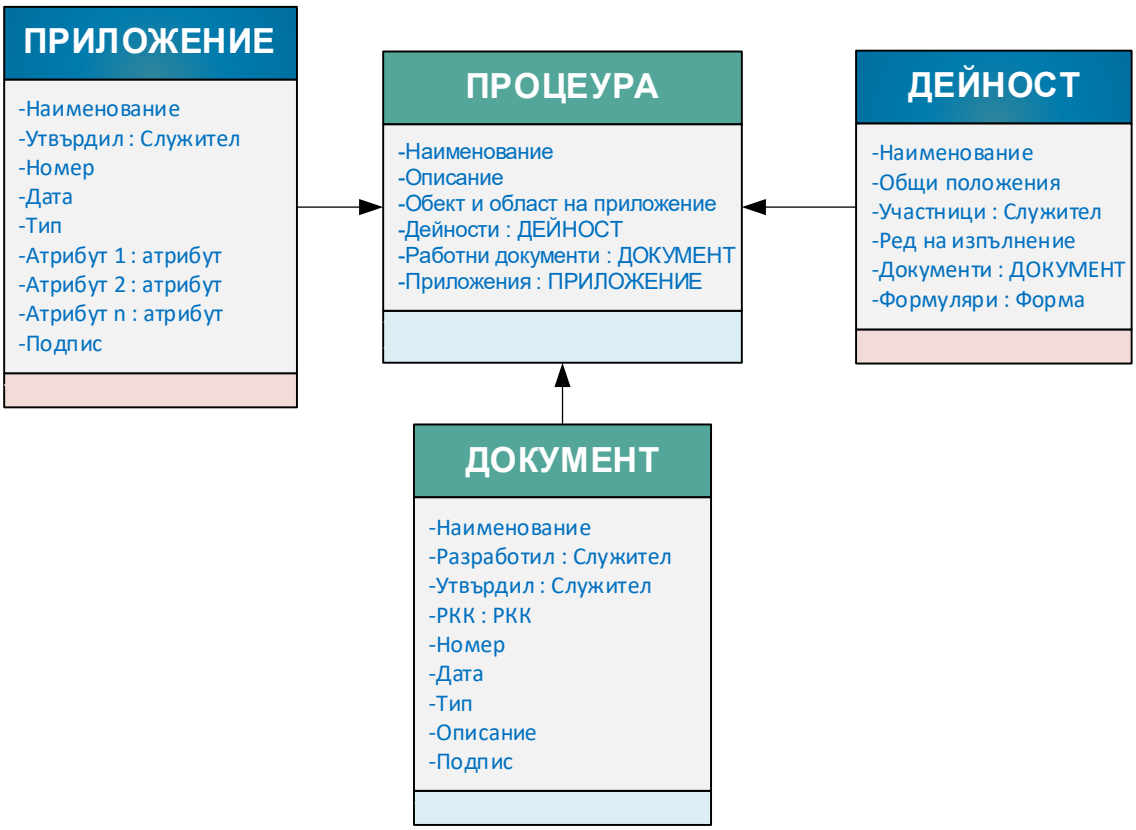


Таблица 18 Описание клас Процедура

Описание		
Тип	**Наименование /Формат**	**Описание**
Клас	Процедура	
Атрибут	Наименование: nvarchar (200)	Наименование на процедурата
Подклас	Описание: nvarchar (400)	Описание на процедурата, съобразно стандарта

Атрибут	Обект на приложение: nvarchar (400)	Обекта на приложение на процедурата, съобразно стандарта;
Подклас	Дейности (n): Дейност	Дейности необходими за изпълнението на процедурата n на брой.
Подклас	Работни документи (n): Документ	Работни документи свързани с процедурата Подклас „Документ” n на брой.
Подклас	Приложения(n): Приложение	Приложения към процедурата. Подклас „Приложение“ n на брой.

3.3.3.7 Клас „Процес”

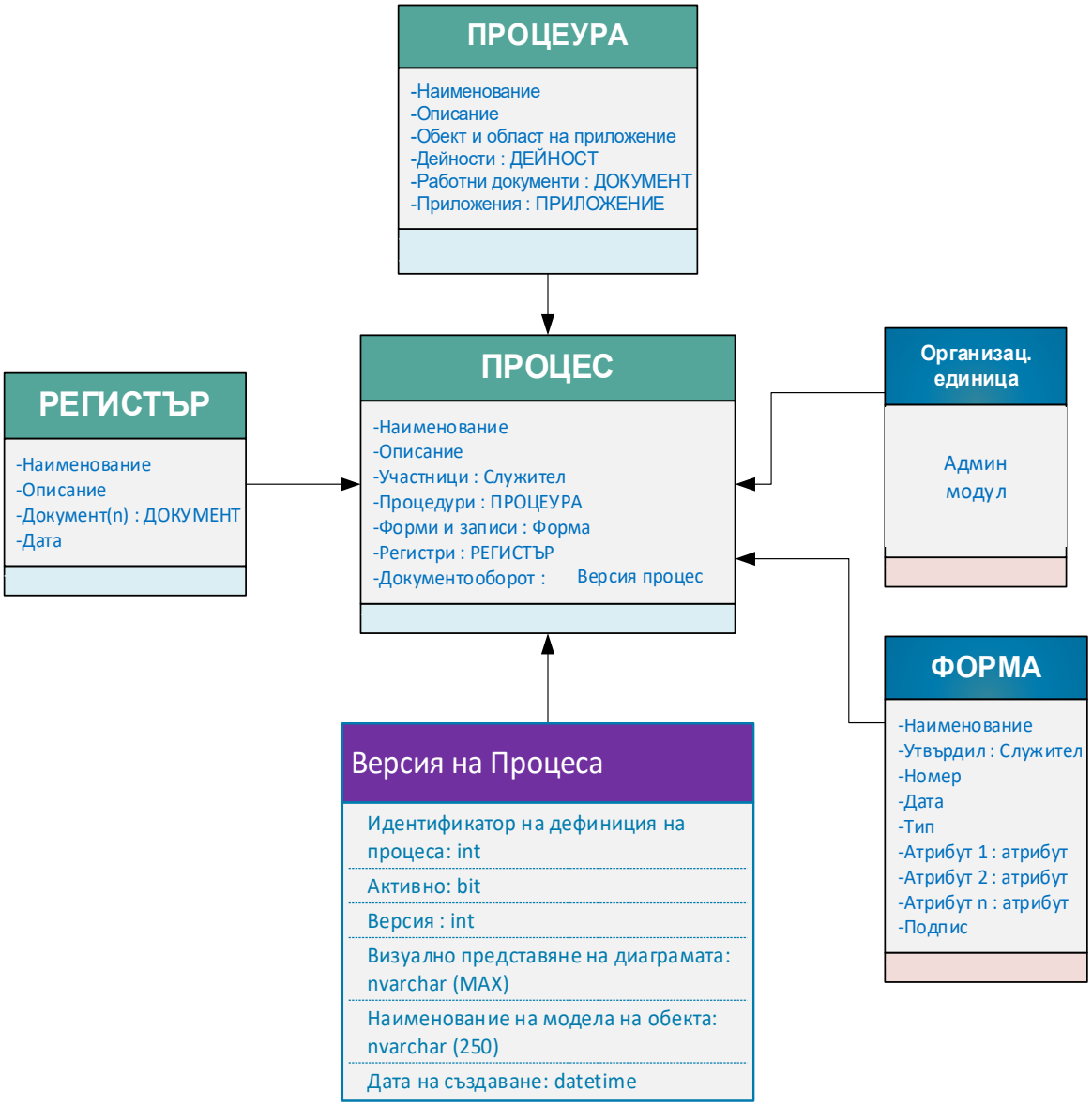


Таблица 19 Описание клас Процес

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Процес	
Атрибут	Наименование: nvarchar (200)	Наименование на процеса съгласно изискванията на конкретния стандарт
Атрибут	Описание: nvarchar (400)	Описание на процеса съгласно документацията на стандарта
Подклас	Участници(n): Организационна единица	Служители участници в процеса. Клас Организационна единица е описан в Административния модул
Подклас	Процедури (n): Процедура	Процедури за администриране и управление на процеса.
Подклас	Форми и записи (n): Форма	Форми и записи ползвани от процеса.
Подклас	Регистри (n): регистър	Регистри свързани с процеса
Подклас	Документооборот: Версия на процеса	Път на документите по процеса.

3.3.3.8 Клас „Документ”

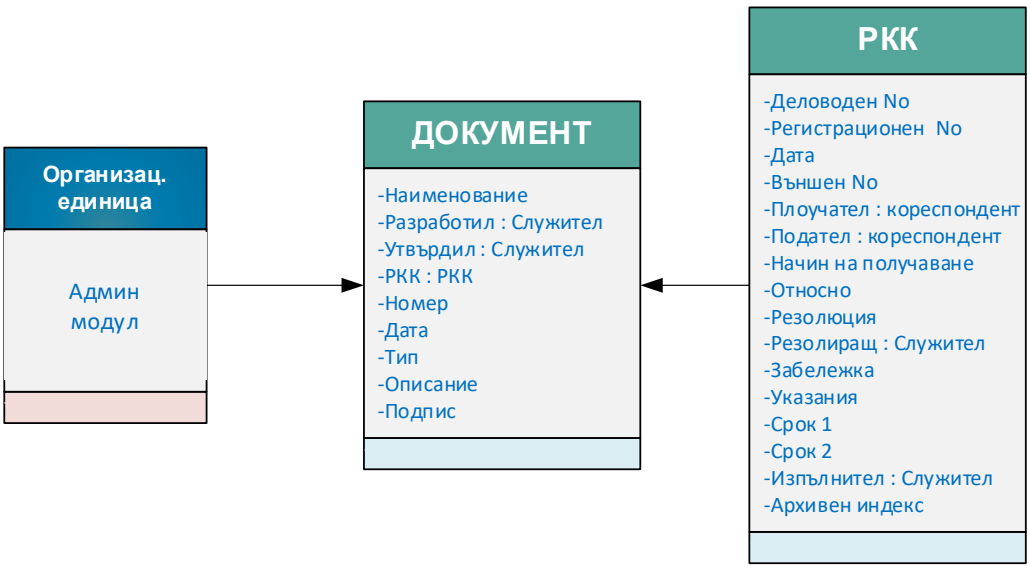


Таблица 20 Описание клас Документ

Описание		
Тип	**Наименование/**	**Описание**

	Формат	
Клас	Документ	
Атрибут	Наименование	Наименование на документа. Заглавие
Подклас	Разработил: Организационна единица	Разработил документа. Служител подклас от общо ниво.
Подклас	Утвърдил: Организационна единица	Утвърдил документа. Служител подклас от общо ниво.
Подклас	РКК: РКК	Регистрационно контролна карта. РКК - подклас от общо ниво.
Атрибут	Номер: nvarchar (200)	Регистрационен номер на документа
Атрибут	Дата: date	Дата на документа
Атрибут	Тип: nvarchar (200)	Тип на документа
Атрибут	Описание: nvarchar (200)	Описание. Съдържание на документа.
Атрибут	Подпис: nvarchar (200)	Поле за подписи на подписващите.

3.3.3.9 Клас „РКК” – Регистрационно контролна карта

Таблица 21 Описание клас РКК

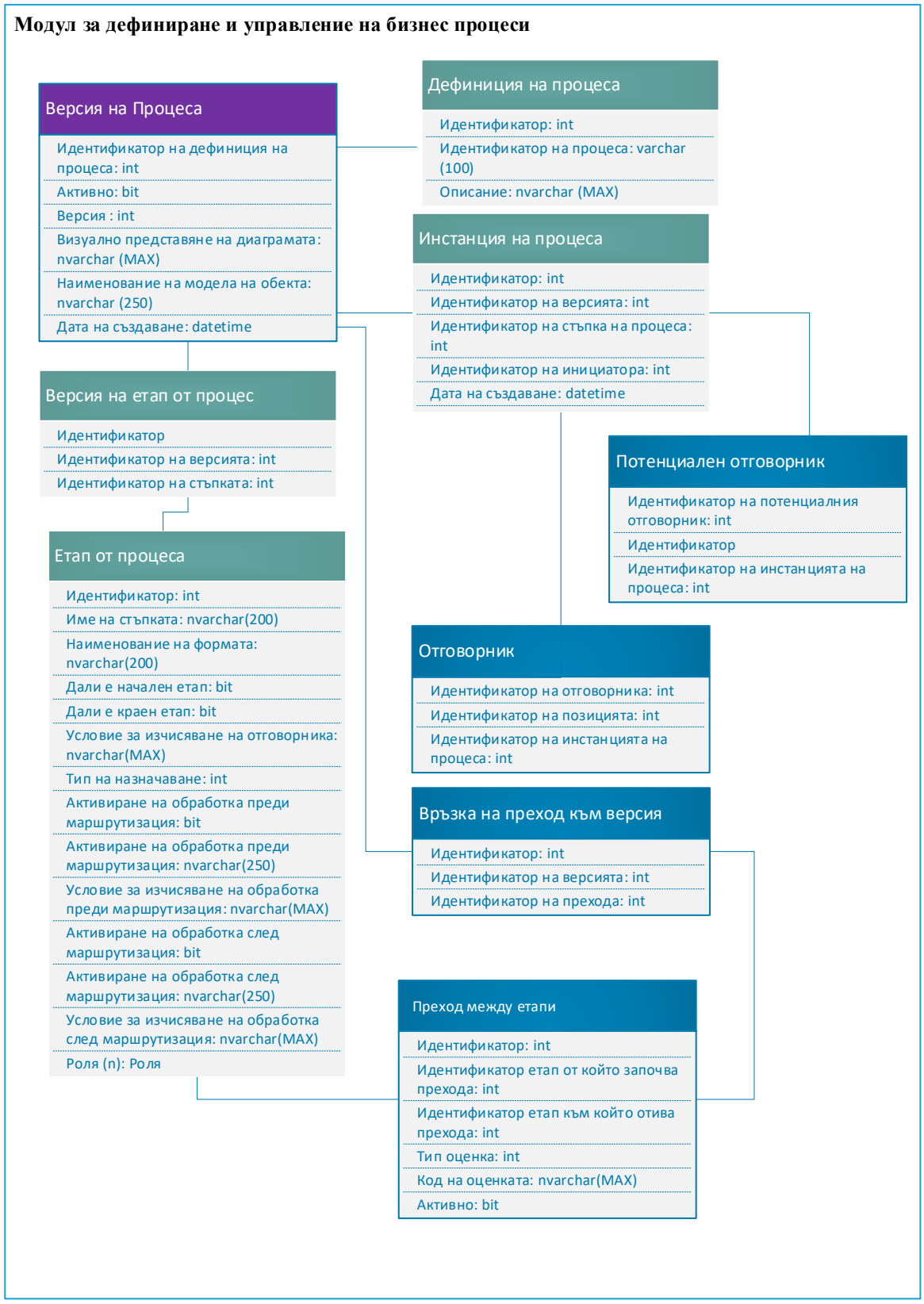
Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	РКК	Регистрационно контролна карта
Атрибут	Деловоден номер: nvarchar (200)	Деловоден номер на документа
Атрибут	Регистрационен номер: nvarchar (200)	Регистрационен номер. Ако има номер от регистър.
Атрибут	Външен номер: nvarchar (200)	Външен номер на документа Номер, който подателя е сложил
Атрибут	Дата: date	Дата на документа
Подклас	Получател: кореспондент	Получател – Юридическо или физическо лице от подклас „кореспондент”.

Подклас	Подател: кореспондент	Подател – Юридическо или физическо лице от подклас „кореспондент” от общо ниво
Атрибут	Начин на получаване: nvarchar (200)	Начин на получаване ако е входящ документа – номенклатура.
Атрибут	Относно: nvarchar (200)	Относно - Кратко описание на документа
Атрибут	Резолюция: nvarchar (200)	Резолюция - Обработка или направление на документа
Подклас	Резолиращ: Организационна единица	Резолиращ – служител извършил резолюцията; Подклас „Организационна единица ”
Атрибут	Забележка: nvarchar (200)	Забележка. Текстова бележка към документа.
Атрибут	Указания: nvarchar (200)	Указания - текстово поле към документа.
Атрибут	Срок 1: date	Срок 1 - срок за изпълнение или придвижване към следваща точка
Атрибут	Срок 2: date	Срок 2 - срок за изпълнение или придвижване към следваща точка
Подклас	Изпълнител: Организационна единица	Изпълнител по документа Подклас „Организационна единица ” .
Атрибут	Архивен Индекс: nvarchar (200)	Архивен Индекс – индекс на папката от архива, в която ще се прикачи документа.

3.3.4 Модул за дефиниране и управление на бизнес процеси ДУБП

Модула за дефиниране и управление на бизнес процеси позволява на оторизирани лица с право на достъп да дефинират и управляват бизнес процеси като позволява:

- Създаване на процеси;
- Промяна на процеси и управление на техните версии;
- Разгръщане (deployment) на процеси, както и тяхното деактивиране;
- Да взаимодейства със системата за управление на права така, че да се дефинират допустимите права и действия на потребителите, както достъпа им до определени информационни обекти, асоциирани към процеса;
- Да има възможност за автоматично пренасочване на процеса към определен потребител или група такива, на базата на таблици за решения и DMN или еквивалентни дефиниции.



