УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО

Факултет „Икономика на инфраструктурата“

Катедра „Национална и регионална сигурност“

инж. Елица Георгиева Павлова

„РЕФЕРЕНТЕН МОДЕЛ ЗА КИБЕРСИГУРНОСТ ПРИ ПРОЕКТИРАНЕТО НА ОНЛАЙН УСЛУГИ ВЪВ ВИСШИ УЧЕБНИ ЗАВЕДЕНИЯ В БЪЛГАРИЯ“

АВТОРЕФЕРАТ

на дисертационен труд за образователна и научна степен „доктор”

по професионално направление 3.8. Икономика научна специалност „Икономика и управление“ (Икономика на отбраната и сигурността)

Научен ръководител: доц. д-р Георги Пенчев

Рецензенти: проф. д-р Димитър Велев

доц. д-р Росен Кирилов

София, 2023 г.

Дисертационният труд е обсъден и насочен за защита от катедра „Национална и регионална сигурност“ към факултет „Икономика на инфраструктурата“ при УНСС на заседание, проведено на 28.02.2023 г.

Трудът е в обем от 137 страници основен текст. Състои се от увод, изложение в четири глави, заключение, списък на използваната литература, 18 таблици, 32 фигури, 18 приложения (70 страници).

Използваната литература съдържа 60 заглавия на български и английски език в т.ч. нормативни документи и официални източници, книги, монографии, статии в научни и периодични издания, доклади и анализи на международни организации, както и електронни източници със специфична информация.

Публичната защита на дисертационния труд ще се състои на 02.03.2023 г.,

от 10:00 ч., в зала Научни съвети на УНСС.

Материалите по защитата са на разположение в сектор „Научни съвети и конкурси“ при Дирекция „Наука“ и на интернет страницата на УНСС www.unwe.bg.

СЪДЪРЖАНИЕ НА АВТОРЕФЕРАТА

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Дигиталната трансформация (ДТ) във висшите училища (ВУ) и изследователските организации е свързана с използването на информационни технологии, организационната структура и процесите, които осигуряват връзката между целите на университета и неговата политика в областта на информационните технологии (ИТ). Университетите възприемат множество нови технологии и методи на преподаване, използват различни приложения и портали за дистанционно обучение необходими за да поддържат онлайн или смесена учебна среда.

Нарастващата комбинация от нови предизвикателства и рискове в сектора налагат поставянето на киберсигурността като стратегически приоритет за защита на информационните активи, и ДТ като критична необходимост.

Актуалността на проблема е свързана с необходимостта от структурирано управление на сигурността при проектирането на нови електронни процедури и услуги във ВО.

В процеса на ДТ университетите увеличават предлаганите от тях онлайн услуги и заедно с тях се увеличават и рисковете от кибер атаки. Това ще изисква нови стандарти и инфраструктура за цифрово обучение, както и допълнително законодателство, което осигурява сигурни онлайн услуги от една страна, и насърчава иновациите от друга страна. По време на ДТ онлайн услугите и процесите свързани с тяхното проектиране се променят едновременно, което прави това наложително преразглеждането на стратегиите и политиките за информационна сигурност. Преминаването към виртуална и облачна архитектура поставя редица въпроси свързани с киберсигурността на съхраняваните данни.

Именно затова разработването и внедряването на модел за киберсигурност при проектирането на онлайн услуги във висшето образование (ВО) ще спомогне да се осигури ефективно и непрекъснато управление на всички важни административни и учебни процеси.

Изследователският проблем на дисертационният труд е идентифицираната липсата на модел за киберсигурност във ВУ обхващащ етапите на проектиране на онлайн услуги, което би повишило качеството на образованието и би спомогнало за идентифициране на основните направления за повишаване на информационната и киберсигурност. Проблемът е свързан с управлението на онлайн услуги и киберсигурността, както и сложната структура на университетите, високите изисквания към тях и бързо променящата се ИТ среда.

Обект на изследването са процесите на проектиране и управление на онлайн услуги във висшето образование в България.

Предмет на изследването са възможностите за повишаване на киберсигурността чрез стандартизирани процеси за разработване, промяна, внедряване

и наблюдение на дигитален модел за управление на ИТ във висшите училища в България.

