СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ”
**Катедра „Бизнес Информатика”**

**Юрий Иванов Кузнецов**

# Приложение на архитектурния подход за изграждане на система за информационна сигурност във висше училище в България

## АВТОРЕФЕРАТ

на дисертационен труд за присъждане на образователната и научна степен „ДОКТОР” по научната специалност „Приложение на изчислителната техника в икономиката“

**Научен ръководител:**
**Доц. д-р Веселин Попов**

Свищов
2018 год.

Дисертационният труд е обсъден и насочен за защита от катедра „Бизнес информатика“ при Стопанска Академия "Д. А. Ценов" – Свищов. Авторът е асистент към катедра „Бизнес информатика“ при Стопанска Академия "Д. А. Ценов" – Свищов. Изследванията и разработката са извършени в същото висше училище.

# I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

## 1. Актуалност на проблема

Архитектурният подход дава възможност за цялостен преглед на всички елементи на една система от различни гледни точки. Той може да се разглежда като процес на описание на отделните компоненти на една организация и разработване на план за изграждане на интегрирана система, съобразена с бизнес процесите и целите й за развитие. Освен като процес на описание и изграждане, архитектурата на организацията е процес, насочен към нейното развитие и трансформирането й в нова архитектура за постигане на целите. Важно място тук заема синхронизирането на целите на организацията и приложението на ИТ.

Архитектурата за информационна сигурност има своите особености, обусловени както от архитектурата на организацията, така и от спецификите на нейното прилагане, в зависимост от влиянието на външната среда, в която функционира самата организация. Важното място на съвременното висше училище (ВУ), повишаването на ролята на висшето образование, все по-голямото внимание, което се обръща на информационната сигурност и защитата на личните данни и не на последно място фактът, че голяма част от висшите училища се финансират с публични средства, ***определят изследването на проблемите при изграждане на системите за информационна сигурност като актуална и социалнозначима тема***.

## 2. Обект и предмет на изследването

***Обект*** на изследване в дисертационния труд са системите за информационна сигурност във висшите училища в Република България, без да се извършва разграничаване между държавни и частни образователни институции. ***Предмет*** на изследване е изграждането на посочените системи чрез използването на архитектурен подход. В аналитичен ракурс вниманието в разработката е фокусирано върху спецификата на системите за управление на съвременните висши училища и как техните особености влияят върху прилагането на архитектурния подход.

## 3. Изследователска теза

***Тезата***, която се развива в дисертационния труд, е, че информационните системи в едно съвременно ВУ имат своите специфични особености, които изискват развитие на комбиниран итеративен архитектурен подход при изграждането на система за информационна сигурност. Комбинирането се налага не само на ниво различни рамки за описание на архитектурите, но и поради добавянето на подходи при оценка на постигнатите резултати и измерване на цялостната ефикасност и ефективност на системата.

## 4. Цел и задачи на дисертационния труд

В съответствие с отстояваната теза, в рамките на изследването е поставена следната основна ***цел*** – *да се аргументира архитектурен подход за изграждане и оценка на системата за информационна сигурност в рамките на системата за управление на висшето училище в България.* За постигане на основната цел са поставени следните конкретни ***задачи***:

- Да се анализират положителните страни и проблемите при използването на архитектурния подход в предприятията чрез теоретично изследване на научната литература и актуалното законодателство.
- Да се дефинират особеностите на архитектурите за информационна сигурност и техните различия спрямо архитектурата на предприятието.
- Да се направи характеристика на системите за управление на иновативното ВУ и особеностите на елементите на неговата система за информационна сигурност.
- Да се дефинира подходяща рамка от архитектурни решения за изграждане и оценка на архитектурата за информационна сигурност с възможност за практическо изграждане на такава система във ВУ.
- Да се конкретизират съществуващите проблеми и да се изведат възможностите за тяхното решаване с цел повишаване качеството на системите за информационна сигурност във ВУ.

На тази основа, при реализирането на поставената цел и решаването на очертаните задачи, основано на задълбочено изследване на системните компоненти и идентифициране на слабите им страни, ще се посочат основните проблемни области при практикоприложното изграждане на системите за информационна сигурност.

## 5. Методология на изследването

При разработването на дисертационния труд са приложени *дедуктивният и индуктивният подход*. Извършено е теоретично изследване на мястото, ролята и значението на информационната сигурност за управлението на ВУ и необходимостта от архитектурен подход при изграждането на системата за информационна сигурност в едно ВУ. Последователно са разгледани и анализирани понятията *архитектура на предприятието, архитектура на информационна сигурност,* както и възможностите за тяхното комбиниране и допълване. Чрез *анализ* на нормативната уредба се дефинира необходимостта от изграждането на система за информационна сигурност във ВУ и са анализирани нейните компоненти. Използван е методът на *абстракция*, за да се дефинират общите елементи в една система за сигурност във висшите училища в България.

В хода на изследването е използван *сравнителен анализ* на особеностите на системите за управление в едно ВУ спрямо тези на класическата бизнес организация. Използван е *системният подход* за разглеждане в цялост на всички компоненти на системите за информационна сигурност чрез *синтезиране* на резултатите от анализа на специфичните особености на системите за управление на висшите училища и произтичащите от това особености на системите за информационна сигурност. Поради спецификата на проблема при изследването е използван и натрупаният *практически опит* на автора[1]. Направени са различни *логически изводи,* базирани върху този опит.

На базата на изследването е *апробиран модел* за приложение на архитектурния подход за информационна сигурност в конкретно ВУ.

[1] Заб. Опитът е натрупан при изпълнение на служебни отговорности като експерт и одитор по информационна сигурност в Стопанска академия „Д. А. Ценов“ – Свищов.

## 6. Ограничения на изследването

В рамките на изследването се вземат предвид следните ***ограничения***:

Поради специфика на информацията, свързана с проблемите на сигурността, са използвани данни от проучвания, направени извън България. Това се предопределя от факта, че в България няма ясно дефинирана нормативна рамка за следене, съхранение и контролиране на достъпа до данните за нарушения, свързани с информационната сигурност. Поради този факт, ръководствата на висшите училища смятат, че би възникнал имиджов проблем, ако разпространят подобни данни (особено към техни конкуренти).

Предложената методика за изграждане на информационна сигурност, независимо от опита за абстракция и унификация, е насочена към ВУ с вече установени традиции и държавно финансиране. Това оказва съществено влияние върху използвания подход при дефиниране на стъпките на методиката, като се отчитат спецификите на основните, управленските и спомагателните процеси в този вид висши училища.

# II. СТРУКТУРА НА ДИСЕРТАЦИОННИЯ ТРУД

## 1. Общо описание

Дисертационният труд е разработен в общ обем от 226 страници, в т.ч. основен текст – 206 страници, 4 приложения, 25 таблици, 32 фигури, 121 литературни източника.

## 2. Съдържание на дисертационния труд

**ВЪВЕДЕНИЕ**

**ПЪРВА ГЛАВА. Архитектурен подход за изграждане на системата за информационна сигурност в предприятията**

1. Архитектурният подход – основа на ефективно работеща информационна система

1.1. Необходимост от архитектурен подход при изграждане на информационната система на предприятието

1.2. Дефиниция на архитектурата на предприятието и нейните компоненти

1.3. Основни компоненти на методиките за изграждане на архитектура на предприятието

2. Особености на архитектурата за информационна сигурност на предприятието

2.1. Място на архитектурата за информационна сигурност в архитектурата на предприятието

2.2. Модел SABSA за изграждане на архитектура за информационна сигурност в предприятието

2.3. Оценка на риска в архитектурите за сигурност

3. Изграждане и оценка на архитектурата за информационна сигурност

3.1. Модели за дефиниране на политики за връзки между субектите и обектите в системите за сигурност

3.2. Модели за оценка на системите за сигурност

3.3. Връзка на архитектурата за сигурност с елементите на бизнес системата

**ВТОРА ГЛАВА. Критичен анализ на особеностите на системата за информационна сигурност във висшето училище**

1. Предизвикателства към съвременното висше училище в 21-ви век

1.1. Нова парадигма за развитието на висшето образование и новите функции на висшето училище

1.2. Промяна в начините за осъществяване на учебния процес

1.3. Промяна в начините на приложение на информационните и комуникационните технологии в съвременното висше училище