Фигура 25 Модул за дефиниране и управление на бизнес процеси

3.3.4.1 Версия на Процеса

Таблица 22 Описание клас Версия на процеса

Описание		
Тип	**Наименование/Формат**	**Описание**
Клас	Версия на Процеса	Версия на Процеса
Атрибут	Идентификатор на дефиниция на процеса: int	Идентификатор на дефиниция на процеса
Атрибут	Активно: bit	Активно
Атрибут	Версия : int	Версия
Атрибут	Визуално представяне на диаграмата: nvarchar (MAX)	Визуално представяне на диаграмата
Атрибут	Наименование на модела на обекта: nvarchar (250)	Наименование на модела на обекта
Атрибут	Дата на създаване: datetime	Дата на създаване

3.3.4.2 Дефиниция на процеса

Таблица 23 Описание клас Дефиниция на процеса

Описание		
Тип	**Наименование/Формат**	**Описание**
Клас	Дефиниция на процеса	Дефиниция на процеса
Атрибут	Идентификатор: int	Идентификатор
Атрибут	Идентификатор на процеса: varchar (100)	Идентификатор на процеса
Атрибут	Описание: nvarchar (MAX)	Описание на процеса

3.3.4.3 Инстанция на процеса

Таблица 24 Описание клас Инстанция на процеса

Описание		
Тип	**Наименование/Формат**	**Описание**
Клас	Инстанция на процеса	Инстанция на процеса
Атрибут	Идентификатор: int	Идентификатор
Атрибут	Идентификатор на версията: int	Идентификатор на версията
Атрибут	Идентификатор на стъпка на процеса: int	Идентификатор на стъпка на процеса

Атрибут	Идентификатор на инициатора: int	Идентификатор на инициатора
Атрибут	Дата на създаване: datetime	Дата на създаване

3.3.4.4 Отговорник

Таблица 25 Описание клас Отговорник

Описание		
Тип	**Наименование/Формат**	**Описание**
Клас	Отговорник	Отговорник
Атрибут	Идентификатор на отговорника: int	Идентификатор на отговорника
Атрибут	Идентификатор на позицията: int	Идентификатор на позицията
Атрибут	Идентификатор на инстанцията на процеса: int	Идентификатор на инстанцията на процеса

3.3.4.5 Версия на етап от процес

Таблица 26 Описание клас Версия на етап

Описание		
Тип	**Наименование/Формат**	**Описание**
Клас	Версия на етап от процес	Връзка на версия към етап от процес
Атрибут	Идентификатор: int	Идентификатор
Атрибут	Идентификатор на версията: int	Идентификатор на версията
Атрибут	Идентификатор на стъпката: int	Идентификатор на стъпката

3.3.4.6 Етап от процеса

Таблица 27 Описание клас Етап

Описание		
Тип	**Наименование/Формат**	**Описание**
Клас	Етап от процеса	Етап/стъпка от процеса
Атрибут	Идентификатор: int	Идентификатор
Атрибут	Име на стъпката: nvarchar(200)	Име на стъпката
Атрибут	Наименование на формата: nvarchar(200)	Наименование на формата
Атрибут	Дали е начален етап: bit	Дали е начален етап
Атрибут	Дали е краен етап: bit	Дали е краен етап

Атрибут	Тип на назначаване: int	Тип на назначаване
Атрибут	Условие за изчисляване на отговорника: nvarchar(MAX)	Условие за изчисляване на отговорника
Атрибут	Активиране на обработка преди маршрутизация: bit	Активиране на обработка преди маршрутизация
Атрибут	Активиране на обработка преди маршрутизация: nvarchar(250)	Активиране на обработка преди маршрутизация
Атрибут	Условие за изчисляване на обработка преди маршрутизация: nvarchar(MAX)	Условие за изчисляване на обработка преди маршрутизация
Атрибут	Активиране на обработка след маршрутизация: bit	Активиране на обработка след маршрутизация
Атрибут	Активиране на обработка след маршрутизация: nvarchar(250)	Активиране на обработка след маршрутизация
Атрибут	Условие за изчисляване на обработка след маршрутизация: nvarchar(MAX)	Условие за изчисляване на обработка след маршрутизация

3.3.4.7 Преход между етапи

Таблица 28 Описание клас Преход между етапи

Описание		
Тип	**Наименование/Формат**	**Описание**
Клас	Преход между етапи	Преход между етапи
Атрибут	Идентификатор: int	Идентификатор
Атрибут	Идентификатор етап от който започва прехода: int	Идентификатор етап от който започва прехода
Атрибут	Идентификатор етап към който отива прехода: int	Идентификатор етап към който отива прехода
Атрибут	Тип оценка: int	Тип оценка
Атрибут	Код на оценката: nvarchar(MAX)	Код на оценката
Атрибут	Активно: bit	Активно

3.3.4.8 Връзка на преход към версия

Таблица 29 Описание клас Връзки на преход към Версия

Описание

Тип	Наименование/Формат	Описание
Клас	Връзка на преход към версия	Връзка на преход към версия на процес
Атрибут	Идентификатор: int	Идентификатор
Атрибут	Идентификатор на версията: int	Идентификатор на версията
Атрибут	Идентификатор на прехода: int	Идентификатор на прехода

3.3.4.9 Клас „Приложение”

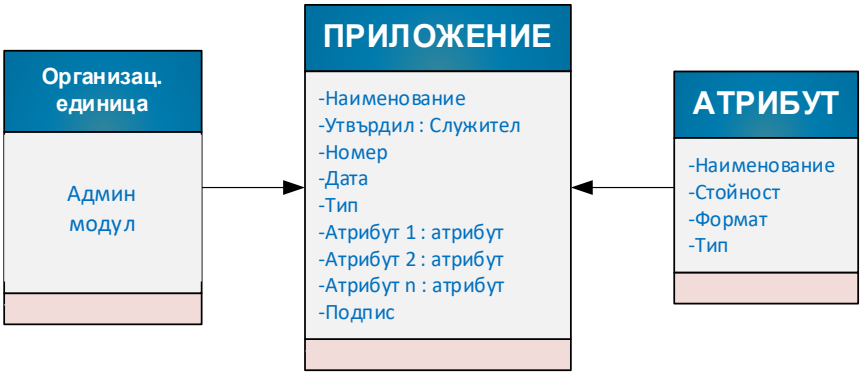


Таблица 30 Описание клас Приложение

Описание		
Тип	**Наименование/Формат**	**Описание**
Клас	Приложение	
Атрибут	Наименование: nvarchar (200)	Наименование на приложението. Заглавие.
Подклас	Утвърдил: Организационна единица	Служител утвърдил приложението
Атрибут	Номер nvarchar (200)	Номер на приложението
Атрибут	Дата: date	Дата на приложението
Атрибут	Тип: nvarchar (200)	Тип на приложението - номенклатура
Подклас	Атрибут (n): Атрибут	Чрез атрибутите се описват задължителните компоненти на формата .
Атрибут	Подпис: nvarchar (200)	Поле за подписи на подписващите.

3.3.4.10 Клас „Атрибут”

Таблица 31 Описание клас Атрибут

Описание		
Тип	**Наименование/Формат**	**Описание**
Клас	Атрибут	

Атрибут	Наименование: nvarchar (200)	Наименование на атрибута
Атрибут	Стойност: nvarchar (200)	Стойност на атрибута. Може да бъде избираема от предварително дефинирани стойности или свободен **запис.**
Атрибут	Формат: nvarchar (200)	Формат на атрибута. Всеки атрибут има предварително дефиниран формат - текст; число; дата; номенклатура
Атрибут	Тип: nvarchar (200)	Тип на атрибута - Автоматичен; Предефиниран; Чек бокс; Свободен

3.3.4.11 Клас „Дейност”

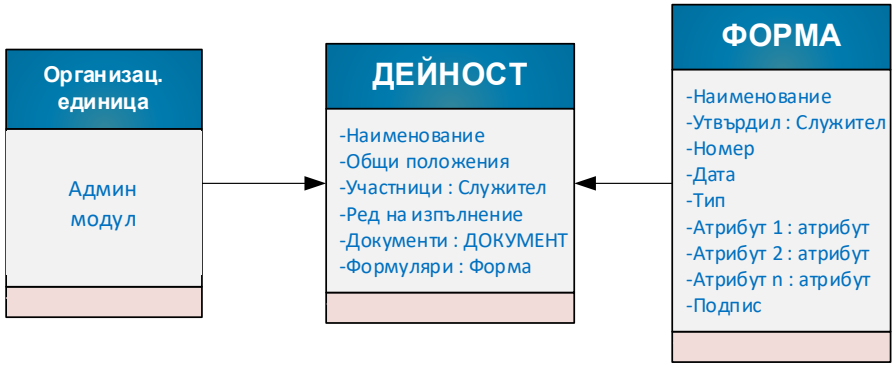
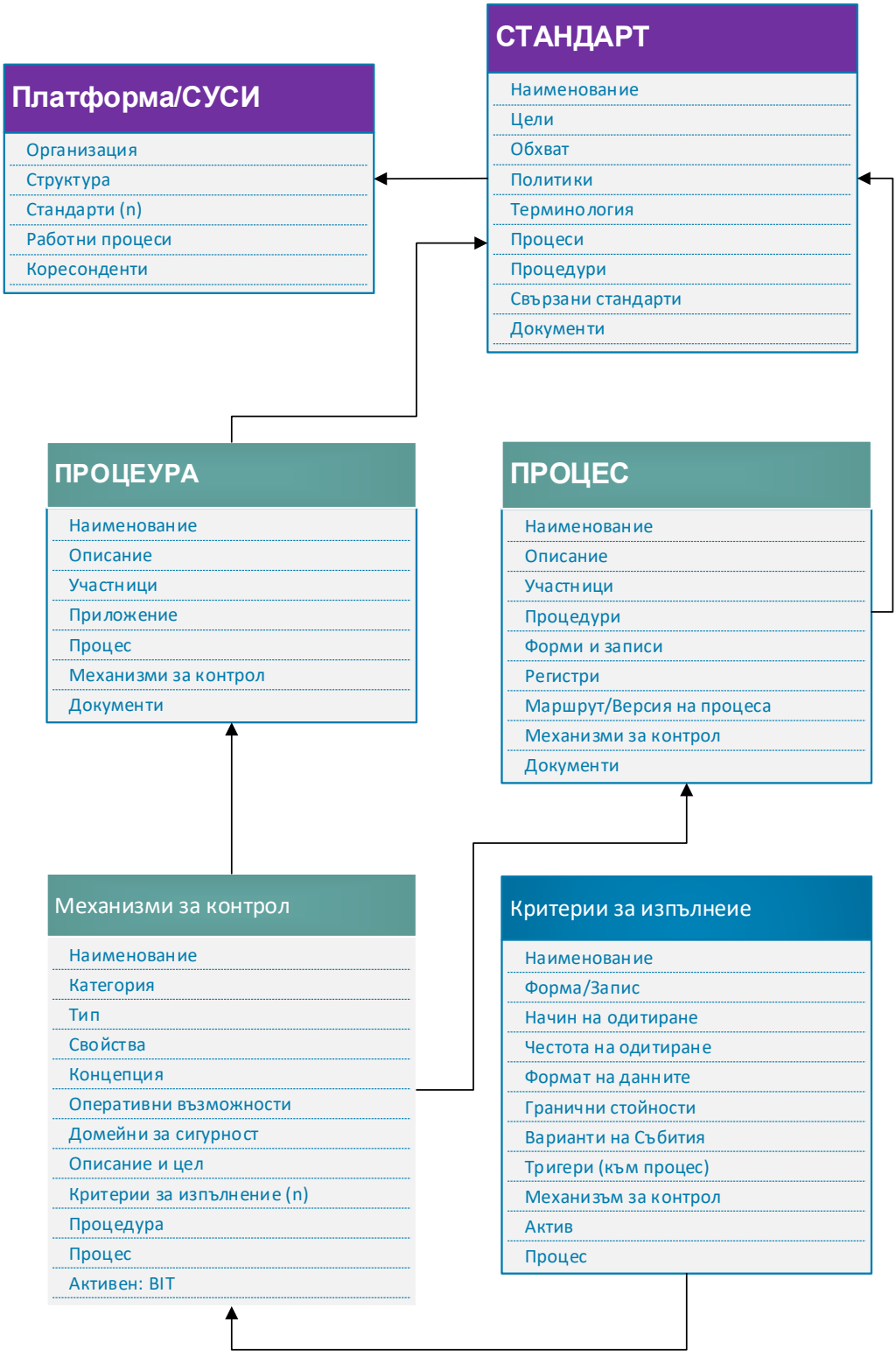


Таблица 32 Описание клас Дейност

Описание		
Тип	**Наименование/Формат**	**Описание**
Клас	Форма	
Атрибут	Наименование: nvarchar (200)	Наименование на дейността
Атрибут	Общи положения: nvarchar (400)	Общи положения и описание на дейността като част от процедурата;
Подклас	Участници: Организационна единица	Участници Служители участващи в дейността;
Атрибут	Ред на изпълнение: nvarchar (400)	Ред на изпълнение дейността. Описание на последователността на дейностите и отговорностите.
Подклас	Документи: Документ	Документи свързани с резултата, контрола и администрацията на дейността. Подклас „Документ” n на брой.
Подклас	Формуляри: Форма	Формуляри, свързани с резултата, контрола и администрацията на дейността Подклас „Форма” n на брой

3.3.5 Модул Одит и контрол



Фигура 26 Модул Одит и контрол

3.3.5.1 Клас „Механизми за контрол“

Таблица 33 Описание клас Механизми за контрол

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Механизми за контрол	Основен клас за администрация и контрол
Атрибут	Наименование: nvarchar (400)	Наименование на Механизма за контрол.
Атрибут	Категория: nvarchar (200)	Категория на механизма за контрол – номенклатура (Организационни; човешки ресурси; физически; технологични др.)
Атрибут	Тип: nvarchar (200)	Тип на механизма за контрол – номенклатура (превантивен, откриващ, коригиращ и др.)
Атрибут	Свойства (n): nvarchar (200)	Свойства за сигурност на информацията – номенклатура (поверителност/конфиденциалност, цялостност/интегритет, наличност и др.).
Атрибут	Концепция (n): nvarchar (200)	Концепции за киберсигурност – номенклатура (идентифициране, защита, откриване, реагиране, възстановяване и др.)
Атрибут	Оперативни възможности (n): nvarchar (200)	Оперативни възможности - Ръководене, Управление на активи Защита на информацията , Сигурност на човешките ресурси, Физическа сигурност, Сигурност на система и мрежа, Сигурност на приложенията, Сигурна конфигурация, Управление на идентичността и достъпа, Управление на заплахи и уязвимости, Непрекъснатост, Сигурност при взаимоотношения с доставчици, Законност и съответствие, Управление на събития свързани със сигурността на информацията, Осигуряване на сигурност на информацията и др.
Атрибут	Домейни за сигурност (n): nvarchar (200)	Домейни за сигурност - Ръководене и екосистема, Защита, Откриване, Устойчивост и др.
Атрибут	Описание и цели: nvarchar (400)	Описание на контролите и цели.
Атрибут	Критерии за изпълнение (n): Критерии за изпълнение	Асоциирани критерии за оценка на изпълнението на контролите
Подклас	Процедура: Процедура	Процедури към които е свързан механизъма за контрол
Подклас	Процеси (n): Процес	Процеси, които се изпълняват по механизъма за контрол
Атрибут	Активен: BIT	Атрибут за активиране/деактивиране на контрола

3.3.5.2 Клас „Критерии за изпълнение“

Таблица 34 Описание клас Критерии за изпълнение

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Критерии за изпълнение	Критерии за изпълнение на механизмите за контрол.
Атрибут	Наименование: nvarchar (400)	Наименование на критерия.
Подклас	Форма/запис: Форма	Форма/запис свързана с критерия.
Атрибут	Начин на одитиране: nvarchar (200)	Начин на проверка на критерия – номенклатура
Атрибут	Честота на одитиране: nvarchar (200)	Честота на извършване на проверка на параметрите по критерия
Атрибут	Формат на данните: nvarchar (200)	Формат на данните свързани с критерия
Атрибут	Гранични стойности: nvarchar (200)	Гранични стойности за наблюдения при които се реагира
Атрибут	Варианти на събития (n): nvarchar (200)	Събития които се отчитат от критерия
Атрибут	Тригери: nvarchar (400)	Тригери към процес в зависимост от настъпила гранична стойност или събитие.
Подклас	Механизми за контрол: Механизми за контрол	Механизми за контрол към които е свързан критерия.
Подклас	Процеси (n): Процес	Процеси, които се тригерират от критерия.
Атрибут	Активен: BIT	Атрибут за активиране/деактивиране на критерия

3.4 Архитектура

Платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията се реализира като централизирана уеб базирана система с архитектура ориентирана към услугите (SOA), комбинираща в себе си основните модули, които от своя страна използват инфраструктура от стандартизирани услуги за реализация на обработката за конкретните типове информация. [63]

Ориентираната към услуги архитектура (Service-oriented Architecture) е модел, специално предназначен да намали разходите, да увеличи гъвкавостта и да опрости представянето на бизнеса и операциите на различни части от дейността. Основен принцип на SOA е структурирането на бизнес дейностите в услуги, което дава възможност за тяхното бързо идентифициране и преизползване на вече съществуващите функционалности, както и избягване на дублирането им по време на

разработка. Стандартизацията на поведението на тези услуги води до ограничаване на неочакваните въздействия при промени, както и до успешното им прогнозиране и избягване. [64] Архитектура ориентирана към услугите (SOA) е съвкупност от независими софтуерни елементи, предоставящи като услуга софтуерна функционалност на други приложения. [65]

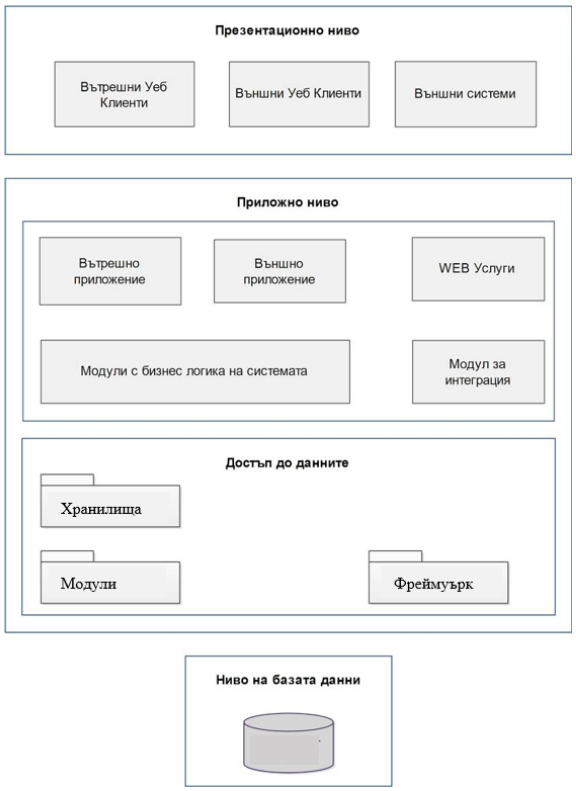
Основни предимства на SOA подхода:

- Независимост от доставчик, продукт или технология;
- Услугата е самостоятелна функционална единица. Услугите могат да бъдат комбинирани с други софтуерни приложения, за да се осигури пълна функционалност на по-голямо софтуерно приложение.