Понятието „висши учебни заведения“ използвано в Закона за висшето образование преди промените от февруари 2020 година и промяната му с понятието „висши училища“ не се отразяват върху анализа в настоящото изследване[1]. Промяната не засяга управлението на ИТ във висшите училища. Поради забавяне в промяната на заглавието и съответно риска защитата на труда да бъде забавена след срока на докторантурата, както и поради това, че законовата промяна на понятията не се отразява на изследването бе решено да не се променя темата на труда. В изследването е използвана новата законова дефиниция „висши училища“.

Теза на изследването е, че към момента няма специализиран модел за киберсигурност във ВО, затова е необходимо да бъдат изследвани възможностите и да бъде създаден такъв. Основни характеристики на модела трябва да включват подобряване на комуникацията и обмена на информация между различните структурни звена, създаване на условия за бързо въвеждане на нови електронни процедури и услуги, както и стандартизирани критерии за анализ и повишаване на киберсигурността. Внедряването на такъв модел ще увеличи информационната сигурност във всички етапи на управление на онлайн услуги.

Целта на дисертационния труд е след анализ на основните характеристики на процесите на ДТ да бъде създаден референтен модел за киберсигурност и управление на онлайн услуги на ВУ в Република България.

Моделът трябва да обхване изискванията на нормативните и законови разпоредби да осигури стандартизирани приложения на принципите на киберсигурност във всички етапи и процеси.

Изпълнението на тези изисквания ще позволи модела да се използва като инструмент за самооценка, прилагане на конкретна политика за сигурност и изготвяне на доклади за съответствие.

За изпълнението на поставената цел са определени следните задачи:

1. Да бъдат анализирани дейността и процесите на ВУ в областта на ИТ технологиите и онлайн услугите да бъдат изведени основните характеристики свързани с управлението на киберсигурността.
2. На базата на преглед на литературата, посветена на управлението на киберсигурността, да бъдат идентифицирани успешните решения и добри практики за проектиране на сигурни онлайн услуги.
3. Да бъде създаден референтен модел за киберсигурност и стандартизиране на процесите на управление на онлайн услугите във ВУ в България.

[1] {Citation}

4. Моделът да бъде верифициран и валидиран чрез анализ на документи и интервюта с експерти. Референтният модел да бъде внедрен чрез създаване на онлайн приложение.

За установяване на състоянието на управление на киберсигурността е направен преглед на сайтовете на водещите ВУ в България и света.

Използвани са данни и изследвания свързани с киберсигурността във висшето образование във Европейския Съюз (ЕС). Разгледана е съответната литература, свързана с общата киберсигурност, най-добрите практики и рамки за киберсигурност. Изследването включва интервюта, анализ на документация и експертно мнение за верификация и валидация на референтния модел.

Използваните методи в дисертационният труд включват документен и сравнителен анализ, както и приложението на международни подходи и стандарти за управление на ИТ, информационна сигурност и киберсигурност: Рамката за целите за контрол на информацията и свързаните технологии (COBIT 2019), Библиотеката на ИТ инфраструктурата (ITIL) е подход, описващ най-добри практики за управление на ИТ услуги, Стандарт за управление на информационната сигурност (ISO/IEC 27001:2022), Рамка за киберсигурност на Национален институт за стандарти и технологии (NIST CSF) и Контролите за ефективна киберзащита (CIS CSC).

Изследването е ограничено до етапа на проектиране на нови онлайн услуги, без да се навлиза в детайли на етапите на тяхното внедряване и усъвършенстване.

Потребители на резултатите от дисертационния труд, могат да бъдат Министерство на електронното управление и Министерство на образованието и науката на Република България, всички висши учебни заведения, както и изследователи, студенти и обществеността като цяло.

Използвани са некласифицирани източници на данни и информация - монографии, учебници, научни публикации, статии и данни от Интернет.

Дисертационният труд обхваща четири глави:

В *Глава първа* са анализирани състоянието и проблемите при управлението на киберсигурността на ВУ в България. Изяснени са понятията, които са нужни за изследването. Идентифицирани са основните етапи на ДТ и е направен преглед на нормативната рамка на ЕС и България. Анализиран е чуждият опит в областта на киберсигурността във ВУ.

В *Глава втора* са анализирани подходите и стандартите за управление на информационни технологии и киберсигурност във ВО. Представени са най-често използваните референтни модели за управление на ИТ услуги и киберсигурност. Идентифицирани са техните основни характеристики и възможности за използването им при проектирането на онлайн услуги. Определени са изискванията и ограниченията към референтния модел.