2. Особености на информационната система на висшето училище

2.1. Компоненти на информационната система за управление на висшето училище

2.2. Специфични особености на информационната система за управление на висшето училище

2.3. Характерни черти на системата за управление на висшето училище

3. Особености на системата за информационна сигурност във висшето училище

3.1. Необходимост от изграждане на система за информационна сигурност във висшето училище

3.2. Особености на системата за информационна сигурност във висшето училище

3.3. Анализ на защитеността на публичната комуникационна инфраструктура на висшите училища в България

**ТРЕТА ГЛАВА. Методика за изграждане на система за информационна сигурност във висшето училище чрез използване на архитектурен подход**

1. Дефиниране на стратегия и планиране на процеса по изграждане на системата за информационна сигурност

1.1. Подготовка на програмата по изграждане на архитектура за информационна сигурност

1.2. Изграждане на контекстуална архитектура

1.3. Изграждане на концептуална архитектура

2. Проектиране на системата за информационна сигурност

2.1. Проектиране на логическата архитектура

# III. КРАТКО СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

## Първа глава. Архитектурен подход за изграждане на системата за информационна сигурност в предприятията

В първа глава от дисертационния труд се представя авторски критичен анализ на особеностите на архитектурата за информационна сигурност, нейните особености спрямо архитектурата на предприятието и необходимостта от тяхната интеграция. Разгледани са възможностите за комбинация на архитектурните решения и начините за оценяване на изградената система.

В **първия параграф** е разгледана необходимостта от прилагане на архитектурен подход при изграждане на информационната система на едно предприятие. Според Шишманов[2], Лаудън[3] и други автори с най-голяма възвръщаемост, но и с най-голям риск се явява смяната на парадигмата, която включва цялостно преосмисляне на естеството на бизнеса и естеството на организацията. Промяната на парадигмата и редизайнът на бизнес процесите често се провалят, защото изискват предварителен анализ, подготовка и сложна организация при тяхното осъществяване.

При реализирането на такава сложна програма най-подходящо е използваното на архитектурен подход. Архитектурата на предприятието отразява най-важното от бизнеса, ИТ и тяхната връзка и еволюция. Ето защо архитектурата е полезна в запазването на най-важното за бизнеса, като същевременно позволява максимална гъвкавост и адаптивност. Без добра архитектура е трудно да се постигне бизнес успех. Най-важната характеристика на архитектурата на предприятието е, че тя осигурява цялостен поглед върху предприятието.

В резултат на направения преглед на научната литература, свързана с теоретичните постановки за архитектурата на предприятието, са направени следните изводи:

[2] Шишманов, К. Анализ на възможностите за развитие на информационните системи на предприятията. // Бизнес управление, Година XXIII, кн.2, стр. 83-100; Академично издателство „Ценов“, Свищов, 2013.

[3] Laudon, K., Laundon, J. Management Information Systems, 14 ed., Pearson Education Limited 2016.

- Архитектурата на предприятието може да се разглежда като процес на описание на отделните компоненти на предприятието и разработване на план за изграждане на интегрирана система, съобразена с бизнес процесите и целите за развитие.
- Архитектурата на предприятието предоставя цялостен поглед върху системата и дава възможност да бъдат визуализирани отделните елементи през призмата на различни нива на абстракция.
- Архитектурата на предприятието е процес на развитие на архитектурата и нейното трансформиране в нова архитектура за постигане целите на бизнеса.
- Архитектурата на предприятието подпомага синхронизирането на бизнес целите на предприятието и приложението на ИТ.
- Архитектурата се намира в тясна взаимовръзка с останалите елементи на системата за управление.

Съществуващите архитектурни методики може да бъдат систематизирани в следните основни групи:

- матричен тип (например методика на Захман) – методики, при които имаме описание на елементите във вид на матрица;
- карти на бизнес процесите (APQC) – двумерни схеми;
- структури, базирани на нива (FEAF, TEAF, PBGC) – отделните нива се представят във вид на тримерни фигури, като кубове или пирамиди;
- процесно ориентиран (TOGAF) – методиката съдържа последователността от действия за изграждане на архитектурата;
- планиране и добри практики (EAP);
- базирани на референтни модели (FEA);
- метамодели (DoDaf).

Класифицирането може да се фокусира към три аспекта при изграждането на архитектура на предприятието:

- начин на описание на текущото и бъдещото състояние на системата;
- начин за трансформиране на системата;
- начин за съхранение и класифициране на добрите практики и моделите.

Във **втория параграф на първа глава** са разгледани особеностите на архитектурата на информационна сигурност в предприятието.

Използването на ИТ в предприятието е свързано не само с повишаване на ефективността на бизнес процесите, но и с осигуряване сигурност на информацията при автоматизираната ѝ обработка, съхранение и пренасяне. Това предполага, сигурността да залегне като основен компонент в архитектурата. Съвременните методологии за изграждане на архитектурата на предприятието акцентират на този аспект, като посочват, че информационната сигурност има следните особености[4]:

- архитектурата на сигурността има собствена методология;
- архитектурата на сигурността предполага различни архитектурни гледни точки;
- архитектурата на сигурността се характеризира с вертикални връзки, преминаващи през различните елементи и изгледи, без те да бъдат повлияни от конкретния бизнес процес;
- елементите на архитектурата по сигурността имат уникално целево предназначение;
- изграждането на архитектурата изисква допълнителни специализирани умения и компетенции в предприятието и конкретните ИТ архитекти.

Могат да бъдат изведени и дефинирани следните изисквания, на които да отговаря архитектурата за информационна сигурност на предприятието:

- да представлява **опростена, дългосрочна визия за управление**. Без да се прави компромис с нивата на сигурност, архитектурата трябва да осигурява необходимото ниво на сигурност, без да влиза в противоречие с бизнес целите на организацията;
- да представлява **единна визия за елементите за сигурност**. Архитектурният цялостен подход на разглеждане елементите на системата позволява намирането на потенциални слабости и дефекти в системата;
- да предоставя **начин за трансформиране и усъвършенстване**. Проблемите, открити в системата за сигурност, трябва да дават възможности за трансформирането на архитектурата в такава,

[4] TOGAF v9.2

позволяваща по-висока степен на сигурност. Този процес трябва да бъде в синхрон с бизнес процесите, да отчита финансовите параметри и да се базира на оценката на риска на заплахите.

- да е **достатъчно адаптивна**, за да може да посреща бъдещи заплахи, без да пречи на функционирането на съответните бизнес функции.

Целите пред архитектите на информационна сигурност трябва да бъдат обособени в следните направления:

- да предоставят на ИТ архитектите насоки за изграждане на архитектури с отчитане на сигурността и необходимите допълнителни инвестиции за осъществяване на този процес;
- да бъде изградена технологична инфраструктура, свързана със сигурността;
- да се извърши анализ на политиките и стандартите и да се разработят при необходимост допълнения;
- да опишат стратегии за подпомагане вземането на решения в областта на ИТ сигурността;
- осигуряване на съвместимост с външни изисквания на стандарти и регулации, свързани с ИТ сигурността и защитата на личните данни;
- прилагане добрите практики на актуалните стандарти и методологии;
- документиране на елементите на архитектурата за по-добра взаимовръзка с останалите елементи на архитектурата на предприятието;
- дефиниране на цялостната архитектура на сигурност в мястото на цялостната архитектура на предприятието;
- да се търси намаление на разходите, чрез използването на единни средства за осигуряване на защита.

Най-разпространеният модел за разработване на архитектура на информационната сигурност е SABSA[5], разработен от Джон Шервуд. В модела са доразвити идеите, заложени в холистичния модел на Захман. В настоящия момент SABSA е изпозлван в Министерството на отбраната на Великобритания, канадското

[5] Sherwood Applied Business Security Architecture.

правителство, ISACA и т.н. Стандартът е отворен и позволява лесна интеграция с други стандарти.

В структурно отношение моделът представя системата за сигурност в 6 различни ракурса (вж. фиг 1). Посочените шест архитектури съответстват на гледните точки на различните заинтересовани лица (вж. Таблица 1).