Платформата се реализира чрез използването на следните SOA стандарти:

- eXtensible Markup Language (XML) - за предоставяне на данни;
- Web Services Definition Language (WSDL) - за осигуряване на достъп до Web-услугите; [62]
- Simple Object Access Protocol (SOAP) – за обмяна на данни. [66]

3.4.1 Логическа архитектура



Фигура 27 Системна архитектура на реализацията на Платформата – трислойна архитектура MVC

Архитектура на платформата може да бъде декомпозирана на отделни слоеве (нива), комуникиращи помежду си по строго определени интерфейси. Основно предимство при този подход е, че позволява в отделните слоеве да бъдат извършвани

значителни промени без това да оказва влияние на останалите, което води до изключителна гъвкавост. Слоевете са определени така, че да групират елементите, които варират независимо. При централизираните системи доказан модел е разделянето на следните слоеве:

- Слой на базата данни;
- Слой на бизнес логиката;
- Слой на потребителския интерфейс (презентационен слой);

Всеки слой в последствие се декомпозира на отделни модули, като комуникацията между модулите се осъществява по строго специфицирани интерфейси. Разделението на ясно разграничени слоеве и обособяването на слоя на базата данни от слоевете на бизнес логиката позволява да се осигури възможността цялостното решение да бъде съвместимо както със съществуващата инфраструктура в организацията, така и с виртуална инфраструктура. [67]

3.4.1.1 Слой за достъп до базата данни

Задачата на слоя за достъп на базата данни е да обслужва и съхранява данните на информационната система. Слоя за управление на данните се реализира на базата на механизъм за поддържане на обектно- релационни съответствия. Използването на подход за автоматизирано поддържане на съответствията между информационни обекти и релационната база данни осигурява няколко основни предимства:

- Функционалността за съхраняване на данните става независимо от спецификата на съхраняващото базата данни СУБД;
- Промените в структурата на информационните обекти може да бъде автоматично отразена в релационния модел;
- Допълнителния слой на абстракция позволява по голяма гъвкавост по отношение на физическия модел на данните – т.е. улеснява скалирането на базата данни и евентуалното му разпределяне в повече бази данни;
- Осигурява се пълна поддържка на транзакции на ниво на слоя за достъп до данните, като така се гарантира изпълнението на заявката към базата данни на приложението, да отговарят на изискванията:
    - Atomicity – атомарност (при грешка се отменят всички заявки от транзакцията, за да е успешна транзакцията са изпълнени всички заявки от нея);
    - Consistency – цялост на данните след всяка изпълнена транзакция;
    - Isolation – изолация на данните по отношение на други транзакции;
    - Durability – стабилност на транзакцията, липса на възможност за загуба на данни.

Основното предимство на модела се изразява във възможността да не се влага логика в услугите използващи съдържанието на базата данни, тъй като слоя до данните му дава нужните методи и отделя със слой на абстракция по-ниските нива на работа с информационните обекти и базата данни. [68]

Слоя за достъп до данните съхранява електронно съдържание в релационната база данни. Базата данни се проектира предвид следните аспекти:

- Възможност за ефективна работа с големи обеми от данни;
- Възможност за осигуряване на ефективен механизъм за резервиране на данните;
- Високо ниво на сигурност.

3.4.1.2 Слой на бизнес логиката

Функцията на слоя на бизнес логиката е да обработва заявките за обработка получени от интерфейса на системата, да поддържа тяхната валидност спрямо идентифицираните бизнес процеси и правила и да осигури управлението на потока от данни, съобщения, и документи, свързани с работата на платформата, като ги съхранява и извлича от слоя за достъп до данните. Според логическата архитектура на системата в слоя с бизнес логиката се разполагат всички модули, функции и процедури, които реализират функционалността на системата. [69]

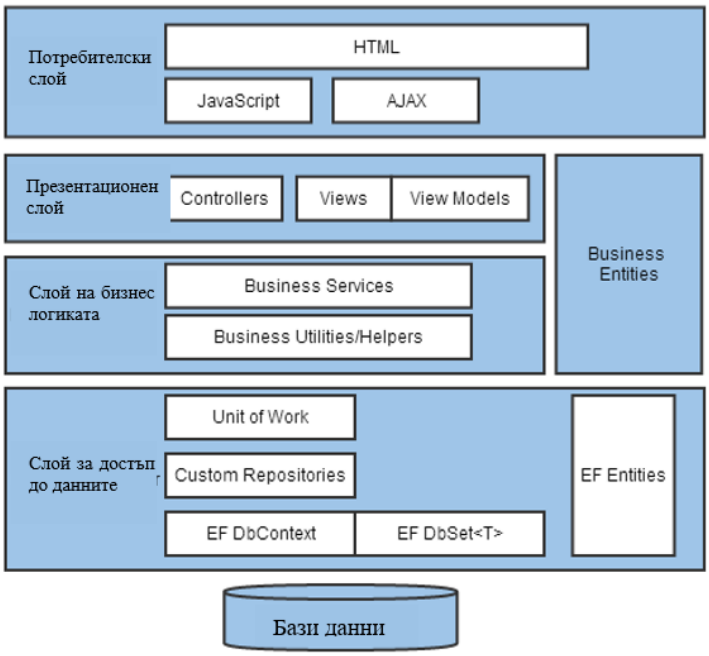
Реализацията на слоя на бизнес логиката включва набор от отделни компоненти които изграждат това ниво:

- От гледна точка на по-добра сигурност и гъвкавост на платформата вътрешната и външната част на приложението се обособяват като отделни приложения, които дават достъп до различна част от функционалността на системата, но се реализират използвайки общата основа от модули и общ модел на данните, така че да се улесни максимално бъдещото развитие и на двете части на системата;
- Бизнес логиката за дефиниране, изпращане, обобщаване и представяне на информацията се реализира съгласно обектно ориентирания подход в гранулярно дефинирани независими компоненти – модули на системата, които си взаимодействат спрямо дефинирани между тях интерфейси. В допълнение се реализира модул за интеграция с външни системи, който позволява обмен на данни и изпълнение на части от функционалността на модулите на бизнес логиката при интеграция със системите.

3.4.1.3 Слой на потребителския интерфейс

Задачата на слоя на потребителският интерфейс е да взаимодейства с потребителите на системата, така че да обслужва техните заявки и да представя необходимата им информация в определения формат. В този слой се организира и използва интерфейса на системата, от потребителите, за да извършват желаната от тях работа. Въведените данни в този слой се подават на слоя на бизнес логиката за

последващата им обработка и съхранение в базата данни. Той се реализира от шаблона за дизайн Модел – изглед – контролер (Model-View-Controller /MVC/).



Фигура 28 Многослойна Архитектура

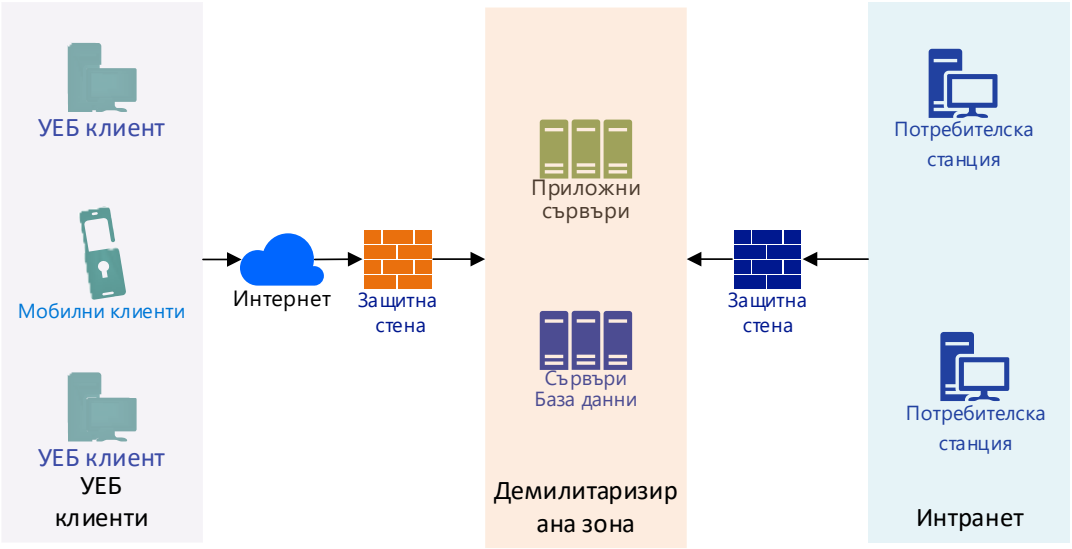
Контролерите, които посрещат заявките на потребителите ги предават за обработка към бизнес логиката, попълват необходимите данни във екраните и връщат съответният изглед, който предоставя визуализация на потребителския интерфейс. За реализирането на богат и удобен за работа потребителски интерфейс, който не изисква постоянно презареждане от сървъра изгледа, който се рендира в браузъра се реализира, като се използва библиотеката за динамично уеб съдържание. [70]

Прилагането на MVC парадигмата осигурява следните преимущества:

- **Преизползваемост на компонентите**. Разделението на модела от изгледа позволява компонентите на модела да бъдат преизползваеми за различни изгледи.
- **Скалируемост.** Моделът осигурява както хоризонтална, така и вертикална скалируемост. Позволява промяна на броя потребители, транзакции, обръщения към системата. Функционалността на системата може да бъде променена, без промени във всички слоеве
- **Гъвкавост.** Моделът осигурява лесната заменяемост на отделните слоеве като поддържа обособеност на отделните нива и следи да еднопосочност на връзките между тях. Определя и входно – изходни точки между слоевете

3.4.2 Физическа архитектура

Платформата се базира на гъвкава архитектура, която ще може да се разгръща както в физическа среда, така и във виртуализирана (облачна) среда, или друго хибридно решение.



Фигура 29 Физическа архитектура

Платформата се адаптира към съществуващата хардуерна, мрежова и приложна среда в организацията, като има два основни физически компонента:

- Приложен сървър, изпълняващ заявките към уеб приложението на системата, чрез който потребителите работят със системата.
- Сървър за управление на базите данни на системата.

Съображенията за максимално добро обособяване и осигуряване на информационна сигурност предопределят отделяне на сървърите в т. нар. DMZ или „демилитаризирана зона“ – зона от мрежата, която е изолирана от останалите части на вътрешната мрежа, отделена от външната среда с външна защитна стена, но и с вътрешна защитна стена, така че евентуален пробив да не доведе до риск за сървъра с приложението на системата или сървъра съхраняващ неговите бази данни. [71]

3.5 Основни изводи към Глава 3

- Въвежда се авторската теория за **Документна матрица**, като основа за оперативно управление на компанията и концептуалния модел на Платформата.
- Съобразно описаната методика за моделиране е изграден модел на Платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията.
- Предложена е логическа и физическа архитектура за реализация на платформата.
- UML кода на модела е представен в **Приложение 5 (Plant UML)**
- Реализацията на Платформата по модули с Python в ООП стил е представено **в Приложение 6.**
- Реализацията на базата данни е дадена в **Приложение 7** ORM (Object-Relational Mapping) реализация чрез (SQL Alchemy стандарт в Python).

4. ОСНОВНИ ИЗВОДИ И ЗАКЛЮЧЕНИЯ

4.1 Научни и научно-приложни приноси

4.1.1 Научни приноси

- Предложени са алгоритъм и методология за изследване и моделиране на автоматизирана стандартизирана платформа за управление на сигурността на информацията;
- Представена е авторската теория за **документна матрица**, като основа за оперативно управление на организация и компания.

4.1.2 Научно-приложни приноси

- Представен е анализ на системите за управление на сигурността на информацията в аспекти: Сигурността на информацията; Стандартите за информационна сигурност; Системите за управление на сигурността на информацията СУСИ; Софтуерните приложения за ИС.
- Определени, дефинирани и анализирани са работни процеси и потоци, които подлежат на автоматизация чрез разработваната платформа;
- Дефинирани са функционалните и нефункционалните изисквания след извършено изследване и анализ на данните, на потребителските групи и на стандартите за информационна сигурност;
- Идентифицирани са общите характеристики на системата, с използването на евристични методи;
- Разработен е модел на комплексна платформа за **моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията.** Модела се базира на мониторинг, анализ и управление на документната матрица, работните процеси и информационните потоци и активи на организацията.
- Предложена е архитектура на платформата, която е в съответствие със съвременните изисквания за модулност, автоматизация и съвместимост със стандарти.

4.2 Насоки за бъдещи изследвания

Постигнатите резултати в дисертационната работа очертават следните насоки за бъдещи изследвания:

- Развитие на Платформата с интеграция с изкуствен интелект, който анализира:
    - Информационните единици и записи;
    - Системните, програмни и комуникационни логове;
    - Информацията генерирана от критериите по контролите.
- Въз основа на извършените анализи с АИ могат да се доразвият

функционалностите на платформата в аспекти:

- Предлагане на оптимизация на СУСИ;
- Показване на аномалии параметри и активности извън норма;
- Изчисляване на вероятностни събития и предвижда рискови фактори. [72]

- Системите за управление на сигурността на информацията могат да се моделират с невронни мрежи, управлявани от Платформата. Това е подход за повишаване на ефективността и ефикасността на критични системи за управление на информационната сигурност.
- Генеративната неконтролирана невронна мрежа - машина на Болцман (Boltzmann Machine) използва техники върху входните данни за анализиране на нормалните състояния на СУСИ, за да предвиди нежеланите ситуации. Международно признатите стандарти определят набор от контроли за сигурност за наблюдение, одит и управление на СУСИ. Те са разпределени в категории и всяка от тях има стандартизирани атрибути. Невронните единици на машината на Болцман са базирани на инфраструктурата за контрол на сигурността на СУСИ. [73] [74] [75] [76]
- Интегрирането на невронни мрежи в СУСИ може значително да подобри способността на организацията да открива, прогнозира и реагира на аномалии в сигурността. НМ се използват до голяма степен в почти всички области на информационната и киберсигурност, но за моделиране на поведението на СУСИ като цялостна сложна система, те са иновативен метод за намаляване на разходите и времето, както и за предотвратяване или смекчаване на щетите. [77] [78] [79]

4.3 Апробация на резултатите

Основните резултати, получени при разработката на дисертационната работа, са докладвани в три публикации и на специализирани международни конференции.

4.3.1 Статии и цитирания

1. Velev T., Dobrinkova N., “Unified innovative Platform for administration and automated management of internationally recognized standards”, Book Title: “Digital Transformation, Cyber Security and Resilience of Modern Societies”, book series “Studies in Big Data”, Springer. DOI:10.1007/978-3-030-65722-2_5, eBook ISBN: 978-3-030-65722-2, ISBN: 978-3-030-65721-5, (https://www.scopus.com/pages/publications/85129091048) ISSN: 2197-6503, 2021, vol. 84, p. 61 – p. 75
2. Velev T, “Heuristic essentials for modeling and optimization of a platform for automation and management of standardized information security management systems”, 28–29 October 2021, Sofia, Bulgaria, 2021 Big Data, Knowledge and Control Systems,

Engineering (BdKCSE) IEEE | DOI: 10.1109/BDKCSE53180.2021.9627263, ISBN:978-1-6654-1042-7, https://ieeexplore.ieee.org/document/9627277;

3. Velev T., Dobrinkova N., "The logical model of unify, innovative Platform for Automation and Management of Standards (PAMS)" 1st International Scientific Conference Digital Transformation, Cyber Security and Resilience" DIGILIENCE2019, Sofia 2-4 October 2019. ISIJ Digital Transformation, Cyber Security and Resilience, ISSN 0861-5160 (print), ISSN 1314-2119 (online), vol. 43, no. 1 (2019): 113-120, 2019, p.113-p.120 https://doi.org/10.11610/isij.4310
   - Citation 1: Wang, Z., Guan, X., Zeng, Y., Liang, X. and Dong, S., "Utilizing data platform management to implement "5W" analysis framework for preventing and controlling corruption in grassroots government". Heliyon Volume 10, Issue 7, 15 April 2024, e28601, DOI: 10.1016/j.heliyon.2024.e28601, 2024 (Scopus referenced: https://www.scopus.com/pages/publications/85188751354)

4.3.2 Конференции

- International Conference on Big Data, Knowledge and Control Systems Engineering BdKCSE'2018, (21-22 November 2018), доклад: "Unified innovative Platform for administration and automated management of internationally recognized standards"
- DIGILIENCE 2019: Digital Transformation, Cyber Security and Resilience Central Military Club Sofia, Bulgaria, October 2-4, 2019, доклад: "The logical model of unify, innovative Platform for Automation and Management of Standards (PAMS)"

4.3.3 Проекти

Част от изследванията в дисертационния труд са от проект № BG161PO003-1.1.06–0036-C0001 "Унифицирана платформа за администрация автоматизация и управление на международно признати стандарти", изпълняван в сътрудничество от екипите на **Перфект Плюс ЕООД (ръководител Тодор Велев) и ИИКТ – БАН (ръководител Светозар Маргенов).** Проектът е за индустриално изследване на високотехнологичен иновативен продукт в областта на информационните технологии с продължителност 22 месеца.