В *Глава трета* е структурирано приложението на методиката за разработване на референтния модел. Направена е оценка на риска според въздействие и вероятност от уязвимости на университетските системи и произлизащите от тях онлайн услуги. Реферирани са контролите за сигурност към функциите на модела. Разработени са процедурите за работа с референтния модел и са установени ролите и отговорностите, свързани с управлението на ИТ във ВУ.

В *Глава четвърта* е верифициран и валидиран на референтния модел. Апробацията на модела е направена посредством софтуерно приложение, базирано на система за управление на съдържанието. С цел да се валидира предложеният модел и да бъдат установени възможностите за усъвършенстването му е направено проучване базирано на експертно мнение на хора от ИТ сектора.

II. ОБЕМ И СТРУКТУРА

Дисертационният труд е в обем от 137 страници основен текст. Състои се от увод, изложение в четири глави, заключение, списък на използваната литература, 18 таблици, 32 фигури, 18 приложения.

Използваната литература съдържа 60 заглавия на български и английски език, в т.ч. нормативни документи и официални източници, книги, монографии, статии в научни и периодични издания, доклади и анализи на международни организации, както и електронни източници със специфична информация.

Дисертационният труд има следната структура:

Списък със съкращения

Увод

Глава I. Състояние и проблеми при управлението на киберсигурността на висшите училища в България

1.1. Основни понятия и етапи на дигитална трансформация. Нормативна рамка за киберсигурност

1.2. Изследване на чуждият опит в областта на киберсигурността на ВУ

1.3. Предизвикателства и проблеми в областта на киберсигурността пред университетите в България

Изводи към Глава I

Глава II. Подходи и стандарти за управление на информационни технологии и киберсигурност във висшето образование

2.1. Основни подходи. Рамка за управление на ИТ и киберсигурност

2.2. Сравнителен анализ на подходите и стандартите за управление на ИТ и киберсигурност

2.3. Референтни модели за управление на киберсигурността. Изисквания.

2.4. Идентифициране на основни характеристики на референтен модел за кибер сигурност на висшите училища. Методика за разработване на модела.

Изводи към Глава II

Глава III. Приложение на методиката за разработване на референтния модел

3.1. Събиране и анализ на данни

III. СИНТЕЗИРАНО ИЗЛОЖЕНИЕ

Глава I. Състояние и проблеми при управлението на киберсигурността на висшите училища в България

Университетите в България са на различни етапи от своята дигитална трансформация спрямо наличната инфраструктура и средства, с които разполагат. Дигитализацията включва промяна на графика и провеждането на учебните програми, промяна на организационната структура, създаване на интерактивно съдържание, трансформиране на университетската инфраструктура. Постигането на успешна ДТ е свързано с последователна и целенасочена политика за усъвършенстване на предоставяни услуги, изграждане на нови структурни звена, обвързване на стратегическите цели на университета с целите за развитие на ИТ, осведоменост и обучение на персонала.

В Глава I са изпълнени следните поставени задачи:

1. Да бъдат анализирани дейността и процесите на ВУ в областта на ИТ технологиите и онлайн услугите.
2. Да бъдат изведени основните характеристики на онлайн услугите, свързани с управлението на киберсигурността.

В раздел 1.1 се описват основни понятия и етапи на дигитална трансформация и нормативната рамка за киберсигурност. Подходът, който се използва за анализ на основните понятия и тяхното дефиниране за нуждите на изследването се основава на един от най-влиятелните източници за международно научно цитиране Web of Science[2]. Понятията, използвани като ключови думи на търсенето в базата данни са дигитална трансформация, информационна сигурност, киберсигурност, контроли за киберсигурност и референтен модел.

Тези понятия се откриват в заглавията на 463 научни изследвания за последните три години, като най-голям брой от тях са в категория „Образование“ (45%), следвани от „Управление“ (8%) и „Икономика“ (7%). Киберсигурността във ВУ е изследвана в 110 доклада.

Най-цитираните понятия необходими за изследването са разгледани по-долу.

Дигитална трансформация

Едно от получилите висока популярност понятие, свързано с управлението на ИТ е „дигиталната трансформация“. То има значение при промяната на дейността на организациите или при значима промяна на технологиите и тяхното пълно внедряване.