*Фигура 1. SABSA нива на представяне*[6]

*Таблица 1*

*Съответствие между архитектурите и гледните точки*

| **Архитектура** | **Гледна точка** |
|---|---|
| Контекстуална | Бизнес |
| Концептуална | Архитект |
| Логическа | Дизайнер |
| Физическа | Изграждащ |
| Компонентна | Създател |
| Управление на услугите (Оперативна) | Мениджър услуги |

[6] Източник: Адаптирано по SABSA.

В **третия параграф на първа глава** са особеностите на изграждането и оценката на архитектурата за информационна сигурност.

При оценка на моделите за дефиниране на политиките за връзка между субектите и обектите в системите за сигурност е направен извода, че за едно ВУ е най-подходящо да се използват модели, базирани на роли (RBAC – Role Based Access Control[7]). Моделите от този тип дават възможност правата да се пренасят на ниво отделно приложение. Тук по-добре се дефинират възможностите на един субект да има различни функции в една система. В резултат на това този субект получава повече от една роля в зависимост от процесите, в които участва. Особеното на модела е пренасянето на правата не върху конкретен обект, а върху транзакция, която може да включва повече от един обект.

На базата на направено проучване на литературата и емпирични изследвания са изведени и някой проблеми при прилагане на моделите, базирани на роли:

- **Наличието на сесии** – при изграждането на архитектури на предприятието описанието на сесиите не се явява част от методиките за описание на архитектурата. Въпреки някои предимства на сесийния подход, той затруднява практическата реализация на архитектурата. При създаването на политиките за определяне на роли ще трябва да се спазва правилото, че при авторизация на даден потребител той получава достъп до всички свои роли.
- Системи, при които е разрешено **наличието само на една роля**. Поради гореизложените причини смятаме, че ако в една система даден потребител се ограничава само с една роля в сесия, при системи, при които един потребител има няколко роли, ефективността на система ще бъде силно компрометирана.
- **По-добра йерархична система**. При изграждане на йерархични структури на роли трябва да има яснота за трансформиране на структура, наследяването на роли и делегиране на права.
    - **Брой на потребителите** – по принцип всеки потребител е обект и потенциален участник в дадена роля. При голям брой потребители предварително трябва да се анализират какви са уникалните роли, за да се прецени колко роли се разпределят на обектите.

[7]Ferraiolo, David F., Kuhn, D. Richard. Role-Based Access Controls, 15th National Computer Security Conference, 1992.

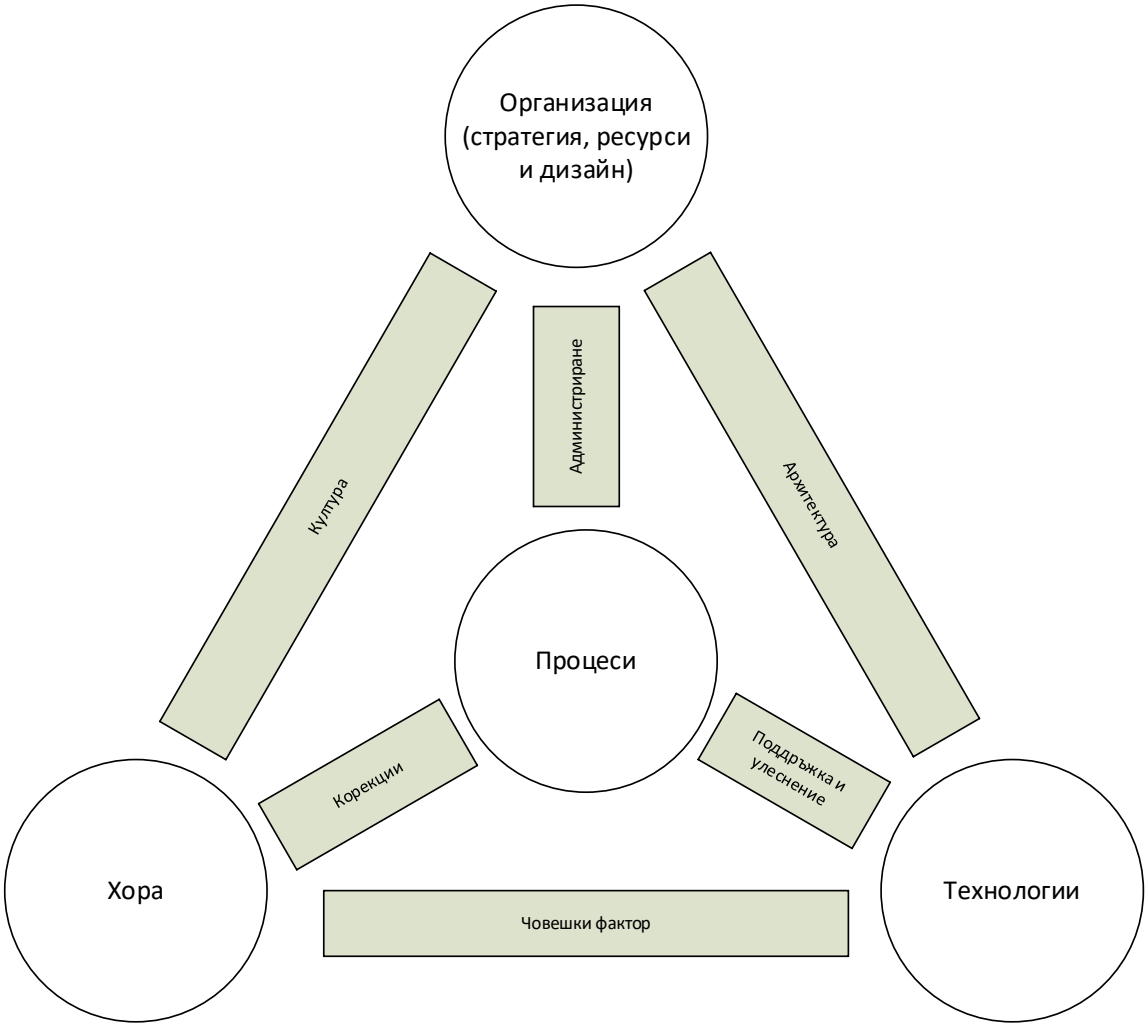
- **Брой на системите**. Влиянието на системите върху броя на ролите е в експоненциална форма. Ако една система изисква около 20 роли, при 10 системи ролите нарастват на 6500!
- **Управление на ролите на субектите**. Във функционирането на системата има динамика на ролите. Тези промени се появяват при промяна на задължения на отделен субект или структурно звено. При промяна на роля трябва да има механизъм за контролиране, дали субектът покрива критериите за новата роля. Това изисква ясно разписани правила за управлението на ролите.
- **Цена на ролевия модел**. Трябва да се има предвид, че внедряването на модела изисква не малки финансови ресурси и допълни изисквания към персонала за управление на ролите.

При изграждане на архитектура за сигурност архитектът трябва да разполага с точни изисквания към системата. Това предполага запознаване с целите на управление, изискванията на собствениците на процесите и ИТ специалистите в предприятието. Първоначално трябва да бъдат разработени основните принципи на изграждане на архитектурата. При процеса на детайлизация на елементите на архитектурата трябва да се търси съответствие с тези принципи. Заедно с принципите е необходимо да се разработят изискванията към архитектурата. Извикванията могат се обособят в две основни групи:

- **Функционални изисквания** – определят задачите, които трябва да бъдат реализирани при изграждане на архитектурата. Описват се активите, подлежащи на защита, начините на защита, видовете уязвимости и т.н. Функционалните изисквания описват кои елементи на архитектурата за сигурност ще бъдат включени в нея.
- **Нефункционални изисквания** – определят параметрите на архитектурата на системата, описващи нейното качество. В тази група изисквания се определят различни критерии за надеждност и производителност.

За нуждите на архитектите по информационна сигурност ISACA разработва методика за разглеждане на информационната сигурност през призмата на бизнес

процесите в предприятието, наречена BMIS[8] . В нея са описани основните **елементи** на системата за сигурност и **връзките** между тях (вж. фиг. 2).




Фигура 2. Структура на BMIS

[8] Business model for information security, ISACA, 2010.