Голяма част от резултатите са апробирани в проект „Разработка и въвеждане в експлоатация на Единна система за управление, контрол и анализ на дейностите (ЕСУКАД) за нуждите на Българския институт по метрология (БИМ)", ръководен от Тодор Велев.

Благодарности

Изказвам своята благодарност на научният си ръководител проф. д-р Нина Добринкова, за ценни напътствия, професионална компетентност и съдействие при подготовката на дисертационния труд. Благодаря за помощта и съветите на колегите от ИККТ на БАН и от Solent University Southampton .

Декларация за оригиналност

Декларирам, че дисертацията съдържа оригинални резултати, получени при проведени от мен научни изследвания с подкрепата и съдействието на научния ми ръководител.

Резултатите, които са получени, описани и/или публикувани от други учени са коректно и подробно цитирани в библиографията.

Настоящият дисертационен труд не е прилаган за придобиване на научна степен в друго висше училище, университет или научен институт.

Подпис:…….

Приложения

Приложение 1 Основна терминология в стандартизацията:

- **Международна стандартизация** - стандартизация, в която могат да участват съответните **органи** на всички страни;
- **Регионална стандартизация -** стандартизация, в която могат да участват съответните органи на страни само от един географски, политически или икономически регион в света;
- Национална стандартизация - стандартизация, която се извършва на равнището на една определена страна;
- Основен документ - документ, който дава правила, насоки или характеристики за дейности или резултати от тях;
- Стандарт - документ, създаден чрез консенсус и одобрен от признат орган, който определя за общо и повтарящо се прилагане правила, насоки или характеристики за дейности или техните резултати за постигане на оптимален ред в дадена съвкупност от обстоятелства;
- Международен стандарт - стандарт, който е приет от международна организация по стандартизация или от международна организация с дейност по стандартизация и е общодостъпен;
- Регионален стандарт - стандарт, който е приет от регионална организация по стандартизация или от регионална организация с дейност по стандартизация и е общодостъпен;
- Национален стандарт - стандарт, който е приет от национален орган по стандартизация и е общодостъпен;
- Предварителен стандарт - документ, приет за временно прилагане от орган с дейност по стандартизация и е общодостъпен, за да може да се натрупа необходимият опит при неговото прилагане, на основата на който ще бъде разработен стандарт;
- Кодекс за добра практика - документ, който препоръчва начини на действие или процедури за проектиране/разработване, производство, монтаж, поддържане или използване на технически средства, конструкции или продукти;
- Орган с дейност по стандартизация - орган, който извършва признати дейности в областта на стандартизацията;
- Орган по стандартизация - орган с дейност по стандартизация, признат на национално, регионално или международно равнище, чиято основна функция според статута му е подготовката, одобряването или приемането на стандарти, които са общодостъпни;
- Национален орган по стандартизация - орган по стандартизация, признат на

национално равнище, на който е дадено право да бъде национален член в съответни международни и регионални организации по стандартизация;

- Основен стандарт - стандарт, който е с общо предназначение или съдържа общи предписания за определена област;
- Терминологичен стандарт - стандарт, който се отнася за термини, обикновено придружени с техните определения и понякога с обяснителни бележки, илюстрации, примери и т.н;
- Стандарт за изпитване - стандарт, който се отнася за методи за изпитване, понякога придружен от други предписания, отнасящи се до изпитването, като вземане на проби, използване на статистически методи, последователност на изпитването;
- Стандарт за продукт - стандарт, който определя изискванията, на които трябва да отговаря даден продукт или група продукти, за да се осигури неговата (тяхната) пригодност за използване по предназначение;
- Стандарт за процес - стандарт, който определя изискванията, на които трябва да отговаря един процес, за да бъде осигурена неговата пригодност за използване по предназначение;
- Стандарт за услуга - стандарт, който определя изискванията, на които трябва да отговаря една услуга, за да бъде осигурена нейната пригодност за използване по предназначение;
- Задължителен стандарт - стандарт, прилагането на който е задължително по силата на закон от общ характер или на безусловно позоваване в наредба;
- Позоваване на стандарти (в нормативен акт) - Препращане към един или повече стандарти вместо включване на техни конкретни предписания в нормативен акт;
- **Международно признати стандарти**

Международният стандарт е документ, установен от призната международна организация за стандартизация, като например Международната организация по стандартизация (ISO) или Международната електротехническа комисия (IEC). Тези стандарти служат за уеднаквяване на спецификации на продукти, безопасност и качество в различни страни по света, като по този начин улесняват международната търговия и подпомагат сътрудничеството между компании от различни държави. Те могат да включват технически изисквания, методи за тестване, правила за работна среда, и много други аспекти в различни индустрии. Международните стандарти се разработват чрез съгласие между експерти от различни страни, които представляват заинтересованите страни, като правителства, индустрия, научни институции, и потребители. Този процес гарантира, че стандартите отразяват общи интереси, технологични иновации и добри практики на глобално ниво.

Главна задача на международните организации за стандартизация (ISO, IEC) е да съдействат за развитието на стандартизацията и свързаните с нея дейности с цел

улесняване на международния търговски обмен със стоки и услуги; укрепване на сътрудничеството в интелектуалната сфера, в научната, техническата и икономическата дейност. Международните стандарти се разработват от експерти от техническите комитети на ISO/IEC. Международен стандарт се счита за приет, само ако е одобрен от 75 % от членуващите организации.

- **Европейските стандарти**

Европейските стандарти са инструмент за поддържане на интересите на обществото и са важен фактор в подкрепата на законодателството. Европейската комисия и Съветът признават стандартите като средство за оценяване и доказване на съответствието. Те предприемат действия за подпомагане и засилване на европейската стандартизация като инструмент, който обслужва политиката и целите на общността и укрепва Общия пазар, повишава конкурентността, улеснява прилагането на постиженията на науката и технологиите и подпомага търговията. Решението на Съвета за ролята на стандартизацията от 28 октомври 1999 г. (OJ C 141/01 от 2000 г.) призовава държавните власти и страните-членки да окажат необходимото съдействие на стандартизационния процес, особено когато стандартизацията е в подкрепа на политиката на общността или на обществения интерес.

- **Хармонизиран стандарт**

Хармонизиран стандарт е европейски стандарт (EN), разработен по мандат на Европейската комисия и Европейската асоциация за свободна търговия (EFTA), който поддържа съществените изисквания на директивите от нов подход. Прилагането на хармонизираните стандарти е доброволно, но е най-лесният начин за доказване на съответствието на продуктите със съществените изисквания на директивите. Обяснението за връзката между хармонизирания стандарт и за кои от съществените изисквания на директивите се прилага е дадено в приложение към всеки стандарт, разработен по мандат.

За да станат хармонизирани стандарти, е необходимо страните членки да преведат заглавията на стандартите на техния национален език, да ги изпратят чрез административните центрове на CEN/CENELEC на Европейската комисия и секретариата на EFTA за публикуване в Официалния вестник (Official Journal) на Европейския съюз. С този акт европейските стандарти, разработени по мандат, стават хармонизирани стандарти. От датата на публикуване тези стандарти могат да се прилагат за доказване на съответствието на продуктите с директивите.

- **Оценяване на съответствието**

Оценяване на съответствието е всяка дейност (вземане на проби, изпитване, сертификация и контрол), чиято цел е да се докаже, че даден продукт, процес, услуга, система, лице или орган отговарят на определени изисквания. Тези изисквания, както и процедурите за оценяване на съответствието, вземането на проби, методите за изпитване са разработени в международни, европейски или национални стандарти, ръководства или други нормативни документи. Оценяването на съответствието се

осъществява чрез систематично изследване степента на съответствие на даден продукт, процес или услуга. Изискванията могат да бъдат по отношение на безопасност, опазване на здравето и околната среда или по отношение на определени характеристики, свързани с качеството. Оценяването на съответствието може бъде задължително, когато това е уредено с нормативен акт и е свързано с безопасността и опазване на здравето и околната среда, или доброволно - за доказване на качеството на продукт, процес или услуга.

Целта е потребителите да са сигурни, че продуктите, процесите, услугите или системите са в съответствие с определени изисквания, което ги прави по-добре приети на пазара.

Стандартите предоставят възможност за широко прилагане и признаването им като основа при оценяване на съответствието. Като се отчитат добрите практики, те са подходящи за използване от всички заинтересувани страни, в т.ч. оценяване и доказване на съответствието както от производителя (декларация за съответствие), така и от трета независима страна (орган за сертификация).

Приложение 2 Сертификационни (одитиращи) организации

Сертификационни компании със световен обхват.

В различните държави развиват дейност по сертификация по международно признати стандарти фирми с акредитации от службите по акредитации членки на IAF. В таблицата по-долу са посочени сертифициращи компании с интернационален обхват, изпълняващи дейност в различна географска дислокация. [38]

✓ Managing For Quality
✓ Abacus Quality Training Services Inc
✓ Abbassi Ltd AO17482
✓ Accredited Certification International Ltd (ACI)
✓ AFNOR Groupe
✓ AJA Academy
✓ BM TRADA
✓ BSCIC Certifications Pvt. Ltd
✓ BSI Training
✓ Bureau Veritas Certification
✓ Capable People
✓ Cavendish Scott, Inc.
✓ CMC International (UK) Ltd
✓ DNV GL Business Assurance
✓ EQMS India PVT. LTD.
✓ Esenek Training Centre
✓ European Quality Assurance
✓ Ferriby Marine
✓ Gablesmead Ltd
✓ Genesys Training
✓ GlobalGROUP Of Companies Limited
✓ Guardian Independent Certification Pte Ltd
✓ Hermes Infotech Inc.
✓ Hong Kong Veritas Ltd
✓ ICS Technologies
✓ Independent European Certification Limited
✓ Indian Institute of Quality Management
✓ Inspired Pharma Training Ltd
✓ Integrated Management Systems Associates Ltd
✓ International Register Training Institute
✓ Intertek
✓ IQCS Certification Sdn Bhd

✓ IQMS
✓ Irish Quality Centre
✓ ISOQAR Egypt Ahmed Mahmoud & Part. Co.
✓ ISOQAR Limited
✓ JAD Associates
✓ Kelmac Group Limited
✓ KPMG Audit Plc
✓ Lloyd's Register Quality Assurance Ltd
✓ Maximus International
✓ Neville-Clarke International Pte Ltd
✓ Nigel Bauer & Associates
✓ NQA Training
✓ NSF Health Sciences
✓ PERA
✓ Perry Johnson Inc
✓ qSkills GmbH & Co. KG
✓ Qualico (UK) Ltd
✓ Quality Austria Gulf
✓ Reading Scientific Services Ltd
✓ Resource Inspections Canada Incorporated
✓ Robere & Associates (Thailand) Ltd
✓ SGS United Kingdom Ltd
✓ SOGEA/RINA Training Factory
✓ SQMC Ltd
✓ Standard Management Certification Co., Ltd.
✓ TCB Cert. Worldwide LLC
✓ TEC Transnational
✓ The Quality Partnership
✓ TMS Insight (Training & Development) Ltd
✓ TUV Asia Pacific Limited
✓ TUV Rheinland Akademie GmbH
✓ Verité
✓ VOREST AG
✓ Worldwide Responsible Accredited Production (WRAP)

Сертификационни компании с най-голяма популярност, опериращи на европейски пазар.

✓ Lloyd's Register Quality Assurance Ltd

✓ Nigel Bauer & Associates
✓ BSI Training
✓ SGS United Kingdom Ltd
✓ Intertek
✓ AJA Academy
✓ Gablesmead Ltd
✓ TUV Rheinland Akademie GmbH
✓ TUV Asia Pacific Limited
✓ VOREST AG
✓ DNV GL Business Assurance
✓ Bureau Veritas Certification
✓ Hermes Infotech Inc.
✓ NSF Health Sciences
✓ qSkills GmbH & Co. KG

Сертификационни организации на Българския пазар

✓ ABS Quality Evaluations, Inc.
✓ ACM Limited
✓ AQ Cert Ltd.
✓ AFNOR Certification
✓ Bureau Veritas Certification
✓ Център за Изпитване и Европейска Сертификация ЕООД
✓ Certification Association "Russian Register"
✓ Certification International (UK) Ltd.
✓ CERTIND
✓ CSB Ltd.
✓ DAS Certification Ltd.

✓ DQS GmbH
✓ Европейска Сертификация България ЕООД
✓ Евросертификейшънс България ЕООД
✓ Евросертификейшънс ЕООД
✓ Ен Джи Ен ООД
✓ Ес Пи Ди Серт ЕООД
✓ ESC CERT GmbH
✓ ETSC SA
✓ EURO CERT
✓ for you Cert GmbH
✓ Germanischer Lloyd Certification GmbH
✓ Intertek
✓ Интернешънал Сертификейшънс България ЕООД
✓ IQA Ltd.
✓ Lloyd's Register Quality Assurance (LRQA)
✓ OHMI EuroCert GmbH
✓ QMS Certification Services Pty Ltd
✓ RINA
✓ Сертификация ЕАД
✓ СЖС България ЕООД
✓ SystemCERT Zertifizierungsgesellschaft
✓ T-Серт s.r.o.
✓ Transpacific Certifications Limited.
✓ ТЮФ Рейнланд България ЕООД
✓ United Registrar of Systems Ltd. (URS)
✓ Верификация ЕООД

Приложение 3 Изследване на данните

Изследване на данните свързани с механизмите за контрол

Организационни механизми за контрол

№	Описание	Тип и формат на данните
1	Политики за сигурност на информацията	Неструктурирани Документи
2	Роли и отговорности за сигурност на информацията	Структурирани Номенклатура Служител
3	Разпределение на задълженията	Структурирани Номенклатура Служител
4	Отговорности за управление	Структурирани Номенклатура Служител
5	Контакт с овластените органи	Структурирани Служител
6	Контакт с групи със специални интереси	Структурирани Служител
7	Събиране на сведения за заплахите	Структурирани Неструктурирани Документи Данни
8	Сигурност на информацията в управлението на проекти	Неструктурирани Документи
9	Опис на информацията и други свързани активи	Структурирани Данни
10	Допустимо използване на информация и други свързани активи	Структурирани Номенклатура
11	Връщане на активи	Структурирани Данни
12	Класификация на информацията	Структурирани Номенклатура
13	Етикетиране на информация	Структурирани Номенклатура
14	Пренос на информация	Структурирани Неструктурирани

№	Описание	Тип и формат на данните
		Документи Данни Служител
15	Контрол на достъпа	Структурирани Данни Служител
16	Управление на идентичността	Структурирани Данни Служител
17	Информация за автентификация	Структурирани Данни Служител
18	Права за достъп	Структурирани Данни Служител
19	Сигурност на информацията при взаимотношения с доставчици	Структурирани Неструктурирани Документи Данни
20	Поддържане на сигурността на информацията в рамките на споразуменията с доставчици	Структурирани Неструктурирани Документи Данни
21	Управление на сигурността на информацията във веригата на доставки на ИКТ	Структурирани Неструктурирани Документи Данни
22	Мониторинг, преглед и управление на промените в услугите на доставчика	Структурирани Неструктурирани Документи Данни
23	Сигурност на информацията при ползване на услуги в облак	Структурирани Данни
24	Планиране и подготовка за управление на инциденти, свързани със сигурността на информацията	Неструктурирани Документи

№	Описание	Тип и формат на данните
25	Оценяване и вземане на решения относно събития, свързани със сигурността на информацията	Структурирани Неструктурирани Документи Данни
26	Реагиране на инциденти, свързани със сигурността на информацията	Структурирани Неструктурирани Документи Данни
27	Извличане на поука от инцидентите, свързани със сигурността на информацията	Структурирани Неструктурирани Документи Данни
28	Събиране на доказателства	Структурирани Неструктурирани Документи Данни
29	Сигурност на информацията по време на прекъсване	Структурирани Неструктурирани Документи Данни
30	Готовност на ИКТ за непрекъснатост на бизнеса	Структурирани Неструктурирани Документи Данни
31	Правни, законови, регулаторни и договорни изисквания	Неструктурирани Документи
32	Права върху интелектуалната собственост	Структурирани Неструктурирани Документи Данни
33	Защита на записи	Структурирани Неструктурирани Документи Данни
34	Право на неприкосновеност на личния живот/лична неприкосновеност и защита на ЛИИ	Структурирани Неструктурирани Документи Данни

№	Описание	Тип и формат на данните
35	Независим преглед на сигурността на информацията	Структурирани Неструктурирани Документи
36	Съответствие с политики, правила и стандарти за сигурност на информацията	Структурирани Неструктурирани Документи
37	Документирани оперативни процедури	Структурирани Неструктурирани Документи

Механизми за контрол на човешките ресурси

№	Описание	Тип на Данните
38	Скрининг	Структурирани Данни Документи Служител
39	Условия за наемане на работа	Структурирани Данни Служител
40	Осъзнаване, образование и обучение в областта на сигурността на информацията	Структурирани Данни Документи Служител
41	Дисциплинарен процес	Структурирани Данни Документи Служител
42	Отговорности след прекратяване или промяна на трудовото правоотношение	Структурирани Данни Документи Служител
43	Споразумения за поверителност или неразкриване на информация	Структурирани Данни Документи Служител
44	Дистанционна работа	Структурирани Данни Документи

№	Описание	Тип на Данните
		Служител
45	Докладване на събития свързани със сигурност на информацията	Структурирани Данни Документи Служител

Механизми за контрол за физическа сигурност

№	Описание	Тип на Данните
46	Периметри за физическа сигурност	Структурирани Данни Документи
47	Физическо влизане	Структурирани Данни Документи Служител
48	Обезопасяване на офиси, стаи и съоръжения	Структурирани Данни Документи
49	Мониторинг на физическата сигурност	Структурирани Неструктурирани Данни Документи Служител
50	Защита срещу физически заплахи и заплахи от околната среда	Структурирани Неструктурирани Данни Документи Служител
51	Работа в защитени зони	Структурирани Неструктурирани Данни Документи Служител
52	Чисто бюро и чист екран	Структурирани Данни Документи Служител

№	Описание	Тип на Данните
53	Разположение и защита на оборудването	Структурирани Данни Документи
54	Сигурност на активи извън организацията	Структурирани Данни Документи
55	Носители за съхранение на информация	Структурирани Данни
56	Поддържащи комунални услуги	Структурирани Данни Документи
57	Защита на окабеляването	Структурирани Данни Документи
58	Поддръжка на оборудването	Структурирани Данни Документи
59	Сигурно ликвидиране или повторна употреба на оборудването	Структурирани Данни Документи

Технологични механизми за контрол

№	Описание	Тип на Данните
60	Потребителски крайни устройства	Структурирани Данни Служител
61	Права за привилегирован достъп	Структурирани Данни Служител
62	Ограничаване на достъпа до информация	Структурирани Данни Служител
63	Достъп до изходния код	Структурирани Данни Служител
64	Сигурна автентификация	Структурирани Данни Служител

№	Описание	Тип на Данните
65	Управление на капацитета	Структурирани Неструктурирани Данни Документи
66	Защита срещу зловреден софтуер	Структурирани Неструктурирани Данни Документи
67	Управление на технически уязвимости	Структурирани Неструктурирани Данни Документи
68	Управление на конфигурация	Структурирани Неструктурирани Данни Документи
69	Изтриване на информация	Структурирани Неструктурирани Данни Документи
70	Маскиране на данни	Структурирани Данни
71	Предотвратяване на изтичането на данни	Структурирани Данни Документи
72	Резервиране на информацията	Структурирани Данни
73	Резервиране на средствата за обработване на информация	Структурирани Данни
74	Регистриране (Влизане в системата)	Структурирани Данни
75	Дейности по мониторинг	Структурирани Неструктурирани Данни Документи
76	Синхронизация на часовника	Структурирани Данни
77	Използване на привилегировани спомагателни програми	Структурирани Данни Документи

№	Описание	Тип на Данните
78	Инсталиране на софтуер върху операционни систем	Структурирани Данни Документи
79	Сигурност на мрежите	Структурирани Данни
80	Сигурност на мрежовите услуги	Структурирани Данни Документи
81	Разделяне на мрежи	Структурирани Данни
82	Уеб филтриране	Структурирани Данни
83	Използване на криптография	Структурирани Данни
84	Жизнен цикъл на сигурно разработване	Структурирани Данни Документи
85	Изисквания за сигурност на приложението	Структурирани Данни Документи
86	Архитектура на сигурни системи и принципи на инженеринга	Структурирани Данни Документи
87	Сигурно кодиране	Структурирани Данни Документи
88	Тестване на сигурността при разработване и приемане	Структурирани Данни Документи
89	Разработване от външни изпълнители	Структурирани Данни Документи
90	Разделяне на средите за разработване, тестване и производство	Структурирани Данни
91	Управление на промените	Структурирани Неструктурирани Данни Документи
92	Информация за тестването	Структурирани Неструктурирани

№	Описание	Тип на Данните
		Данни Документи
93	Защита на информационните системи по време на одитно тестване	Структурирани Неструктурирани Данни Документи

Изследване на данни свързани с функционалните изисквания за Платформата

Документалистика и архивистика

№	Описание	Тип и вид на Данните
1	Документ (реквизити) – входящ, изходящ, вътрешен с функции: информационна, комуникативна, управленска и функция.	Структурирани Данни Документи Номенклатури
2	Съхранение на документ	Структурирани Данни Документи
3	Архивиране на документ - процес, индекси, параметри.	Структурирани Данни Документи Номенклатури
4	Регистрация на документ - процес, индекси, параметри.	Структурирани Данни Документи Служител Номенклатури
5	Кореспонденти кореспондентски групи	Структурирани Данни Физически – юридически лица Номенклатури
6	Класификация на документи	Структурирани Данни Номенклатури
7	Сроков контрол	Структурирани Данни Номенклатури

№	Описание	Тип и вид на Данните
8	Документооборот – автоматизирана маршрутизация на документите, съобразно моделираните, работни процеси.	Структурирани Данни Номенклатури Служител
9	Моделиране на организационната структура – организационни звена, длъжности, служители	Структурирани Данни Номенклатури Служител
10	Анализ на работните процеси	Структурирани Данни
11	Контрол на изпълнението	Структурирани Данни Документи Служител Номенклатури

Администриране

№	Описание	Тип и вид на Данните
12	Управление на достъпа и оторизация. Матрица за управление на достъпа Списъци за управление на достъпа (ACL) Управление на достъпа според способностите (ACC) Ролево-базирано управление на достъпа (RBAC) Базирано на правила управление на достъпа (PBAC) Задължителен контрол на достъпа (Mandatory Access Control - MAC) Контекстно-базиран контрол на достъпа (Context-Based Access Control - CBAC) Потребителски-базиран контрол на достъпа (Uuser-Based Access Control - UBAC)	Структурирани Данни Документи Номенклатури
13	Съхранение на данните – хранилище на данни, база данни.	Структурирани Данни Документи

№	Описание	Тип и вид на Данните
14	Архивиране на данните.	Структурирани Данни Документи Номенклатури
15	Бекъп на данните.	Структурирани Данни Документи Номенклатури
16	Възстановяване на системата след срив или инцидент.	Структурирани Данни Документи Номенклатури
	Управление на потребители	Структурирани Данни Документи Номенклатури
17	Управление на шаблони и образци	Структурирани Данни Документи Номенклатури
18	Управление на дефиниции и на срокове	Структурирани Данни Документи Номенклатури
19	Управление на номенклатури	Структурирани Данни Документи Номенклатури
20	Конфигурация на платформата	Структурирани Данни Документи Номенклатури
21	Мониторинг и анализ на системата	Структурирани Данни Документи Номенклатури
	Управление на базата от данни	Структурирани Данни Документи Номенклатури

Комуникация

№	Описание	Тип и вид на Данните
22	Управление и мониторинг на комуникационните сървиси между модулите на системата	Структурирани Данни Параметри
23	Управление и мониторинг на комуникационните сървиси с външни системи	Структурирани Данни Документи
24	Управление и параметризация на системната среда за вътрешна комуникация и нотификация на потребителите	Структурирани Данни Документи Номенклатури
25	Комуникационни образци и шаблони	Структурирани Данни Документи Номенклатури
26	Маршрутизация на съобщенията, съобразно субординацията в организацията.	Структурирани Данни Документи Номенклатури

Приложение 4 Актуалност и промяна на документите и управление на записите.

Актуалност на документите

Системите за управление на сигурността на информацията са съставени от множество документи, чийто брой често надхвърля цифрата 100. Големият брой води до трудности при осигуряването на **актуалност на документите**, особено при по-големи организации и фирми.

Документацията на СУСИ включва различни видове документи - наръчник, процедури, инструкции, формуляри. Всеки документ се отнася за различен аспект от системата и притежава собствени отличителни белези, които показват неговата **идентификация** и **статус**. Всеки документ от системата за управление има наименование, за какво се отнася, коя е поредната версия, дата на влизане в сила на документа. Един от често срещаните проблеми е актуалността на документа към настоящия момент и дали не е извършена промяна след датата на влизане в сила на документа.

Регистъра на документите от системата за управление дава информация за текущото съдържание на документите от системата и тяхната актуалност. Той съдържа необходимата информация, включваща:

- идентификация - код или съкращение за обозначаване на документите;
- наименование на документа;
- версия, редакция, изменение или друго обозначение на статуса на документа;
- дата на влизане в сила.

В началото при разработването на системата за управление е лесно, защото на всеки документ се поставя версия 1 от датата на нейното внедряване. Но в процеса на работа на организацията се налагат промени по различни причини - разширяване на обхват, закупуване на ново оборудване, промяна в нормативни изисквания, внедряване на нови системи и др. Независимо обаче от вида на промяната, отразяването й е свързано с изменение на документите от системата за управление. Това е моментът, в който възниква проблема с актуалността на документите.

След извършване на първата промяна без списъка с документите, не може да се управлява системата, защото в него се отразява всяка промяна в документите и той съдържа информация за актуалния статус на всеки един от тях.

На базата на информацията в списъка упълномощените служители от организацията ще имат възможността да проверяват статуса на използваните от тях документи и при възникнали несъответствия да сигнализират.

Освен това регистърът помага при разпространението на документите от системата за управление. С цел предпазване от използване на невалидни документи,

те се изтеглят от употреба и на тяхно място се предават новите и актуални към момента документи. За целта трябва да се знае кои документи с кои да се заменят, а това най-ясно се вижда от списъка с документите от системата за управление. Така лесно се проследява коя версия на документите е разпространена и коя е актуалната към момента и се гарантира, че "на местата за използване е налична подходящата версия на приложимия документ".

Промяна на документите

Редът за извършване на промяна по документите е определен в процедурата **Управление на документи**, която е задължителна за всяка система за управление. В нея точно и ясно е описано как се управляват документите - създаване, изменение, изземване и разпространение, архивиране, унищожаване. Освен това процедурата съдържа информация за **идентификацията** на документите, като например, идентификация с буквено-цифров код - ПХ-уу, където: П - означава процедура; Х - посочва раздела от стандарта, към който се отнася процедурата; уу - пореден номер на процедурата към съответния раздел.

Всяка промяна се отразява в документацията на системата, чрез изменение на съответните документи, запознаване на заинтересованите лица и провеждане на обучение/ако е необходимо/.

Принципно положение е мениджърът на системата да извършва промените по системата, но предложения за изменения могат да бъдат давани от всеки служител на организацията**.** Важно е организацията да си изработи подходящ регламент описан в процедурата Управление на документи.

При малка организация, с малък обем документи като количество и съдържание и не се правят чести изменения по документите е достатъчно да се използва само версия и дата на влизане в сила. В такъв случай се увеличава версията на документа при всяка промяна. И обратно, при голяма организация, с обемна документация е необходимо да се предвиди по-гъвкава система за управление на измененията, която обаче да не води до объркване и архивиране на купища хартия.

Управление на записи

Записите са особен вид *"документ, съдържащ получени резултати или предоставящ доказателство за извършени дейности"*. Записът представлява документ, който дава конкретна информация за изпълнението на дадена дейност**.** Например бланката, която показва каква информация трябва да се попълни в Плана за провеждане на вътрешен одит представлява документ, често наричан формуляр. Когато се попълни формуляра с конкретната информация за предстоящия вътрешен одит, като: обхват; критерии за одит; метод на одит; екип от одитори; разпределение на одитираните дейности по часове, този **документ вече се превръща в запис**.

Разграничението на записите като особен вид документи налага определянето на **специфични изисквания** относно тяхното управление, включващо определянето на *"необходимите мерки за идентификация, съхраняване, защита, достъпност,*

запазване и унищожаване на записите". В отговор на изискванията на стандарта е необходимо съставянето на процедура - Управление на записи, в която да се опишат правилата възприети от организацията по отношение на изброените направления.

Когато няма точно и ясно разбиране за правилата се създават условия за формулирането на неподходящи регламенти, водещи до усложнения при управлението на системата, неразбиране от страна на персонала и възникване на несъответствия.

Идентификацията на записите е свързана с тяхното разграничаване. Обикновено това става чрез уникалното наименованието на записа, номер и дата, специфичен код /ако има такъв/, име на лицето изготвило записа.

Изискванията относно **съхранението** на записите могат да бъдат различни, в зависимост от тяхното приложение. При определяне на сроковете за съхранение на записите трябва да се вземат под внимание изискванията поставени от нормативните разпоредби. Необходимостта от съхранение на записите е породена от факта, че трябва да се докаже съответствието с определените изисквания. В тази връзка записите трябва да бъдат ясни, четливи и съхранявани на подходящи места. В повечето случаи отговорниците за създаване и съхранение на записите са описани в съответните процедури, но за по-голямо улеснение може да се използва списък, в който да бъдат изброени всички записи с посочени отговорници за създаване, съхранение, вид на записа-електронен или хартиен, право на достъп, срок за съхранение и др.

Достъпът до записите също може да бъде различен. Ограничението се налага тъй като лицето, създаващо записа е отговорно за изпълнението на съответната дейност. В много случаи достъпа до записите е свързан с осигуряването на **конфиденциалност** на информацията в тях и определянето на регламент за предоставяне на записи на външни лица. Организацията трябва да определи кой до какви записи има достъп и съответно какви права притежава - създава, променя, разпространява, архивира и т.н., което е свързано и с тяхната защита.

Необходимо е да се осигурят мерки за **защита** на записите, които да предпазват записите от повреждане, загуба, унищожение или неоторизиран достъп.

Запазването на записите е свързано с тяхното **архивиране**. След изтичане на периода на съхранение записите се архивират за период определен от организацията, с изключение на случаите регламентирани със закон.

След изтичане на определения срок за архивиране записите се **унищожават**. Необходимо е да определите кои записи подлежат на унищожение, кой ще ги унищожи и по какъв начин.

Приложение 5 UML код на модела (Plant UML).

Административен модул

```
@startuml
title Модул: Администрация
class AdministrativenModul {
   -име : nvarchar(400)
   -тип : varchar(200)
}
class OrganizacionnaEdinica {
   -име : nvarchar(400)
   -тип : varchar(200)
   -родителID : int
}
class Potrebitel {
   -име : nvarchar(400)
   -потребителскоИме : nvarchar(200)
   -имейл : nvarchar(200)
   -паролаHash : nvarchar(400)
   -паролаSalt : nvarchar(400)
   -бележки : nvarchar(MAX)
   -датаНазначаване : datetime
   -датаНапускане : datetime
   -блокиран : bit
   -certificateThumbprint : nvarchar(200)
   -телефон : nvarchar(100)
}
class Rola {
   -име : nvarchar(200)
   -права : varchar(200)
}
class Pravo {
   -име : nvarchar(200)
   -описание : nvarchar(MAX)
}
```

```
' Връзки
AdministrativenModul --> OrganizacionnaEdinica : съдържа
OrganizacionnaEdinica --> OrganizacionnaEdinica : родител
OrganizacionnaEdinica --> Potrebitel : включва потребители
Potrebitel --> Rola : притежава
Rola --> Pravo : предоставя
@enduml
```

Модул: Бизнес процеси ДУБП

```
@startuml
title Модул: Бизнес процеси
class DefiniciaNaProcess {
   -идентификатор : int
   -име : nvarchar(250)
   -версия : int
   -датаСъздаване : datetime
   -активно : bit
   -описание : nvarchar(MAX)
   -моделНаОбект : nvarchar(250)
}
class Etap {
   -идентификатор : int
   -имеНаСтъпка : nvarchar(200)
   -далиНачален : bit
   -далиКраен : bit
   -типНазначаване : int
   -активиранеПредиМаршрутизация : bit
   -условиеПредиМаршрутизация : nvarchar(MAX)
   -активиранеСледМаршрутизация : bit
   -условиеСледМаршрутизация : nvarchar(MAX)
}
class InstanciaNaProcess {
   -идентификатор : int
   -идентификаторНаВерсия : int
   -идентификаторНаДефиниция : int
   -идентификаторНаОтговорник : int
```

```
    -идентификаторНаИнициатор : int
    -идентификаторНаПозиция : int
    -датаНачало : datetime
}
class PrehodMezhduEtapi {
    -идентификатор : int
    -етапОтID : int
    -етапДоID : int
    -идентификаторНаВерсия : int
    -описание : nvarchar(MAX)
    -визуалноПредставяне : nvarchar(MAX)
}
class PotencialenOtgovornik {
    -идентификатор : int
    -име : String
    -условиеЗаИзчисляване : nvarchar(MAX)
}
DefiniciaNaProcess --> Etap : дефинира
DefiniciaNaProcess --> InstanciaNaProcess : създава инстанции
Etap --> PrehodMezhduEtapi : има преход
PrehodMezhduEtapi --> Etap : насочва към
Etap --> PotencialenOtgovornik : може да има
InstanciaNaProcess --> Etap : съдържа текущ етап
@enduml
```