# Втора глава. Критичен анализ на особеностите на системата за информационна сигурност във висшето училище

Във втора глава от дисертационния труд е представен авторски критичен анализ на особеностите на системата за информационна сигурност във ВУ с фокус върху триединството от процеси – обучение, изследвания, администриране за целите на осигуряване качеството на функциониране и конкурентоспособността на институционалното развитие.

Специално внимание е обърнато на различни слабости на елементите в системите за сигурност на висшите училища. За тази цел са анализирани уязвимостите на Интернет свързаността на ВУ с помощта автоматизирани аналитични инструменти. Предложени са решения, които отчитат изискванията на действащата нормативна база и на добрите практики.

В **първия параграф** се анализират предизвикателствата към съвременните висши училища, които влияят върху процесите и прилагането на информационните и комуникационните технологии.

През последните години както в международен, така и в национален мащаб се забелязва формирането на нов модел на висшето образование, който съществено се различава от традиционния, познат до скоро модел. Новата парадигма се обуславя от новите изисквания, поставени от потребностите на общественото развитие. Тези изисквания са толкова специфични и различни от познатата ни до този момент система, че налагат радикални промени в стратегията, формите и методите за обучение, системата за управление на ВУ и респективно радикални промени в управленската информационна система.

Проучванията показват нуждата от промяна в начина на функционирането на университетите:

- **гарантиране на много по-голямо разнообразие**, отколкото досега, по отношение на целевите групи, режими на обучение, входни и изходни точки, съчетанието от дисциплини и компетентности в учебните програми и т.н.;
- **установяване на повсеместна "култура на високи постижения"**, която се концентрира върху финансиране не само в центрове и мрежи, които вече са

дали резултат в определена област на научни изследвания или обучение, но също и в такива, които имат потенциала да станат перспективни;

- **да се осигури по-голяма гъвкавост на пазара на труда в преподаването** чрез пълно използване потенциала на информационните и комуникационните технологии;
- **разширяване на достъпа чрез многообразие от програми**, по-голяма мобилност, подобряване на професионалното ориентиране и консултиране, гъвкава политика на приемане и по-евтини такси (стипендии, заеми, настаняване на достъпни цени и т.н.);
- **улесняване на признаването на придобито ниво на знание**;
- **укрепване на човешките ресурси на университетите чрез насърчаване на благоприятна професионална среда**, основана по-специално на открити, прозрачни и конкурентни процедури;
- **създаване на европейска рамка за висше образование** и мрежа от агенции за осигуряване на качеството.

Съчетаването на новата парадигма за развитие на висшето образование и външните фактори променя начина на функциониране и управление на ВУ. Забелязва се употребата на все повече „бизнес“[9] подходи при администриране. Прилагат се различни количествени методи за оценка на процесите. При управлението на академичния персонал също се възприемат подходи по планиране, постоянно обучение, наставничество и други, рядко използвани във висшето образование до този момент методики.

Дефинирани са особеностите на Иновативното ВУ (И-ВУ) и различията му спрямо традиционното ВУ (Т-ВУ).

В настоящия момент се отбелязват следните нови тенденции в осъществяване на учебния процес:

- „обръщане“ на класната стая (Flipped Classroom);
- онлайн курсове с голям брой записани студенти (MOOC);
- виртуализация на висшите училища.

[9] Rondo-Brovetto, P., Saliterer, I. The University as a Business?, VS Verlag für Sozialwissenschaften | Springer Fachmedien Wiesbaden GmbH 2011.

Извършването на кардиналната промяна на висшето образоване изисква използването на съвременните информационни и комуникационни технологии в следните направление:

- подпомагане на осъществяването на преподавателската и научноизследователската работа чрез внедряване на иновативни методи за обучение;
- изграждане на интегрирана система за управление на процесите във ВУ;
- съхранение на интелектуалната собственост на ВУ.

Във **втория параграф на втора глава** се разглеждат особеностите на информационната система на ВУ. Разглеждат се особеностите, които оказват влияние на информационната сигурност.

Структурата на връзките и информационните потоци в системата за управление на едно ВУ е сложна и на пръв поглед объркана. Анализът показва, че системата се различава от системите в други отрасли не само по отделните процеси, но и по взаимовръзките и участниците в тези процеси. За нуждите на системата за защита на данните ще се спрем на следните специфични особености:

- академична култура и традиции;
- организационна структура;
- място на обучаемите в процесите.

Академичната култура и традициите са отличителна черта на едно ВУ. Създадени от преди повече от 50 години, учебните заведения се гордеят със своята история, дух и традиции. Силата на едно ВУ е съчетаването на тези традиции с динамиката на съвременното общество. Основно предизвикателство пред съвременното ВУ е нуждата от реинжинеринг на процесите, за да се постигне по голяма конкурентоспособност. Особеното на процесите е, че периодът на някои от продуктите е голям. Например образователният продукт (услуга) в ОКС „бакалавър“ е с „производствен“ цикъл от четири[10] години. Това означава, че, правейки промени, трябва да се мисли за започналите своето обучение студенти, за да се избегнат сътресения.

[10] Заб. Смятаме, че законодателните промени с идеи за съкращаване на периодите за обучение не биха повлияли положително в България.

Често, за да се запази някакъв вид приемственост, вместо да се ревизира даден процес, се добавя нов процес и съответно звено, което да го реализира. Изграждането на центрове или други помощни звена по-скоро затормозява цялата система, отколкото да повиши качеството. В даден момент се появяват множество паралелно протичащи сходни процеси, управлявани по различен начин.

Специфична особеност на системата за управление във ВУ е организационната структура и йерархичната подчиненост. На трудов договор в едно ВУ има две групи персонал: академичен състав (хабилитиран състав, нехабилитиран състав и преподаватели) и неакадемичен състав (администрация, поддръжка, обслужващ персонал и т.н.). Спецификата във ВУ в това отношение се изразява в следните направления:

- **Културни различия между двете групи персонал**;
- **Участие на академичен състав в управлението**;
- **Наличие на паралелни йерархии**;
- **Участие в повече от една йерархия;**
- **Управление на персонала;**
- **Наличие на участници, които не са на основен трудов договор**.

Специфична особеност е и мястото и ролята на студентите в едно ВУ. Още се води дискусия дали те са продукт, клиент или участник. И доколко те са вътрешни или външни за системата за управление на ВУ. Смятаме, че няма еднозначен отговор поради следните причини:

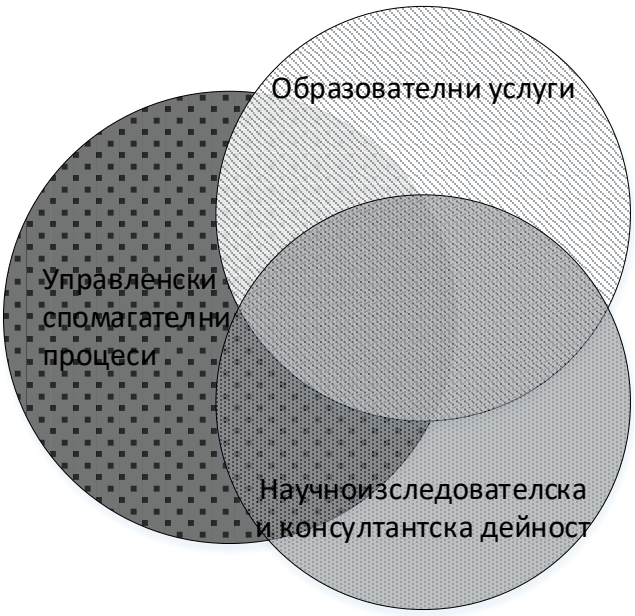
- **Разнообразие на обучаемите в едно ВУ**.
- **Различни гледни точки върху ролята на отделния обучаем.**
- **Пряко участие на обучаемите в процеси, различни от тяхното обучение**.
- **Ролята на родителите и спонсорите.**

Системата за управление (СУ) на едно ВУ е комплексна и интегрирана система. Тя е изградена от модули, които могат да бъдат класифицирани в следните три основни групи (вж. фиг. 3):

- **Обучение**. Тук се намират системите за управление на: планирането и приема на обучаеми; студентското състояние и студентското портфолио; учебната

документация; аудиторния фонд; учебната натовареност; обучителния процес и др.