Модул за изпълнение на бизнес процеси ИБП

```
@startuml
title Модул: Документооборот
class Dokument {
    -регистрационенНомер : nvarchar(200)
    -външенНомер : nvarchar(200)
    -относно : nvarchar(MAX)
    -датаНаПолучаване : date
    -часНаПолучаване : datetime
    -кодЗаДостъп : nvarchar(200)
    -бележка : nvarchar(MAX)
```

```
}
class Prepiska {
   -номерНаРодителскаПреписка : nvarchar(200)
   -видДокумент : String
   -типДокумент : String
   -етап : String
   -дата : date
   -статус : BIT
}
class Korrespondent {
   -име : nvarchar(200)
   -булстат : int
   -мол : nvarchar(200)
   -типКореспондент : String
   -адресПоРегистрация : nvarchar(200)
   -адресЗаКореспонденция : nvarchar(200)
   -телефон : nvarchar(200)
   -факс : nvarchar(200)
   -електроненАдрес : nvarchar(200)
}
class Sluzhitel {
   -име : nvarchar(200)
   -длъжност : String
   -дирекция : String
   -прякРъководител : String
   -телефон : String
}
class Vyzlagane {
   -описание : nvarchar(MAX)
   -датаНаВъзлагане : date
   -срокДо : date
   -видВъзлагане : String
}
class FinansovoZadalzhenie {
   -дължимаСума : decimal(18,2)
   -датаНаВъзникване : date
```

```
    -датаНаПлащане : date
    -основание : nvarchar(MAX)
    -номерНаДокумент : nvarchar(200)
    -статус : String
    -платеноЧрез : String
}
Dokument --> Korrespondent : изпратен от/до
Dokument --> Prepiska : част от преписка
Prepiska --> Sluzhitel : въведена от / до служител
Prepiska --> Vyzlagane : съдържа възлагане
Vyzlagane --> Sluzhitel : възложено на
Prepiska --> FinansovoZadalzhenie : свързано със задължение
@enduml
@startuml
title Модул: ИБП (Изпълнение на Бизнес Процеси)
class InstanciaNaProcess {
    -идентификатор : int
    -идентификаторНаВерсия : int
    -идентификаторНаДефиниция : int
    -инициаторID : int
    -датаСъздаване : datetime
}
class Stypka {
    -идентификатор : int
    -име : nvarchar(200)
    -типОценка : int
    -кодОценка : nvarchar(MAX)
    -описание : nvarchar(MAX)
    -началенЕтап : bit
    -краенЕтап : bit
}
class EtapOtVersiya {
    -идентификатор : int
    -име : String
    -дата : datetime
    -формуляр : nvarchar(200)
```

```
}
class Prehod {
   -идентификатор : int
   -етапОтID : int
   -етапДоID : int
}
class VryzkaKymVersiya {
   -идентификаторНаПрехода : int
   -идентификаторНаВерсията : int
}
class Otgovornik {
   -идентификатор : int
   -име : String
   -тип : String
}
class PotencialenOtgovornik {
   -идентификатор : int
   -име : String
   -условие : nvarchar(MAX)
}
class Marshrut {
   -активиранеПредиМаршрутизация : bit
   -условиеПреди : nvarchar(MAX)
   -активиранеСледМаршрутизация : bit
   -условиеСлед : nvarchar(MAX)
}
InstanciaNaProcess --> Stypka : съдържа
InstanciaNaProcess --> Otgovornik : изпълнява се от
Stypka --> EtapOtVersiya : съответства на
EtapOtVersiya --> Prehod : има преход
Prehod --> VryzkaKymVersiya : свързан с
EtapOtVersiya --> PotencialenOtgovornik : възможни изпълнители
EtapOtVersiya --> Marshrut : дефинира поведение
@enduml
```

Модул: Контрол и Стандарти

```
@startuml
title Модул: Контрол и Стандарти
class Standart {
   -наименование : String
   -цели : String
   -обхват : String
   -описание : nvarchar(MAX)
}
class Protsedura {
   -наименование : String
   -описание : nvarchar(MAX)
   -редНаИзпълнение : nvarchar(MAX)
}
class Forma {
   -наименование : String
   -тип : String
   -дата : date
   -номер : String
   -утвърдил : Sluzhitel
}
class Dokument {
   -наименование : String
   -разработил : Sluzhitel
   -утвърдил : Sluzhitel
   -тип : String
   -дата : date
   -номер : String
   -описание : nvarchar(MAX)
}
class Registr {
   -наименование : String
   -дата : date
   -документи : List<Dokument>
}
```

```
class Termin {
   -термин : String
   -определение : String
}
class Prilozhenie {
   -наименование : String
   -стойност : String
   -формат : String
   -тип : String
}
class RKK {
   -номер : String
   -дата : date
   -ркк : String
   -подпис : String
}
Standart --> Protsedura : дефинира
Protsedura --> Forma : използва
Standart --> Registr : поддържа
Forma --> Dokument : придружава
Dokument --> Prilozhenie : има приложения
Dokument --> Termin : използва терминология
Standart --> RKK : подлежи на контрол
Forma --> Sluzhitel : утвърдена от
@enduml
```

Модул СУСИ

```
@startuml
title Модул: СУСИ / Платформа
class SUSIPlatform {
   -име : String
   -описание : String
   -активна : bit
}
class Kompania {
   -име : nvarchar(200)
```

```
    -булстат : nvarchar(20)
    -мол : nvarchar(200)
    -адрес : nvarchar(200)
    -ддсНомер : String
}
class Sluzhitel {
    -име : nvarchar(200)
    -длъжност : String
    -дирекция : String
    -телефон : String
    -електроннаПоща : String
}
class Dokumentooborot {
    -индекс : String
    -наименование : String
    -тип : String
}
class Standart {
    -код : String
    -описание : String
    -обхват : String
}
class OrganizatsionnaStruktura {
    -наименование : String
    -описание : String
    -тип : String
}
class KontrolenMehanizum {
    -име : String
    -тип : String
    -честота : String
    -начинНаОдit : String
}
class Politika {
    -име : String
    -описание : String
```

```
    -домейнСигурност : String
}
class KriteriiZaIzpylnenie {
    -име : String
    -стойност : String
    -формат : String
    -тригер : String
}
SUSIPlatform --> Kompania : принадлежи на
SUSIPlatform --> Sluzhitel : има служители
SUSIPlatform --> Dokumentooborot : съдържа индекси
SUSIPlatform --> Standart : включва стандарти
SUSIPlatform --> OrganizatsionnaStruktura : използва
SUSIPlatform --> KontrolenMehanizum : прилага
SUSIPlatform --> Politika : дефинира политики
SUSIPlatform --> KriteriiZaIzpylnenie : задава критерии
@enduml
```

Модул Одит и Контрол

```
@startuml
title Модул: Одит и Контрол
class Audit {
    -идентификатор : int
    -обхват : String
    -начинНаОдитиране : String
    -честотаНаОдит : String
    -описание : nvarchar(MAX)
    -датаНаОдит : date
}
class KontrolenMehanizum {
    -име : String
    -тип : String
    -граничниСтойности : String
    -тригери : String
    -форматНаДанните : String
}
```

```
class KriteriiZaIzpylnenie {
   -име : String
   -стойност : String
   -единица : String
   -праг : String
}
class Forma {
   -наименование : String
   -тип : String
   -дата : date
}
class Protses {
   -наименование : String
   -описание : nvarchar(MAX)
}
class Politika {
   -име : String
   -домейн : String
   -описание : String
}

Audit --> KontrolenMehanizum : проверява чрез
Audit --> KriteriiZaIzpylnenie : оценява по
Audit --> Forma : записва резултати във
Audit --> Protses : одитира процеси
Audit --> Politika : подлежи на политика
@enduml
```

Приложение 6 Реализация на Платформата с Python

Административен модул

```
from typing import List, Optional
from datetime import datetime
class Pravo:
    def __init__(self, opisanie: str):
        self.opisanie = opisanie
class Rola:
    def __init__(self, ime: str, prava: Optional[List[Pravo]] = None):
        self.ime = ime
        self.prava = prava if prava else []
class Potrebitel:
    def __init__(self,
                 ime: str,
                 potrebitelsko_ime: str,
                 email: str,
                 parola_hash: str,
                 parola_salt: str,
                 data_naznachavane: datetime,
                 data_napusnane: Optional[datetime],
                 blokiran: bool,
                 telefon: Optional[str] = None,
                 belezhki: Optional[str] = None):
        self.ime = ime
        self.potrebitelsko_ime = potrebitelsko_ime
        self.email = email
        self.parola_hash = parola_hash
        self.parola_salt = parola_salt
        self.data_naznachavane = data_naznachavane
        self.data_napusnane = data_napusnane
        self.blokiran = blokiran
        self.telefon = telefon
        self.belezhki = belezhki
        self.roli = []  # Списък от Rola
class OrganizacionnaEdinica:
```

```
    def __init__(self,
                 ime: str,
                 tip: Optional[str] = None,
                 roditelska: Optional['OrganizacionnaEdinica'] = None):
        self.ime = ime
        self.tip = tip
        self.roditelska = roditelska
        self.potrebiteli: List[Potrebitel] = []
class AdministrativenModul:
    def __init__(self, ime: str, tip: Optional[str] = None):
        self.ime = ime
        self.tip = tip
        self.organizacionni_edinici: List[OrganizacionnaEdinica] = []
```

Бизнес процеси ДУБП

```
from typing import List, Optional
from datetime import datetime
class DefiniciaNaProcess:
    def __init__(self,
                 identifikator: int,
                 ime: str,
                 versiya: int,
                 data_sazdavane: datetime,
                 aktivno: bool,
                 opisanie: Optional[str] = None,
                 model_na_obekt: Optional[str] = None):
        self.identifikator = identifikator
        self.ime = ime
        self.versiya = versiya
        self.data_sazdavane = data_sazdavane
        self.aktivno = aktivno
        self.opisanie = opisanie
        self.model_na_obekt = model_na_obekt
        self.etapi: List['Etap'] = []
        self.instancii: List['InstanciaNaProcess'] = []
class Etap:
```

```
    def __init__(self,
                 identifikator: int,
                 ime_na_stypka: str,
                 nachalen: bool,
                 kraen: bool,
                 tip_naznachavane: int,
                 aktivirane_predi: bool,
                 uslovie_predi: Optional[str],
                 aktivirane_sled: bool,
                 uslovie_sled: Optional[str]):
        self.identifikator = identifikator
        self.ime_na_stypka = ime_na_stypka
        self.nachalen = nachalen
        self.kraen = kraen
        self.tip_naznachavane = tip_naznachavane
        self.aktivirane_predi = aktivirane_predi
        self.uslovie_predi = uslovie_predi
        self.aktivirane_sled = aktivirane_sled
        self.uslovie_sled = uslovie_sled
        self.prehodi: List['PrehodMezhduEtapi'] = []
        self.potencialni_otgovornici: List['PotencialenOtgovornik'] = []
class InstanciaNaProcess:
    def __init__(self,
                 identifikator: int,
                 versiya_id: int,
                 definiciya_id: int,
                 otgovornik_id: Optional[int],
                 poziciya_id: Optional[int],
                 initiator_id: Optional[int],
                 data_nachalo: datetime):
        self.identifikator = identifikator
        self.versiya_id = versiya_id
        self.definiciya_id = definiciya_id
        self.otgovornik_id = otgovornik_id
        self.poziciya_id = poziciya_id
        self.initiator_id = initiator_id
```

```
        self.data_nachalo = data_nachalo
class PrehodMezhduEtapi:
    def __init__(self,
                 identifikator: int,
                 etap_ot_id: int,
                 etap_do_id: int,
                 versiya_id: int,
                 opisanie: Optional[str] = None,
                 vizualno_predstaviane: Optional[str] = None):
        self.identifikator = identifikator
        self.etap_ot_id = etap_ot_id
        self.etap_do_id = etap_do_id
        self.versiya_id = versiya_id
        self.opisanie = opisanie
        self.vizualno_predstaviane = vizualno_predstaviane
class PotencialenOtgovornik:
    def __init__(self,
                 identifikator: int,
                 ime: str,
                 uslovie: Optional[str]):
        self.identifikator = identifikator
        self.ime = ime
        self.uslovie = uslovie
```

Модул ИБП (Изпълнение на Бизнес Процеси)

```
class Korrespondent:
    def __init__(self,
                 ime: str,
                 bulstat: Optional[int],
                 mol: Optional[str],
                 tip: Optional[str],
                 adres_registracia: Optional[str],
                 adres_korespondencia: Optional[str],
                 telefon: Optional[str],
                 faks: Optional[str],
                 email: Optional[str]):
```

```
        self.ime = ime
        self.bulstat = bulstat
        self.mol = mol
        self.tip = tip
        self.adres_registracia = adres_registracia
        self.adres_korespondencia = adres_korespondencia
        self.telefon = telefon
        self.faks = faks
        self.email = email
class Sluzhitel:
    def __init__(self,
                 ime: str,
                 dlujnost: Optional[str],
                 direktcia: Optional[str],
                 pryak_ryk: Optional[str],
                 telefon: Optional[str]):
        self.ime = ime
        self.dlujnost = dlujnost
        self.direktcia = direktcia
        self.pryak_ryk = pryak_ryk
        self.telefon = telefon
class Dokument:
    def __init__(self,
                 registracionen_nomer: str,
                 vunshen_nomer: Optional[str],
                 otnosno: Optional[str],
                 data_poluchavane: Optional[datetime],
                 chas_poluchavane: Optional[datetime],
                 kod_dostap: Optional[str],
                 belejka: Optional[str],
                 korrespondent: Optional[Korrespondent] = None):
        self.registracionen_nomer = registracionen_nomer
        self.vunshen_nomer = vunshen_nomer
        self.otnosno = otnosno
        self.data_poluchavane = data_poluchavane
        self.chas_poluchavane = chas_poluchavane
```

```
        self.kod_dostap = kod_dostap
        self.belejka = belejka
        self.korrespondent = korrespondent
class FinansovoZadalzhenie:
    def __init__(self,
                 suma: float,
                 data_vaznikvane: datetime,
                 data_plashtane: Optional[datetime],
                 osnovanie: str,
                 status: Optional[str],
                 nomer_dokument: Optional[str],
                 plateno_chrez: Optional[str]):
        self.suma = suma
        self.data_vaznikvane = data_vaznikvane
        self.data_plashtane = data_plashtane
        self.osnovanie = osnovanie
        self.status = status
        self.nomer_dokument = nomer_dokument
        self.plateno_chrez = plateno_chrez
class Vyzlagane:
    def __init__(self,
                 opisanie: str,
                 data_vyzlagane: datetime,
                 srok_do: Optional[datetime],
                 vid_vyzlagane: Optional[str],
                 ot: Optional[Sluzhitel],
                 do: Optional[List[Sluzhitel]]):
        self.opisanie = opisanie
        self.data_vyzlagane = data_vyzlagane
        self.srok_do = srok_do
        self.vid_vyzlagane = vid_vyzlagane
        self.ot = ot
        self.do = do if do else []
class Prepiska:
    def __init__(self,
                 nomer_rod_pr: Optional[str],
```

```
                vid_dokument: Optional[str],
                tip_dokument: Optional[str],
                etap: Optional[str],
                data: Optional[datetime],
                status: bool,
                dokumenti: List[Dokument],
                sluzhitel: Optional[Sluzhitel],
                vyzlagania: List[Vyzlagane],
                finansovo: Optional[FinansovoZadalzhenie]):
        self.nomer_rod_pr = nomer_rod_pr
        self.vid_dokument = vid_dokument
        self.tip_dokument = tip_dokument
        self.etap = etap
        self.data = data
        self.status = status
        self.dokumenti = dokumenti
        self.sluzhitel = sluzhitel
        self.vyzlagania = vyzlagania
        self.finansovo = finansovo
class Otgovornik:
    def __init__(self, identifikator: int, ime: str, tip: str):
        self.identifikator = identifikator
        self.ime = ime
        self.tip = tip
class Marshrut:
    def __init__(self,
                aktivirane_predi: bool,
                uslovie_predi: Optional[str],
                aktivirane_sled: bool,
                uslovie_sled: Optional[str]):
        self.aktivirane_predi = aktivirane_predi
        self.uslovie_predi = uslovie_predi
        self.aktivirane_sled = aktivirane_sled
        self.uslovie_sled = uslovie_sled
class Stypka:
    def __init__(self,
```

```
                identifikator: int,
                ime: str,
                tip_ocenka: Optional[int],
                kod_ocenka: Optional[str],
                opisanie: Optional[str],
                nachalen_etap: bool,
                kraen_etap: bool):
            self.identifikator = identifikator
            self.ime = ime
            self.tip_ocenka = tip_ocenka
            self.kod_ocenka = kod_ocenka
            self.opisanie = opisanie
            self.nachalen_etap = nachalen_etap
            self.kraen_etap = kraen_etap
        class EtapOtVersiya:
            def __init__(self,
                identifikator: int,
                ime: str,
                data: datetime,
                formulyar: Optional[str],
                marshrut: Optional[Marshrut],
                potencialni_otgovornici: Optional[List[PotencialenOtgovornik]] =
None):
            self.identifikator = identifikator
            self.ime = ime
            self.data = data
            self.formulyar = formulyar
            self.marshrut = marshrut
            self.potencialni_otgovornici = potencialni_otgovornici if
potencialni_otgovornici else []
        class Prehod:
            def __init__(self,
                identifikator: int,
                etap_ot_id: int,
                etap_do_id: int):
            self.identifikator = identifikator
```

```
        self.etap_ot_id = etap_ot_id
        self.etap_do_id = etap_do_id
class VryzkaKymVersiya:
    def __init__(self,
                 identifikator_na_prehoda: int,
                 identifikator_na_versiya: int):
        self.identifikator_na_prehoda = identifikator_na_prehoda
        self.identifikator_na_versiya = identifikator_na_versiya
```

Контрол и Стандарти

```
class Termin:
    def __init__(self, termin: str, opredelenie: str):
        self.termin = termin
        self.opredelenie = opredelenie
class Prilozhenie:
    def __init__(self, naimenovanie: str, stojnost: str, format: str, tip: str):
        self.naimenovanie = naimenovanie
        self.stojnost = stojnost
        self.format = format
        self.tip = tip
class Sluzhitel:  # Ако вече е дефиниран, тази дефиниция се пропуска
    def __init__(self, ime: str):
        self.ime = ime
class Dokument:
    def __init__(self,
                 naimenovanie: str,
                 razrabotil: Sluzhitel,
                 utvardil: Sluzhitel,
                 tip: str,
                 data: datetime,
                 nomer: str,
                 opisanie: Optional[str],
                 prilozhenia: Optional[List[Prilozhenie]] = None,
                 termini: Optional[List[Termin]] = None):
        self.naimenovanie = naimenovanie
        self.razrabotil = razrabotil
```

```
        self.utvardil = utvardil
        self.tip = tip
        self.data = data
        self.nomer = nomer
        self.opisanie = opisanie
        self.prilozhenia = prilozhenia if prilozhenia else []
        self.termini = termini if termini else []
class Forma:
    def __init__(self,
                 naimenovanie: str,
                 tip: str,
                 data: datetime,
                 nomer: str,
                 utvardil: Sluzhitel):
        self.naimenovanie = naimenovanie
        self.tip = tip
        self.data = data
        self.nomer = nomer
        self.utvardil = utvardil
class Protsedura:
    def __init__(self,
                 naimenovanie: str,
                 opisanie: str,
                 red_na_izpalnenie: str,
                 formi: Optional[List[Forma]] = None):
        self.naimenovanie = naimenovanie
        self.opisanie = opisanie
        self.red_na_izpalnenie = red_na_izpalnenie
        self.formi = formi if formi else []
class Registr:
    def __init__(self,
                 naimenovanie: str,
                 data: datetime,
                 dokumenti: Optional[List[Dokument]] = None):
        self.naimenovanie = naimenovanie
        self.data = data
```

```
        self.dokumenti = dokumenti if dokumenti else []
class Standart:
    def __init__(self,
                 naimenovanie: str,
                 celi: str,
                 obhvat: str,
                 opisanie: str,
                 protseduri: List[Protsedura],
                 registri: List[Registr]):
        self.naimenovanie = naimenovanie
        self.celi = celi
        self.obhvat = obhvat
        self.opisanie = opisanie
        self.protseduri = protseduri
        self.registri = registri
```

Модул СУСИ

```
class Kompania:
    def __init__(self,
                 ime: str,
                 bulstat: str,
                 mol: str,
                 adres: str,
                 dds_nomer: str):
        self.ime = ime
        self.bulstat = bulstat
        self.mol = mol
        self.adres = adres
        self.dds_nomer = dds_nomer
class OrganizatsionnaStruktura:
    def __init__(self, naimenovanie: str, opisanie: str, tip: str):
        self.naimenovanie = naimenovanie
        self.opisanie = opisanie
        self.tip = tip
class Dokumentooborot:
    def __init__(self, indeks: str, naimenovanie: str, tip: str):
```

```
        self.indeks = indeks
        self.naimenovanie = naimenovanie
        self.tip = tip
class Politika:
    def __init__(self, ime: str, opisanie: str, domein_sigur: str):
        self.ime = ime
        self.opisanie = opisanie
        self.domein_sigur = domein_sigur
class KriteriiZaIzpylnenie:
    def __init__(self, ime: str, stojnost: str, format: str, trigger: str):
        self.ime = ime
        self.stojnost = stojnost
        self.format = format
        self.trigger = trigger
class KontrolenMehanizum:
    def __init__(self, ime: str, tip: str, chestota: str, nachin_na_odit: str):
        self.ime = ime
        self.tip = tip
        self.chestota = chestota
        self.nachin_na_odit = nachin_na_odit
class SUSIPlatform:
    def __init__(self,
                 ime: str,
                 opisanie: str,
                 aktivna: bool,
                 kompaniya: Kompania,
                 sluzhiteli: List[Sluzhitel],
                 indeksirane: List[Dokumentooborot],
                 standarti: List[Standart],
                 struktura: OrganizatsionnaStruktura,
                 kontroli: List[KontrolenMehanizum],
                 politiki: List[Politika],
                 kriterii: List[KriteriiZaIzpylnenie]):
        self.ime = ime
        self.opisanie = opisanie
        self.aktivna = aktivna
```

```
        self.kompaniya = kompaniya
        self.sluzhiteli = sluzhiteli
        self.indeksirane = indeksirane
        self.standarti = standarti
        self.struktura = struktura
        self.kontroli = kontroli
        self.politiki = politiki
        self.kriterii = kriterii
```

Одит и Контрол

```
class Audit:
    def __init__(self,
                 identifikator: int,
                 obhvat: str,
                 nachin_na_odit: str,
                 chestota_na_odit: str,
                 opisanie: Optional[str],
                 data_na_odit: datetime):
        self.identifikator = identifikator
        self.obhvat = obhvat
        self.nachin_na_odit = nachin_na_odit
        self.chestota_na_odit = chestota_na_odit
        self.opisanie = opisanie
        self.data_na_odit = data_na_odit
        self.kriterii: List[KriteriiZaIzpylnenie] = []
        self.kontroli: List[KontrolenMehanizum] = []
        self.formi: List[Forma] = []
        self.protsesi: List[Protsedura] = []
        self.politiki: List[Politika] = []
    # Забележка: класовете KriteriiZaIzpylnenie, KontrolenMehanizum, Forma, Protsedura и Politika
    # вече са дефинирани в предишните модули и тук се използват чрез асоциации.
    # Няма нужда от дублиране, ако ще се използват в един проектен код.
```

Приложение 7 ORM (Object-Relational Mapping) реализация – SQL Alchemy

Административен модул

```
from sqlalchemy import Column, Integer, String, DateTime, Boolean, ForeignKey, Table
from sqlalchemy.orm import relationship, declarative_base
from datetime import datetime
Base = declarative_base()
# Примерна many-to-many релация между Potrebitel и Rola
potrebitel_rola = Table(
   'potrebitel_rola',
   Base.metadata,
   Column('potrebitel_id', Integer, ForeignKey('potrebiteli.id')),
   Column('rola_id', Integer, ForeignKey('roli.id'))
)
class Pravo(Base):
   __tablename__ = 'prava'
   id = Column(Integer, primary_key=True)
   opisanie = Column(String)
   def __repr__(self):
      return f"<Pravo(id={self.id}, opisanie='{self.opisanie}')>"
class Rola(Base):
   __tablename__ = 'roli'
   id = Column(Integer, primary_key=True)
   ime = Column(String)
   prava = Column(String)  # или връзка с таблица `prava`
   potrebiteli = relationship("Potrebitel", secondary=potrebitel_rola, back_populates="roli")
   def __repr__(self):
      return f"<Rola(id={self.id}, ime='{self.ime}')>"
class Potrebitel(Base):
   __tablename__ = 'potrebiteli'
   id = Column(Integer, primary_key=True)
   ime = Column(String)
   potrebitelsko_ime = Column(String)
```

```
    email = Column(String)
    parola_hash = Column(String)
    parola_salt = Column(String)
    data_naznachavane = Column(DateTime)
    data_napusnane = Column(DateTime, nullable=True)
    blokiran = Column(Boolean)
    telefon = Column(String, nullable=True)
    belezhki = Column(String, nullable=True)
    roli = relationship("Rola", secondary=potrebitel_rola,
back_populates="potrebiteli")
    organizacionna_edinica_id = Column(Integer, ForeignKey('edinici.id'))
    def __repr__(self):
        return f"<Potrebitel(id={self.id}, ime='{self.ime}')>"
class OrganizacionnaEdinica(Base):
    __tablename__ = 'edinici'
    id = Column(Integer, primary_key=True)
    ime = Column(String)
    tip = Column(String)
    roditelska_id = Column(Integer, ForeignKey('edinici.id'), nullable=True)
    roditelska = relationship("OrganizacionnaEdinica", remote_side=[id])
    potrebiteli = relationship("Potrebitel", backref="edinica")
    modul_id = Column(Integer, ForeignKey('moduli.id'))
    def __repr__(self):
        return f"<OrganizacionnaEdinica(id={self.id}, ime='{self.ime}')>"
class AdministrativenModul(Base):
    __tablename__ = 'moduli'
    id = Column(Integer, primary_key=True)
    ime = Column(String)
    tip = Column(String)
    edinici = relationship("OrganizacionnaEdinica", backref="modul")
    def __repr__(self):
        return f"<AdministrativenModul(id={self.id}, ime='{self.ime}')>"
```

Модул Бизнес процеси ДУБП

```
from sqlalchemy import Text
class DefiniciaNaProcessORM(Base):
```

```
        __tablename__ = 'definicii_na_processi'
        id = Column(Integer, primary_key=True)
        ime = Column(String)
        versiya = Column(Integer)
        data_sazdavane = Column(DateTime)
        aktivno = Column(Boolean)
        opisanie = Column(Text, nullable=True)
        model_na_obekt = Column(String, nullable=True)
        etapi = relationship("EtapORM", back_populates="definiciya")
        instancii = relationship("InstanciaNaProcessORM",
back_populates="definiciya")
    class EtapORM(Base):
        __tablename__ = 'etapi'
        id = Column(Integer, primary_key=True)
        ime_na_stypka = Column(String)
        nachalen = Column(Boolean)
        kraen = Column(Boolean)
        tip_naznachavane = Column(Integer)
        aktivirane_predi = Column(Boolean)
        uslovie_predi = Column(Text, nullable=True)
        aktivirane_sled = Column(Boolean)
        uslovie_sled = Column(Text, nullable=True)
        definiciya_id = Column(Integer, ForeignKey('definicii_na_processi.id'))
        definiciya = relationship("DefiniciaNaProcessORM", back_populates="etapi")
        prehodi = relationship("PrehodMezhduEtapiORM", back_populates="etap")
        potencialni_otgovornici = relationship("PotencialenOtgovornikORM",
back_populates="etap")
    class InstanciaNaProcessORM(Base):
        __tablename__ = 'instancii_na_processi'
        id = Column(Integer, primary_key=True)
        versiya_id = Column(Integer)
        definiciya_id = Column(Integer, ForeignKey('definicii_na_processi.id'))
        otgovornik_id = Column(Integer, nullable=True)
        poziciya_id = Column(Integer, nullable=True)
        initiator_id = Column(Integer, nullable=True)
        data_nachalo = Column(DateTime)
```

```
        definiciya = relationship("DefiniciaNaProcessORM",
back_populates="instancii")
    class PrehodMezhduEtapiORM(Base):
        __tablename__ = 'prehodi_mezhdu_etapi'
        id = Column(Integer, primary_key=True)
        etap_ot_id = Column(Integer)
        etap_do_id = Column(Integer)
        versiya_id = Column(Integer)
        opisanie = Column(Text, nullable=True)
        vizualno_predstaviane = Column(Text, nullable=True)
        etap_id = Column(Integer, ForeignKey('etapi.id'))
        etap = relationship("EtapORM", back_populates="prehodi")
    class PotencialenOtgovornikORM(Base):
        __tablename__ = 'potencialni_otgovornici'
        id = Column(Integer, primary_key=True)
        ime = Column(String)
        uslovie = Column(Text, nullable=True)
        etap_id = Column(Integer, ForeignKey('etapi.id'))
        etap = relationship("EtapORM", back_populates="potencialni_otgovornici")
```

Модул ИБП (Изпълнение на Бизнес Процеси)

```
    class KorrespondentORM(Base):
        __tablename__ = 'korrespondenti'
        id = Column(Integer, primary_key=True)
        ime = Column(String)
        bulstat = Column(String, nullable=True)
        mol = Column(String, nullable=True)
        tip = Column(String, nullable=True)
        adres_registracia = Column(String, nullable=True)
        adres_korespondencia = Column(String, nullable=True)
        telefon = Column(String, nullable=True)
        faks = Column(String, nullable=True)
        email = Column(String, nullable=True)
        dokumenti = relationship("DokumentORM", back_populates="korrespondent")
    class SluzhitelORM(Base):
        __tablename__ = 'sluzhiteli'
```

```
        id = Column(Integer, primary_key=True)
        ime = Column(String)
        dlujnost = Column(String, nullable=True)
        direktcia = Column(String, nullable=True)
        pryak_ryk = Column(String, nullable=True)
        telefon = Column(String, nullable=True)
    class DokumentORM(Base):
        __tablename__ = 'dokumenti'
        id = Column(Integer, primary_key=True)
        registracionen_nomer = Column(String)
        vunshen_nomer = Column(String, nullable=True)
        otnosno = Column(Text, nullable=True)
        data_poluchavane = Column(DateTime, nullable=True)
        chas_poluchavane = Column(DateTime, nullable=True)
        kod_dostap = Column(String, nullable=True)
        belejka = Column(Text, nullable=True)
        korrespondent_id = Column(Integer, ForeignKey('korrespondenti.id'))
        korrespondent = relationship("KorrespondentORM",
back_populates="dokumenti")
    class FinansovoZadalzhenieORM(Base):
        __tablename__ = 'finansovi_zadalzheniq'
        id = Column(Integer, primary_key=True)
        suma = Column(Integer)
        data_vaznikvane = Column(DateTime)
        data_plashtane = Column(DateTime, nullable=True)
        osnovanie = Column(Text)
        status = Column(String, nullable=True)
        nomer_dokument = Column(String, nullable=True)
        plateno_chrez = Column(String, nullable=True)
    class VyzlaganeORM(Base):
        __tablename__ = 'vyzlagania'
        id = Column(Integer, primary_key=True)
        opisanie = Column(Text)
        data_vyzlagane = Column(DateTime)
        srok_do = Column(DateTime, nullable=True)
        vid_vyzlagane = Column(String, nullable=True)
```

```
        ot_id = Column(Integer, ForeignKey('sluzhiteli.id'))
        ot = relationship("SluzhitelORM", foreign_keys=[ot_id])
        # TODO: many-to-many до изпълнители при нужда
    class PrepiskaORM(Base):
        __tablename__ = 'prepiski'
        id = Column(Integer, primary_key=True)
        nomer_rod_pr = Column(String, nullable=True)
        vid_dokument = Column(String, nullable=True)
        tip_dokument = Column(String, nullable=True)
        etap = Column(String, nullable=True)
        data = Column(DateTime, nullable=True)
        status = Column(Boolean)
        sluzhitel_id = Column(Integer, ForeignKey('sluzhiteli.id'), nullable=True)
        sluzhitel = relationship("SluzhitelORM")
        finansovo_id = Column(Integer, ForeignKey('finansovi_zadalzheniq.id'),
nullable=True)
        finansovo = relationship("FinansovoZadalzhenieORM")
        dokumenti = relationship("DokumentORM")
        vyzlagania = relationship("VyzlaganeORM")
    class OtgovornikORM(Base):
        __tablename__ = 'otgovornici'
        id = Column(Integer, primary_key=True)
        ime = Column(String)
        tip = Column(String)
    class MarshrutORM(Base):
        __tablename__ = 'marshruti'
        id = Column(Integer, primary_key=True)
        aktivirane_predi = Column(Boolean)
        uslovie_predi = Column(Text, nullable=True)
        aktivirane_sled = Column(Boolean)
        uslovie_sled = Column(Text, nullable=True)
    class PotencialenOtgovornikORM(Base):
        __tablename__ = 'potencialni_otgovornici_ibp'
        id = Column(Integer, primary_key=True)
        ime = Column(String)
        uslovie = Column(Text, nullable=True)
```

```
        etap_id = Column(Integer, ForeignKey('etapi_ot_versii.id'))
        etap = relationship("EtapOtVersiyaORM", back_populates="potencialni_otgovornici")
    class EtapOtVersiyaORM(Base):
        __tablename__ = 'etapi_ot_versii'
        id = Column(Integer, primary_key=True)
        ime = Column(String)
        data = Column(DateTime)
        formulyar = Column(String, nullable=True)
        marshrut_id = Column(Integer, ForeignKey('marshruti.id'))
        marshrut = relationship("MarshrutORM")
        potencialni_otgovornici = relationship("PotencialenOtgovornikORM", back_populates="etap")
    class StypkaORM(Base):
        __tablename__ = 'stypki'
        id = Column(Integer, primary_key=True)
        ime = Column(String)
        tip_ocenka = Column(Integer, nullable=True)
        kod_ocenka = Column(String, nullable=True)
        opisanie = Column(Text, nullable=True)
        nachalen_etap = Column(Boolean)
        kraen_etap = Column(Boolean)
        instanciq_id = Column(Integer, ForeignKey('instancii_ibp.id'))
        instanciq = relationship("InstanciaNaProcessIBPORM", back_populates="stypki")
    class InstanciaNaProcessIBPORM(Base):
        __tablename__ = 'instancii_ibp'
        id = Column(Integer, primary_key=True)
        versiya_id = Column(Integer)
        definiciya_id = Column(Integer)
        initiator_id = Column(Integer)
        data_sazdavane = Column(DateTime)
        otgovornik_id = Column(Integer, ForeignKey('otgovornici.id'))
        otgovornik = relationship("OtgovornikORM")
        stypki = relationship("StypkaORM", back_populates="instanciq")
    class PrehodORM(Base):
```

```
    __tablename__ = 'prehodi_etapi'
    id = Column(Integer, primary_key=True)
    etap_ot_id = Column(Integer)
    etap_do_id = Column(Integer)
class VryzkaKymVersiyaORM(Base):
    __tablename__ = 'vryzki_kum_versiya'
    id = Column(Integer, primary_key=True)
    prehod_id = Column(Integer, ForeignKey('prehodi_etapi.id'))
    versiya_id = Column(Integer)
```