- **Научноизследователска и консултантска дейност**. Елементи на тази група са системите за управление на: научноизследователските проекти; наблюдение на публикационната дейност; електронните публикации; дейностите на редколегии и др.
- **Системи за автоматизация на спомагателните и управленските процеси**. В тази група попадат модулите за: финансово-счетоводна дейност; обществени поръчки; СФУК; личен състав и ТРЗ; научно израстване; системите за електронен документооборот; поддържането на уебпортал; автоматизиране на процесите по атестиране и акредитация; библиотечните информационни системи; системите за управление на настаняването в общежития; управление на активите; системите за управление на качеството и др.




Фигура 3. Елементи на СУ във висше училище

При анализ на информационната система за управление на ВУ се откриват следните тенденции:

**Концентрация на дейностите в компютърните центрове на ВУ и тяхното претоварване**;

**Дублиране на ИТ решения в основните и първичните звена;**

**Разработки на други звена.**

Направен е изводът, че интензивността в използването на ИКТ и нарастващата сложност на приложенията не позволяват разглеждането на ИКТ като задача, която трябва да бъде решена само от една структурна единица. Напротив, те правят ИКТ хоризонтален въпрос за цялата институция, тъй като броят на участващите и извършените дейности непрекъснато нараства. Това поставя нови предизвикателства пред управлението по-важните от които са свързани с това:

- да се предвидят промените и да се балансира между различните тенденции и интереси;
- да се осигурят устойчиви ресурси, но също и грижа за ограничаване на разходите, да се осигури ефективност и възвръщаемост на инвестициите;
- да се осигури място за експерименти, но също така и да се насочат усилията към стандартизация и по-широко използване на инфраструктурата;
- да се минимализират в умерени граници конфликтите на интереси, например между академични звена и административните единици;
- да се запази балансът между техническите обещания и практическата приложимост;
- при внедряване на нови ИКТ да се осигури по-високо ниво на информационна сигурност;
- да се осигури съобразяване на целта на техническите иновации и организационната промяна с академичната мисия на институцията.

За да отговори на тези предизвикателства, управлението на ИКТ следва да се разглежда като важна задача за централното управление на ВУ. Задачите се простират далеч отвъд простото управлението на техническата инфраструктура. По тази причина смятаме, че е необходимо използването на архитектурния подход при реализацията на трансформирането на ВУ в едно високо технологично и конкурентоспособно средище за предоставяне на образователни и консултантски услуги.

В **третия параграф на втора глава** са разгледани особеностите на системата за информационна сигурност във ВУ.

В последните години се забелязва тенденция за увеличение на пробивите на сигурността във висшите училища. Информационните системи на едно ВУ са привлекателни мишени за хакерите, защото не съдържат само финансови и лични

данни, но и ценна интелектуална собственост. Тези заплахи принуждават академичните среди да направят преоценка на начина, по който се съхраняват и защитават огромни регистри от информация, често намиращи се в децентрализирани компютърни мрежи, достъпни за хиляди студенти, преподаватели и изследователи.

Нуждата от защита на данните и информацията на дадено ВУ може да бъде структурирана в следните направления:

- законови и нормативни изисквания;
- опазване на собствената интелектуална собственост;
- осигуряване на непрекъснатост на процесите;
- имидж на ВУ.

Разгледани са особеностите на системата за информационна сигурност в ВУ според структурата, предложена в стандарт ISO 27001.

Иновативното ВУ е немислимо без качествена връзка до Интернет за нуждите на обучението и научноизследователската дейност. Обучаемите трябва да имат осигурен качествен дистанционен достъп до ресурси за обучение и различни административни услуги, предоставяни от ВУ. За това е препоръчително, ВУ да разполага с минимум два доставчика на Интернет и връзка по IPv4 и IPv6. За по-добро управление на трафика и използване на динамични протоколи за маршрутизиране (BGP) добра практика е, ВУ да разполага със собствено адресно пространство и собствена автономна система (AS). За проверка на прилагането на добрите практики е проведено изследване на мрежите на висшите училища в България, при осъществяването на което са използвани инструменти за IP сканиране и информацията от регионалния за Европа Интернет регистър RIPE. Направеният анализ показва, че само две висши училища удовлетворяват тези изисквания за надеждност.

Правилното използване на HTTPS при изграждането на защитена архитектура във ВУ се явява сериозно предизвикателство. Проучване на използваните цифрови сертификати в сайтовете на водещите ВУ в България показва непознаване на добрите практики и произтичащите от това рискове. С цел проследяване на напредъка при прилагането на HTTPS са направени два анализа: през 2016 и през 2018. Анализът през 2018 година показва, че има подобряване на ситуацията, но все още има проблеми при прилагането на защитени протоколи. Някои университети използват безплатния издател

на сертификати Let’s Encrypt, което по наше мнение носи определени рискове. Все още се забелязва, че независимо от наличие на сертификати те не са правилно конфигурирани и сайтовете са уязвими на различни видове атаки.

# Трета глава. Методика за изграждане на система за информационна сигурност във висшето училище чрез използване на архитектурен подход

Трета глава представя детайлно описание на процесите по изграждането на архитектура на ВУ, като се спазват предписанията на модела SABSA. На всеки етап от реализацията се фокусира върху особеностите на ВУ, които изискват специално внимание при имплементирането на методиката. Като се отчитат тези особености, в дисертацията са предложени различни регистри, които ще улеснят автоматизацията на процесите по изграждането на архитектурата. Голяма част от предложенията са апробирани в процеса на изграждане на системата за информационна сигурност в Стопанска академия „Димитър Апостолов Ценов“ Свищов.

Представена е методика, описваща детайлно начина на реализация на основните дейности при изграждане на архитектурата на информационна сигурност:

- дейности по подготовка;
- изграждане на контекстуална архитектура;
- изграждане на концептуална архитектура;
- проектиране на логическата архитектура;
- проектиране на физическата архитектура;
- проектиране на архитектурата на компонентите;
- управление на политиките за информационна сигурност;
- администриране на информационната сигурност и управление на оперативния риск;
- измерване на информационната сигурност.

В **първия параграф** е описан процесът по дефиниране на стратегия и планиране на процеса по изграждане на системата за информационна сигурност във ВУ.

Стартирането на процеса по изграждане на архитектурата на информационна сигурност се предхожда от сериозни подготвителни дейности. Тези дейности са насочени в няколко направления:

- уточняване на инструментите за изграждане на архитектурата;

- детайлно аргументиране на ползите от архитектурата за информационна сигурност, на необходимостта от нейното изграждане, осигуряване на подкрепата на висшето ръководство на организацията;
- създаване на балансиран екип от специалисти с необходимата квалификация и мотивация;
- осигуряване на канали за събиране на информацията, необходима за изграждане на архитектурата;
- планиране и управление на програма за развитие на архитектурата за информационна сигурност;
- информационно-разяснителни дейности, насочени към основните групи потребители на ИС във ВУ, за да се преодолеят различни стереотипи относно сигурността и да се намери правилен подход за дефиниране на понятието „сигурност“, без противопоставяне с понятията „свобода“ и „академизъм“.

Поради ефикасното интегриране на SABSA с TOGAF, което би довело до по-добро развитие на цялостен архитектурен подход за организация от типа на ВУ, в изграждането на архитектурата за сигурност в едно И-ВУ е използван модела SABSA.

Ръководството на ВУ трябва да бъде убедено, че с изграждането на архитектура за информационна сигурност има за цел да се решат конкретни бизнес проблеми и трябва да разбира и адекватно оценява следните обстоятелства и проблемите, свързани с тях:

- наличие на огромен обем лични данни;
- наличие на интелектуална собственост и свързаните с нея авторски права;
- наличие на бизнес информация за партньорски организации и фирми.

При изграждането на екипи във ВУ съществува реален риск от небалансираност на екипа, породена от множеството йерархични структури. Наличието на представители на служители и преподаватели може да е проблем, защото културните нагласи в едно ВУ сочат, че академичният състав се възприема в ролята на ръководител и носител на идеи, независимо че може да има много по-квалифицирани специалисти с практически опит сред неакадемичния персонал. Създаването на екип само от неакадемичен състав може да доведе до неправилно интерпретиране на бизнес предизвикателствата пред ВУ и до неточно анализиране на основните процеси по обучение вследствие на тяхното

непознаване. От друга страна, създаването на екип само от академичен персонал може да доведе до изпускането на детайли по процесите, които са познати само на пряко ангажираните в тяхното администриране.

Поради тези причини е обосновано, че най-подходящо е изграждането на смесен екип с привличането на външен за ВУ наблюдаващ, който да балансира отношенията. По възможност в екипа трябва да бъдат привлечени вътрешни одитори по системата за управление на качеството. Най-гъвкави са екипи с брой на участниците до 10 човека. Екипи над 15 човека се смятат за трудни за управление.

***Контекстуалната архитектура*** има за цел да се разгледа информационната сигурност на ВУ е от гледна точка на организацията като цяло. На този етап се прави анализ на съществуващото състояние, структурата на процесите, извършва се оценка на риска:

Създаването на архитектура за информационна сигурност трябва да отчита специфичните особеностите на обекта, чиято защита управлява. Особеностите на И-ВУ могат да бъдат систематизирани по следния начин:

- Информацията като фактор за развитие на ВУ.
- Стабилност на информационните процеси и осигуряване на тяхната непрекъснатост
- Навременност и точност на информацията, която се подава на външни организации и партньори.
- Изисквания към сигурността на информацията, свързани с нормативната уредба.
- Зачитане на човешките и гражданските права.

Рисковете, свързани със сигурността в едно ВУ, ни позволяват да очертаем целите на архитектурата на защита. Основните групи рискове са:

- Рискове, свързани с бранда на ВУ.
- Рискове, свързани с измами.
- Рискове, свързани с прекъсване или нарушаване на процесите във ВУ.
- Рискове, свързани с нарушаване изисквания на различни нормативни документи и договори.
- Рискове, свързани с намаляване на доверието към ВУ.

Оценката на рисковите събития в модела, залегнал в SABSA, преминава през пет етапа. За по-добро структуриране на информацията е предложено да бъде изграден „Регистър на заплахите“. Част от регистъра се попълва при описание на контекстуалната архитектура, а друга негова част - при реализиране на концептуалната архитектура.

При анализа на особеностите на процесите във ВУ трябва да се обърне внимание, че дори преподавателите нямат 100% осигуреност на стационарни работни места. Това означава, че или се споделя един и същи компютър, или се работи през собствени устройства. Обучаемите също използват собствени устройства за достъп до ресурсите. Моделите за оценка на риска задължително трябва да отчетат тези особености.

***Концептуалната архитектура*** представлява визията за бъдещето. На базата на събраните данни за текущото състояние и оценката на рисковете архитектът изгражда общата визия за системата за информационната система на ВУ.

***Профилирането чрез бизнес атрибути*** представлява унифициран начин за оценка на бизнес целите и факторите за развитие на организацията чрез стандартни атрибути. За всеки фактор за развитие на бизнеса се съпоставят един или няколко бизнес атрибута За всеки бизнес атрибут съществува начин за измерване. За нуждите на профилирането в предложената методика е заложено да се изгради досие, което да съдържа описание на всеки фактор и свързаните с него бизнес атрибути. За всяка връзка фактор-атрибут се изпълняват следните стъпки:

- Описва се факторът за развитие на бизнеса.
- Посочва се бизнес атрибутът.
- Описват се същности на атрибута в конкретния контекст.
- Определя се начинът за измерване стойността на атрибута. Съществуват два типа измерване: точно измерване (hard metrics) и оценъчно измерване (soft metrics).
- Определя се технологията за измерване.
- Дефинират се целевите стойности на атрибута.
- Събиране на данните за стойностите (оценките) на атрибута и анализ на резултатите.

За дефинирането на контролните цели в едно ВУ се препоръчва да се използват готови набори от контролни цели. Най-подходящ източник се явява ISO 27002. В настоящия момент няма изискване, системите за информационна сигурност да се

сертифицират, но както беше отбелязано, съществува препоръка за организациите, извършващи електронни услуги на гражданите, да се придържат към стандарта ISO 27000. Може да бъдат използвани и други източници, съдържащи контролни цели, като например: ISO/IEC 21827 – “Systems Security Engineering Capability Maturity Model”, BSI- “IT Baseline Protection Catalogs”, Cobit – “Control Objectives for Information and Related Technology”, ISF “Standard for Good Practice” и други.

Важен елемент на концептуалната архитектура е дефинирането на **стратегия за информационна сигурност**. Важен принцип, който трябва да залегне в тази стратегия, е дефинирането на слоеве на защита около обектите, които трябва да бъдат защитавани Обектите в случая представляват информационните активи, явяващи се концептуализация на реалния бизнес. Около тях се разполагат останалите слоеве, всяко с различно ниво на детайлност. Най-близко до активите са криптографските контроли, които въздействат директно върху информационните активи. Във всяко по-външно ниво контролите стават все по-широко приложими. Основно предимство на този многослоен подход е, че се гарантира недопускането на една критична точка в мерките за сигурност. Ако една мярка не успее да спре инцидент по сигурността, съществуват други, които да се справят с него.

Във **втория параграф на трета глава** е описана методологията за проектиране на системата за информационна сигурност във ВУ.

***Логическата архитектура развива*** в детайли разработената концептуална архитектура. Тя има за цел да се придаде съдържание на скелета на концептуалната рамка. Логическият слой разглежда сигурността от функционална гледна точка и определя всеобхватен набор от функционални изисквания към отделните елементи.

Информационната сигурност изисква наличието на услуги за информационна сигурност, които да се грижат за достъпността, интегритета и поверителността на информацията. Част от бизнес атрибутите са пряко свързани с осигуряване сигурността на информацията. Услугите са логически елементи, определени независимо от това, какъв физически механизъм може да се използва, за да ги достави.

Основните типове услуги са:

- услуги за превенция;
- услуги за контрол и ограничаване;

- услуги за откриване и уведомяване;
- услуги по регистриране и проследяване на събития;
- услуги за възстановяване;
- услуги за подсигуряване.

Посочен е начин на реализиране на услугите, който отчита особеностите на ВУ.

Логическата архитектура изисква структурирано съхранение на всички участниците и техните привилегии. За целта се изгражда ***Схема на участниците и профили на привилегиите***. Схемата се състои от атрибути, правила за изграждане на атрибутите и класове на обектите. Трябва да се предвидят атрибути за добавяне на роли към даден обект.

***Физическата архитектура*** на сигурността представлява начина, по който изграждащият (строителят) ще реализира логическата функционалност на системата. На това ниво се конкретизират: описанията на градивните блокове и тяхната производителност; начинът и капацитетът на връзката между елементите, начините на защита на тези връзки и т.н. Тук се прави анализ на физическите структури на данните, които се използват, за да се определят механизмите на физическа защита, които ще реализират функционалността, залегнала в логическите услуги за сигурност :

При описание на модела на данните е необходимо да се определят конкретните методи на защита на тези данни. Контролират се два вида електронни ресурси: файлове и бази от данни. Въпреки високите нива на интеграция на информационните системи във ВУ, няма как да бъде избягнато използването на самостоятелни файлове за пренос и съхранение на данни. Комуникацията с обучаемите също се извършва на ниво файлове. Потребителите трябва да имат прозрачен механизъм за криптиране и проверка на интегритета на файловете. Това предполага използването на системи за управление и съхранение на документи (document management and storage systems).

Една от най-новите тенденции в съвременните системи за управление на бази данни е осигуряването на криптирането на данните в базата данни[11]. Технологично криптирането преминава от криптиране на статичните данни към криптиране на данните в движение. Така например, Microsoft Server разширява своята технология

[11] He, Jingmin and Min Wang, Cryptography and Relational Database Managemen Systems, IBM T. J. Watson Research Center.

Transparent Data Encryption (TDE) (налична във SLQ 2008) с технологията Always Encrypted(AE). Това е нова функция в SQL Server 2016, която криптира данните както в покой, така и в движение (и продължава да ги криптира в паметта)!

При изграждането на физическата системата трябва да се реализира висока защита на съхранението на данните. Използването на масиви от дискове (RAID 5/6) е задължително. Възможно е използването на файлови системи, осигуряващи висока надеждност на съхранение като: ZFS; GPFS; Btrfs.