Контрол и Стандарти

```
class TerminORM(Base):
    __tablename__ = 'termini'
    id = Column(Integer, primary_key=True)
    termin = Column(String)
    opredelenie = Column(Text)
    dokument_id = Column(Integer, ForeignKey('dokumenti_kontrol.id'))
    dokument = relationship("DokumentKontrolORM", back_populates="termini")
class PrilozhenieORM(Base):
    __tablename__ = 'prilozhenia'
    id = Column(Integer, primary_key=True)
    naimenovanie = Column(String)
    stojnost = Column(String)
    format = Column(String)
    tip = Column(String)
    dokument_id = Column(Integer, ForeignKey('dokumenti_kontrol.id'))
    dokument = relationship("DokumentKontrolORM",
back_populates="prilozhenia")
class DokumentKontrolORM(Base):
    __tablename__ = 'dokumenti_kontrol'
    id = Column(Integer, primary_key=True)
    naimenovanie = Column(String)
    tip = Column(String)
    data = Column(DateTime)
    nomer = Column(String)
    opisanie = Column(Text, nullable=True)
```

```
    razrabotil_id = Column(Integer, ForeignKey('sluzhiteli.id'))
    utvardil_id = Column(Integer, ForeignKey('sluzhiteli.id'))
    razrabotil = relationship("SluzhitelORM", foreign_keys=[razrabotil_id])
    utvardil = relationship("SluzhitelORM", foreign_keys=[utvardil_id])
    prilozhenia = relationship("PrilozhenieORM", back_populates="dokument")
    termini = relationship("TerminORM", back_populates="dokument")
class FormaORM(Base):
    __tablename__ = 'formi'
    id = Column(Integer, primary_key=True)
    naimenovanie = Column(String)
    tip = Column(String)
    data = Column(DateTime)
    nomer = Column(String)
    utvardil_id = Column(Integer, ForeignKey('sluzhiteli.id'))
    utvardil = relationship("SluzhitelORM")
class ProtseduraKontrolORM(Base):
    __tablename__ = 'protseduri_kontrol'
    id = Column(Integer, primary_key=True)
    naimenovanie = Column(String)
    opisanie = Column(Text)
    red_na_izpalnenie = Column(Text)
    formi = relationship("FormaORM")
class RegistrORM(Base):
    __tablename__ = 'registri'
    id = Column(Integer, primary_key=True)
    naimenovanie = Column(String)
    data = Column(DateTime)
    dokumenti = relationship("DokumentKontrolORM")
class StandartKontrolORM(Base):
    __tablename__ = 'standarti_kontrol'
    id = Column(Integer, primary_key=True)
    naimenovanie = Column(String)
    celi = Column(Text)
    obhvat = Column(Text)
    opisanie = Column(Text)
    protseduri = relationship("ProtseduraKontrolORM")
```

```
    registri = relationship("RegistrORM")
```

Модул СУСИ

```
class KompaniaORM(Base):
    __tablename__ = 'kompanii'
    id = Column(Integer, primary_key=True)
    ime = Column(String)
    bulstat = Column(String)
    mol = Column(String)
    adres = Column(String)
    dds_nomer = Column(String)
class OrganizatsionnaStrukturaORM(Base):
    __tablename__ = 'organizatsionna_struktura'
    id = Column(Integer, primary_key=True)
    naimenovanie = Column(String)
    opisanie = Column(Text)
    tip = Column(String)
class DokumentooborotORM(Base):
    __tablename__ = 'dokumentooborot'
    id = Column(Integer, primary_key=True)
    indeks = Column(String)
    naimenovanie = Column(String)
    tip = Column(String)
class PolitikaORM(Base):
    __tablename__ = 'politiki'
    id = Column(Integer, primary_key=True)
    ime = Column(String)
    opisanie = Column(Text)
    domein_sigur = Column(String)
class KriteriiZaIzpylnenieORM(Base):
    __tablename__ = 'kriterii_za_izpylnenie'
    id = Column(Integer, primary_key=True)
    ime = Column(String)
    stojnost = Column(String)
    format = Column(String)
    trigger = Column(String)
```

```
class KontrolenMehanizumORM(Base):
    __tablename__ = 'kontrolni_mehanizmi'

    id = Column(Integer, primary_key=True)
    ime = Column(String)
    tip = Column(String)
    chestota = Column(String)
    nachin_na_odit = Column(String)
class SUSIPlatformORM(Base):
    __tablename__ = 'susi_platformi'
    id = Column(Integer, primary_key=True)
    ime = Column(String)
    opisanie = Column(Text)
    aktivna = Column(Boolean)
    kompaniya_id = Column(Integer, ForeignKey('kompanii.id'))
    kompaniya = relationship("KompaniaORM")
    struktura_id = Column(Integer, ForeignKey('organizatsionna_struktura.id'))
    struktura = relationship("OrganizatsionnaStrukturaORM")
    # Връзки към други обекти
    sluzhiteli = relationship("SluzhitelORM")
    indeksirane = relationship("DokumentooborotORM")
    kontroli = relationship("KontrolenMehanizumORM")
    politiki = relationship("PolitikaORM")
    kriterii = relationship("KriteriiZaIzpylnenieORM")
    # Standarti – могат да бъдат общи или свързани чрез отделна таблица
```

Одит и Контрол

```
class AuditORM(Base):
    __tablename__ = 'auditi'
    id = Column(Integer, primary_key=True)
    obhvat = Column(String)
    nachin_na_odit = Column(String)
    chestota_na_odit = Column(String)
    opisanie = Column(Text, nullable=True)
    data_na_odit = Column(DateTime)
    # Връзки към други таблици (one-to-many)
```

```
kriterii = relationship("KriteriiZaIzpylnenieORM")
kontroli = relationship("KontrolenMehanizumORM")
formi = relationship("FormaORM")
protsesi = relationship("ProtseduraKontrolORM")
politiki = relationship("PolitikaORM")
```

Библиография

[1] Velev T., Dobrinkova N., "Unified innovative Platform for administration and automated management of internationally recognized standards", Book Title: "Digital Transformation, Cyber Security and Resilience of Modern Societies", book series "Studies in Big Data", Springer. DOI:10.1007/978-3-030-65722-2, eBook ISBN: 978-3-030-65722-2, ISBN: 978-3-030-65721-5, ISSN: 2197-6503, 2021, vol. 84, p. 61 – p. 75;

[2] John R. Vacca, Computer and Information Security Handbook, Third Edition, Copyright © 2017 Elsevier Inc.;

[3] WHITMAN, M. E. AND MATTORD, H., 2013 Management of information security. 4th edn. United States: Delmar Cengage Learning;

[4] ISO/IEC 27001:2022 Сигурност на информацията, киберсигурност и защита на поверителността. Системи за управление на сигурността на информацията. Изисквания, БЪЛГАРСКИ ИНСТИТУТ ЗА СТАНДАРТИЗАЦИЯ, 2025;

[5] Amoroso E.G, Fundamentals of Computer Security Technology, Prentice-Hall PTR, 1994;

[6] Pipkin D.L, Halting the Hacker – A Practical Guide to Computer Security, Prentice-Hall PTR, ISBN 0-13-243718-X, 1997;

[7] Хауърд М. и Д. Лебланк, Писане на сигурен код, СофтПрес, 2004;

[8] W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135;

[9] ADSHEAD, A. (2014) Data set to grow 10-fold by 2020 as internet of things takes off. (Viewed: 24 May 2016). Available at: http://www.computerweekly.com/news/2240217788/Data-set-to-grow-10-fold-by-2020-as-internet-of-things-takes-off;

[10] TRACY, S.J., 2012. Qualitative research methods: Collecting evidence, crafting analysis, communicating impact. United Kingdom: Wiley-Blackwell (an imprint of John Wiley & Sons Ltd);

[11] Computer Security – ESORICS 2013 18th European Symposium on Research in Computer Security Egham, UK, September 9-13, 2013 Proceedings, Springer;

[12] ACUANT, I. AND RESERVED, A.R., 2015. 101 ways your identity can be stolen and exploited | ACUANT. (Viewed: 14 June 2016).Available at: http://www.acuantcorp.com/101-ways-your-identity-can-be-stolen;

[13] Junaid Ahmed Zubairi, Athar Mahboob, Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies, Copyright © 2012 by IGI Global;

[14] Bulgarian Institute for Standardization http://www.bds-bg.org, 2025;

[15] National Institute of Standards and Technology, "Information Technology Standards", Standards Incorporated by Reference (SIBR) Database, 2025;

[16] Book for the verification of software and computer systems, NASA guide book, http://eis.jpl.nasa.gov/quality/Formal_Methods, 2025;

[17] Feigenbaum, A. V., Total Quality Control, McGraw-Hill Professional, 2008;

[18] IT Service Management Standards A Reference Model for Open Standards-Based ITSM Solutions, An IBM White Paper, April 2006 http://www-07.ibm.com/sg/governance/servicemanagement/downloads/itsmstandardsreferencemodel.pdf;

[19] BS 25999-1:2006 Business Continuity Management – Part 1: Code of Practice;

[20] BS 25999 –A framework for resilience and success, Robert Whitcher, BCI Webinar June, 2009;
[21] Leighton R. Johnson III, Computer Incident Response and Forensics Team Management Conducting a Successful Incident Response, Copyright © 2014 Elsevier Inc;
[22] C. Warren Axelrod, Engineering Safe and Secure Software Systems, © 2013 ARTECH HOUSE;
[23] https://www.isms.online/, 2025;
[24] https://compleye.io/, 2025;
[25] https://www.vanta.com/, 2025;
[26] https://scytale.ai/, 2025;
[27] https://www.apptega.com/, 2025;
[28] https://www.auditboard.com/, 2025;
[29] https://secureframe.com/;, 2025
[30] Chris Fry and Martin Nystrom, Security Monitoring, Copyright © 2009 Chris Fry and Martin Nystrom;
[31] DIGILIENCE 2019: Digital Transformation, Cyber Security and Resilience Central Military Club Sofia, Bulgaria, October 2-4, 2019, доклад: "The logical model of unify, innovative Platform for Automation and Management of Standards (PAMS)";
[32] Velev T, Heuristic essentials for modelling and optimization of a Platform for Automation and Management of Information Security Standards (PAMISS), BdKCSE'2021 – Big Data, Knowledge and Control Systems Engineering, 28–29 October 2021, Sofia, Bulgaria 2021 Big Data, Knowledge and Control Systems, Engineering (BdKCSE) | 978-1-6654-1042-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/BDKCSE53180.2021.9627263;
[33] Poster M.; "The mode of information"; Cambridge, 2002.;
[34] Н. Ненков, Експертни системи, Унив. Издателство "Епископ К. Преславски", Шумен, 2006;
[35] Лодон К., Дж. Лодон, Управление информационными системами, 7 изд., Питер, Москва, 2005;
[36] A. MORTON and M. A. SASSE, 2014. Desperately seeking assurances: Segmenting users by their information-seeking preferences. Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on. Pp.102-111;
[37] Keneth C. Laudon and Jane P. Laudon, Management information systems: managing the digital firm, 9th ed., Prentice Hall, 2010;
[38] Проект № BG161PO003-1.1.06–0036-C0001 "Унифицирана платформа за администрация автоматизация и управление на международно признати стандарти";
[39] Organization for the Advancement of Structured Information Standards (OASIS), Web Services Business Process Execution Language (WSBPEL) Technical Committee, http://www.oasisopen.org/, 2025;
[40] Marshall, G.H.S., Evaluating Management Standards: empirical research into the Scottish Quality Management May-2006, University of Stirling;
[41] ISO/IEC 27002:2022 Сигурност на информацията, киберсигурност и защита на поверителността. Управление на сигурността на информацията., БЪЛГАРСКИ ИНСТИТУТ ЗА СТАНДАРТИЗАЦИЯ, 2025;
[42] Guidelines for Smart Grid Cyber Security:Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, National Institute of Standards and Technology Interagency Report 7628, vol. 1 289 pages (August 2010);

[43] Cerami, E. "Web Services Essentials", O'Reilly. 2002;
[44] Advances in Security of Information and Communication Networks, First International Conference, SecNet 2013 Cairo, Egypt, September 3-5, 2013 Proceedings, Springer;
[45] Jorgensen T.H., M. D. Mellado and A. Remmen, Integrated Management Systems – three different levels of integretion. Jounal of Cleaner Production, 2006;
[46] Стоилов, Т. (2003). Интегриране на информационни ресурси и услуги в глобалната мрежа. сп. „Автоматика и информатика", бр.2/2003;
[47] Attiogbe Ch. (2000), Formal Methods Integration for Software Development: Some Locks and Outlines, Research Report No RR00.8,IRIN, University of Nantes, http://www.sciences.univnantes. fr/irin/Vie/RR/;
[48] Agile (2010), Manifesto for Agile Software Development;
[49] Boehm B., Turner R. (2003), Balancing Agility and Discipline. Addison- Wesley;
[50] Mili H., Fayad M., Brugali D., Hamu D., Dori D. (2002), Enterprise frameworks: issues and research directions, Software - Practice and Experience, Softw. Pract. Exper;
[51] Ragunath P. K., Velmourougan S., Davachelvan P., Kayalvizhi S., Ravimohan R. (2010), A New Model (SDLC Model-2010) for Software Development Life Cycle (SDLC), IJCSNS International Journal of Computer Science and Network Security, Vol.10 No.1, January;
[52] Seidewitz E. (2003), What Models Mean. IEEE Software, 20(5);
[53] Estefan, J. A. (2007). Survey of model-based system engineering (MBSE) methodologies, pp.1-47, INCOSE MBSE Focus Group, May 25;
[54] Laudon K.C., Laudon, J.P., Management information systems, managing digital firm, 15 th edition, 2018;
[55] C. Warren Axelrod, Engineering Safe and Secure Software Systems, ARTECH HOUSE, 2013;
[56] National Institute of Standards and Technology Interagency Report 7628, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, 2025;
[57] van der Aalst W. M. P, Ter Hofstede, A. H. M. (2000), Verification of Workflow Task Structures: A Petri-net-based Approach, In: Information Systems;
[58] Wilkinson, G. & Dale, B.G., Models of management system standards: a review of the integration issues, IJMR, 1999;
[59] Abrahamsson P., Salo O., Ronkainen J., Warsta J. (2002), Agile Software;
[60] Johannesson P., Perjons E. (2001), Design principles for process modellingin enterprise application integration. Information Systems, 26(2), Special Issue on Practical Applications of Agents;
[61] Vliet H. (2007), Software engineering: Principles and Practice, Wiley;
[62] . Velev T., Dobrinkova N., "The logical model of unify, innovative Platform for Automation and Management of Standards (PAMS)" 1st International Scientific Conference Digital Transformation, Cyber Security and Resilience" DIGILIENCE2019, Sofia 2-4 October 2019. ISIJ Digital Transformation, Cyber Security and Resilience, ISSN 0861-5160 (print), ISSN 1314-2119 (online), vol. 43, no. 1 (2019): 113-120, DOI: https://doi.org/10.11610/isij.4310, 2019, p.113-p.120;
[63] Gokul. S., Web Service Security Architectures;
[64] Kleppe A., Warmer J., Bast W. (2003), MDA Explained: The Model Driven Architecture Practice and Promise. Addison Wesley, 2003;
[65] Channabasavaiah, K., K.Holley, M. Edward and Jr. Tuggle (2003). Migrating to a service-oriented architecture, Part 1, www-106.ibm.com.;

[66] Aaron Skonnard, "Understanding SOAP", Microsoft Corporation;
[67] Heather Kreger, "Web Services Conceptual Architecture (WSCA 1.0)", IBM Software Group, May 2001, redebooks.ibm.com.;
[68] Summers R., Secure Computing: Threats and Safeguards, McGraw-Hill, 1997;
[69] Colgrave J., Januszewski K., "Using WSDL in a UDDI Registry, Version 2.0.2", OASIS, 31 June 2004;
[70] D. Clark, Next-Generation Web Services, IEEE Internet Computing, Volume: 6 Issue: 2, Mar/Apr 2002;
[71] Martin F.T., Top Secret Intranet, Prentice-Hall Inc, ISBN 0-13-080898-9, 1999;
[72] Guizzardi G. (2007), On Ontology, ontologies, Conceptualizations, Modeling Languages, and (Meta) Models, In Frontiers in Artifical Intelligence and Applications, Databases and Information Systems IV, ISBN 978-1-58603-640-8, IOS Press, Amsterdam;
[73] Ackley, David H.; Hinton, Geoffrey E.; Sejnowski, Terrence J. (1985). "A Learning Algorithm for Boltzmann Machines". Cognitive Science. 9 (1): 147–169. doi:10.1207/s15516709cog0901;
[74] R. R. Salakhutdinov and H. Larochelle. Efficient learning of deep Boltzmann machines. In Proceedings of the International Conference on Artificial Intelligence and Statistics, 2010.;
[75] R. R. Salakhutdinov and G. E. Hinton. An efficient learning procedure for Deep Boltzmann Machines. Neural Computation, 24:1967 – 2006, 2012;
[76] Hinton, Geoffrey; Salakhutdinov, Ruslan (2012). "A better way to pretrain deep Boltzmann machines" . Advances in Neural. 3: 1–9;
[77] Haohan Wang, Bhiksha Raj "On the Origin of Deep Learning" https://doi.org/10.48550/arXiv.1702.07800;
[78] Takayuki Osogami, "Boltzmann machines and energy-based models", arXiv:1708.06008, , 2024;
[79] Marshall, G.H.S., Evaluating Management Standards: empirical research into the Scottish Quality Management May-2006, University of Stirling;
[80] Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/, 2025