При защитата на потребителите и приложенията съществено място имат механизмите за автентикация на потребителите. Поради големия брой обучаеми е трудно да се спазват добрите практики за управление на паролите за достъп. Често паролите за достъп се съхраняват в некриптиран вид, няма политика за задължителна смяна на паролата и не се поставят изисквания за нейната сложност. Използването на смарт карти за идентификация осигурява високо ниво на сигурност, но разходите за въвеждането на този вид автентикация са големи. По тази причина се търсят комбинирани методи за разширяването на приложението на смарт картите (използването им като разплащателно средство, електронна студентска книжка, карта за намаление и т.н.).

Концепцията на разделянето на производствената среда от средата за разработка придобива важно значение във ВУ поради факта, че в процеса на научноизследователската дейност се извършва разработка на различни модули.

Физическата топология на мрежата е реализацията на логическите области за сигурност. Тя се състои от реални елементи - рутери, защитни стени, сървърни платформи, клиентски платформи и т.н., и реалните мрежови връзки, както LAN и WAN.

***Архитектурата на сигурността на ниво компонент*** е конкретиката, свързана със закупуването на специализирани инструменти и компоненти, чрез които ще се реализира физическата архитектура. За намиране на специфичните инструменти и продукти трябва да бъдат извършени множество дейности по подбор и оценка, които трябва да бъдат базирани на стандартни принципи.

Детайлното проектиране на структурите на данни има следните цели:

- постигане на оперативна съвместимост между отделните системи на ниво данни;

- използването на стандартни методи за защита на тези данни при тяхната обмяна.

Спазването на стандартите е задължително условие при реализирането на компонентната архитектура. В първа глава на настоящия дисертационен труд бяха разгледани най-важните стандартни от гледна точка на използването им в архитектурния модел на ВУ. Беше отбелязвано, че сертифицирането на ВУ по стандарт ISO 27001 е икономически неоправдано, но принципите, залегнали в стандарта, са добра отправна точка при реализиране на цялостната архитектура. Използването на общите критерии (Common criteria) е добър начин за оценка на компоненти чрез комбиниране на функционалните изисквания, изискванията към нивото на доверие и изискванията към средата.

При реализацията на компонентите трябва да се разгледат и изискванията към доставчика на услуги от гледна точка на конкретни технически изисквания и стандартни. Основен компонент на съвременната бизнес архитектура се явява уебсървърът. Архитектурата за предоставяне на уебуслуги се състои от следните компоненти:

- Стандартен начин за представяне на данните.
- Единен формат на съобщение.
- Език за описание на уебуслуги.
- Стандартен подход за откриване на доставчици на услуги.

В **третия параграф на трета глава** се разглеждат дейностите по управление на информационна сигурност.

***Политиката за сигурност*** е най-логичното въплъщение на бизнес изискванията на предприятието за сигурност и контрол. Поради това може да се разглежда като нещо, което, след като е дефинирано, се превръща в основен двигател на програмата за оперативно управление на сигурността като цяло. Политиките за сигурност са мотивационен механизъм (цел) при изграждането на логическата архитектура. От друга страна, процесът по създаването и поддържането на политиките е елемент на оперативната архитектура. Изграждането на политика в едно ВУ трябва да следва културните особености и начина на функциониране на организацията, които са разгледани във втора глава на настоящия дисертационен труд. Политиките за сигурност трябва да бъдат строго насочени. Лоша практика е да се създават общи политики, които

да са насочени както към служителите (академичен и неакадемичен състав) на ВУ, така и към обучаемите. Специфична особеност е, че поради преплитане на функции някои субекти попадат в няколко групи и това налага, те да се запознаят с няколко сходни политики.

Общата политика за управление на операционния риск има за задачата да обедини всички общи теми на управлението на операционния риск с цел избягването на повторения в политиките от по-долно ниво. Политиката за управление на риска се декомпозира на основи политики, свързани със сигурността: обща политика за информационната сигурност, политика за физическата сигурност и политика за осигуряване на непрекъснатост на бизнес процесите.

Разработването на политики изисква класифицирането на отговорностите и ролите на отделните субекти при боравене с информационни ресурси. Един служител, в зависимост от ресурсите, които ползва, може да присъства в различни групи. Основните роли са:

- Собственик (owner) на информационния ресурс;
- Попечителят (пазителят) (custodian) на информацията;
- Потребителят (user) на информацията.

При класификация на потребителите във ВУ се наблюдават следните проблеми:

- Честа практика е, ИТ отделите (компютърните центрове) на ВУ да се превръщат в собственик на информация, която по принцип не им принадлежи. Това, от една страна, освобождава други звена от отговорности, но натоварва ИТ специалистите с функции по класифициране на информацията и разработката на контроли за нейното валидиране.
- Оставяне на „бели петна“ от информация без ясно дефиниран собственик.
- Стремеж на академичния персонал да получи по-голям достъп до информация, собственик, на която се явява служител или звено. Поради културните особености това често води до конфликти и неразбиране.
- Информацията, която е свързана с научноизследователската дейност, често не е изцяло собственост на ВУ. Управлението на тази информация трябва да се съобразява и с правила, поставени от нейните външни собственици (партньорските институции, организациите-източници на емпирични данни

или местата за апробиране на разработките).

- Не е решен проблемът с особеността на информацията, която се генерира в процеса на обучението, и дали ВУ придобива автоматично права върху разработките на обучаемите.

Класифицирането на информационните ресурси също така се явява основен компонент при разработване на политиките. Необходими са сегментация или класифициране на информацията в категории, подпомагащи оценката на относителната стойност на информацията, както и нужния контрол за запазване на нейната стойност. Трябва да се търси консистентност на оценките, която да позволи прилагането на еднакви контроли по осигуряването на защитата на еднотипна информация.

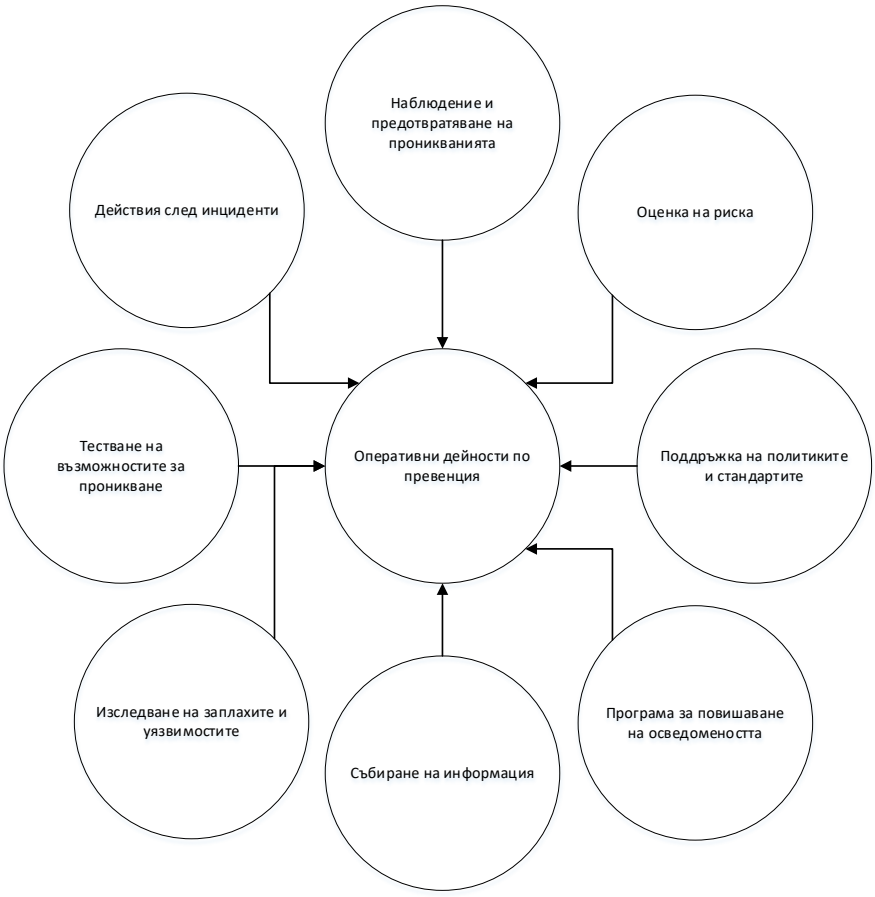
Не трябва да се пропуска и въпросът за изграждането на култура по информационна сигурност във ВУ. Създаването на добри писани политики не е достатъчно. Културните особености във висшето образование, базирани на академичната свобода и автономия, влизат в конфликт с налагането на административни правила и процедури. Въвеждането на правила и ограничения трябва да бъде добре обосновано и добре комуникирано с персонала. Информационната сигурност трябва да бъде обяснявана като фактор за развитие, а не като някаква пречка. Основен двигател на информираността и ангажираността в цялата организация е примерът, даден от управленския персонал. Мениджъри на всички нива трябва да дават добър пример, спазвайки политиката по всяко време.

Друг аспект на развитието на културата по информационна сигурност е **програмата за обучение**. Има няколко различни видове образование и обучение, които трябва да бъдат предприети:

- Кратко въвеждащо обучение за всички нови служители, за да се гарантира, че те са напълно наясно с политиката за сигурност и знаят как да я прилагат по отношение на ежедневните им дейности.
- Информиране на обучаемите поради тяхната важност в цялостната система за сигурност във ВУ. Информационният пакет за новопостъпилите обучаеми трябва да включва и политиките за допустимо използване на ИТК.
- Специализирано обучение за всеки, чиято работа включва техническа дейност, свързана с поддържане на информационната сигурност.

- Професионално развитие на кариерата за хора с мениджърски отговорности по информационна сигурност. Преминаване през магистърски програми или сертификационни курсове.
- Кратки курсове по различни аспекти на информационната сигурност.

Важен елемент на текущите дейности, свързани с информационната сигурност, е ***координацията на процеса на превенция***, който обединява и синхронизира множество оперативни дейности (виж. Фиг. 5).




Фигура 5. Оперативни дейности по превенция

***Рамката за управление на риска*** определя контекста, в който се управляват рисковете, от гледна точка на това, как те ще бъдат идентифицирани, анализирани, контролирани и наблюдавани. Тя трябва да бъде последователна и всеобхватна, с процеси, които са внедрени в ежедневното управление. Оценяването на риска на съществуваща система е подобно на оценяването на риска при изграждането на концептуалната архитектура. Разликата е, че в изграждането на архитектурата на предприятието то се представя като общ набор от системи, докато в оценката на системата за сигурност, базирана на риска, спецификата на системата вече е известна.

Целта на **Регистъра на риска и възможностите** е да се записва информация за всички събития (обстоятелства), които са били идентифицирани, заедно с техния анализ за наличие на рискове и възможности. Описват се мероприятията за управление на риска и възможностите. Предложената примерна структура на регистъра съдържа следните колони:

- Събитие – събитие (обстоятелство), на което се оценява рискът и/или възможностите;
- Описание на риска;
- Процес;
- Отговорник на процеса;
- Тип на риска;
- Ниво на въздействие - ниско, средно, високо;
- Ниво на уязвимост – ниско, средно, високо;
- Оценка на риска (A, B, C, D) – Незначителен риск(D), Приемлив риск (C), Значим риск (B), Висок риск (A)- (Вж. Фиг. 3.1);
- Дата на идентифициране;
- Планирани мероприятия за управление на риска;
- Срок;
- Дата на оценка;
- Остатъчно ниво на въздействие - Ниско, средно, високо;
- Остатъчна ниво на уязвимост Ниско, средно, високо;
- Остатъчна оценка на риска (A,B,C,D);
- Дата на окончателната оценка на риска;
- Описание на възможността;
- Дата на идентифициране на възможността;
- Процес;
- Отговорник;
- Планирани мероприятия за използване на възможността;
- Срок;
- Дата на оценка;
- Оценка на резултата от мероприятието;

- Контрол на достъпа до записа.

Достъпът до регистъра трябва да се контролира, за да се запазят неговата цялост и поверителност. За тази цел служи колонка „Контрол на достъпа“. Трябва да се разработи политика на сигурност на самия регистър, която да определя кой има права да актуализира съдържанието на регистъра и кой има права за четене на неговото съдържание или части от него.

Широко приет принцип на управление е, че една дейност не може да се управлява добре, ако не може да бъде измерена. Изграждането на архитектурата за информационна сигурност е цялостен процес, при реализацията на който освен ефикасност се търси и ефективност спрямо вложените ресурси. Поради тази причина е ***необходимо да се търсят показатели за измерване както на сигурността на системата, така и на постигнатия ефект от нейното изграждане***. Показателите трябва да бъдат в тясна взаимовръзка с бизнес целите на организацията, респективно с целите на ВУ.

Организацията трябва да документира разработените измерители в стандартен формат, за да се гарантира стандартен начин на разработването и настройката на измерителите, събирането на данни и дейностите за докладване. За нуждите на оценката на информационна сигурност във висшите училища се предлага да бъде изграден **Регистър на измерителите,** в който всеки да бъде описан чрез следните полета:

- идентификатор на измерителя;
- цел на измерителя;
- въпроси, на които отговаря измерителят;
- класификация според схемата на Савола;
- измерител, в който се посочва видът на числовата стойност (процент, брой, честота, средно и т.н.);
- бизнес атрибути от SABSA модела;
- алгоритъм на изчисляване;
- удовлетворителна стойност на измерителя;
- честота на измерване;
- отговорници по събирането на данни;

- източници на данни;
- начин и честота на отчитане на първичните данни;
- дали измерителят (данните за измерителя) съдържа лични данни;
- ниво на конфиденциалност на измерителя.

Предлаганата структура позволява да се интегрират добрите практики, препоръчвани в специалната публикация на NIST SP 800-55, по-добрата таксономия и бизнес атрибутите от SABSA, използвани по време на изграждане на архитектурата.

# IV. СПРАВКА ЗА ПРИНОСИТЕ В ДИСЕРТАЦИОННИЯ ТРУД

В дисертационния труд е проведено изследване на приложението на архитектурния подход при изграждането на система за информационна сигурност във висше училище в България. На тази база, се счита, че са постигнати следните научни и научно-приложни приноси:

1. Направен е критичен анализ на мястото на архитектурата на информационна сигурност в архитектурата на предприятието. Анализирани са елементите за изграждане на архитектурата за информационна сигурност и нейната връзка с елементите на бизнес системата.
2. Извършен е анализ на особеностите на информационните системи на съвременното иновативно висше училище.
3. Обоснована е необходимостта от система за сигурност на висшето училище и от прилагането на архитектурен подход при нейното изграждане.
4. Направен е анализ на приложение на добрите практики при използването на протоколи за сигурност във висшите училища в България.
5. Разработена е методика за изграждане на система за сигурност във висшето училище, базирана на използването на модела SABSA. В методиката се предлагат конкретни добри практики и структура на документи и регистри.
6. Части от методиката са апробирани при изграждането на системата за сигурност в Стопанска академия „Димитър Апостолов Ценов“ – Свищов.

# V. СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИОННИЯ ТРУД

## Научни статии:

1. Кузнецов, Ю. Приложение на добрите практики за защита на интернет инфраструктурата на висшите училища в България. // Списание „Диалог“, 2, 2018
2. Кузнецов, Ю. Особености на автоматизирана информационна система за управление на висшето училище.// Годишен Алманах научни изследвания на докторанти, Том X, 2017, Книга 13

## Научни доклади:

1. Компютърна сигурност в научноизследователските организации и учебните заведения, // Информационно осигуряване на бизнеса : Юбилейна международна научна конференция - Свищов, 7-8 юни 2006 г. АИ Ценов, 2006, с. 201-20
2. Необходимост от подобряване на външната нормативна рамка при реализиране на политики за сигурност на данните в областта на образованието, // Четвърта национална конференция с международно участие по електронно обучение във висшето образование : Сборник доклади и резюмета - Свищов, 11-13 май 2012 г. АИ Ценов, 2012, с. 399-405
3. Особености на автоматизираната система за управление на висше училище. // Предизвикателства пред информационните технологии в контекста на "Хоризонт 2020" : Юбилейна научна конференция. Сборник с доклади - Свищов, 07-08 окт. 2016 г.АИ Ценов, 2016, с. 265-270