[2] Web of Science, “Web of Science,” Webofscience.com, 2022, https://www.webofscience.com/wos/woscc/basic-search.

В монографията „Цифрова трансформация във висшето образование“ авторите описват дигитализацията в пет области[3]: ИТ стратегическо планиране, добавяне на стойност на ИТ, управление на риска, измерване на резултатите и управление на ИТ ресурси.

Понятието дигитална трансформация във ВУ, за нуждите на изследването, е определено като поредица от дълбоки и координирани промени, които дават възможност за нови образователни модели и трансформират дейността на институцията, използвайки сигурен и бърз достъп до информационни ресурси, приложения и услуги по всяко време и от всяко устройство.

Информационна сигурност

Докладът „Съвременен инструментариум за оценяване на сигурността“ на доц. д-р Цветан Цветков показва, че оценяването на сигурността и процесът на управление са свързани и взаимозависими, и проблемите на сигурността влияят върху дългосрочния просперитет на организацията и засягат жизненоважни цели на организацията. [4].

За целите на изследването информационната сигурност е дефинирана като способност за защита на вътрешните ресурси на дадено ВУ от заплахи, и нейното управление включва защита на информационните активи чрез прилагане на политики, процедури, организационни структури, инфраструктура и одити. Рамката за управление определя кой е упълномощен да взема решения и как ще бъде установена отчетност за резултатите. Процесите на управление гарантират, че всички критични активи са защитени и рисковете са адекватно смекчени.

Киберсигурност

Киберсигурността е компонент на информацията сигурност и с нея са свързани: мерки за защита на ИТ; степента на защита, произтичаща от прилагането на тези мерки; данни и информация, които се обработват и предават; свързани виртуални и физически елементи на системите.

Докладът „Модел на обучение в областта на киберсигурността“ на гл. ас. д-р Недко Тагарев показва, че основната цел на обучението в областта на киберсигурността е свързана с установяването и подобряването на програмите за защита на компютърните системи, мрежи и други цифрови системи, които са от решаващо значение за предотвратяване на кражби, саботажи и други злоумишлени действия[5].

За целите на изследването киберсигурността е дефинирана като съвкупност от практики и насоки, които се използват за защита на компютърни мрежи, софтуерни програми и информационни активи от неоторизиран достъп, устойчивост

[3] Mark McCormack Christopher Brooks, “Defining Digital Transformation,” Educause.edu, 2020, https://www.educause.edu/ecar/research-publications/driving-digital-transformation-in-higher-education/2020/defining-digital-transformation.

[4] Цветан Цветков, “Съвременен инструментариум за оценяване на сигурността,” Journal Issues - Economic Alternatives, Unwe.bg, 2016, https://www.unwe.bg/alternativi/bg/journalissues/article/8948.

[5] Недко Тагарев, “Модел На Обучение в Областта На Киберсигурността” (www.unwe.bg, 2019), https://www.unwe.bg/uploads/Alternatives/Tagarev4_Alternativi_BG_br_2_2019.pdf.

и възстановяване след кибератака. Приоритетите за киберсигурност са възпиране, превенция, откриване и реакция.

Контроли за киберсигурност

Киберсигурността обхваща контроли, които трябва да се създадат и въведат за защита на информацията, съхранявана в информационните системи.

За целите на изследването контролите за киберсигурност са дефинирани като предпазни мерки или контрамерки за избягване, откриване, противодействие или минимизиране рискове за киберсигурността - вируси, зловреден софтуер, кибер атаки, хакери, опити за фишинг и други.

Референтен модел

Според организация за усъвършенстване на стандартите за структурирана информация референтен модел е „абстрактна рамка за разбиране на значими взаимоотношения между обектите на дадена среда, и за разработване на последователни стандарти или спецификации, поддържащи тази среда[6]. В други източници референтния модел се описва като „концептуална рамка, установяваща общ език за комуникация и разбиране за елементите на системата и техните значими взаимоотношения в рамките на дадена общност".

За целите на изследването понятието референтен модел е дефинирано като концептуална рамка, установяваща общ език между стандартизирани подходи и добри практики за киберсигурност, който може да се използва в ежедневната работа на организациите от сектора на ВО.

Етапи на дигитална трансформация

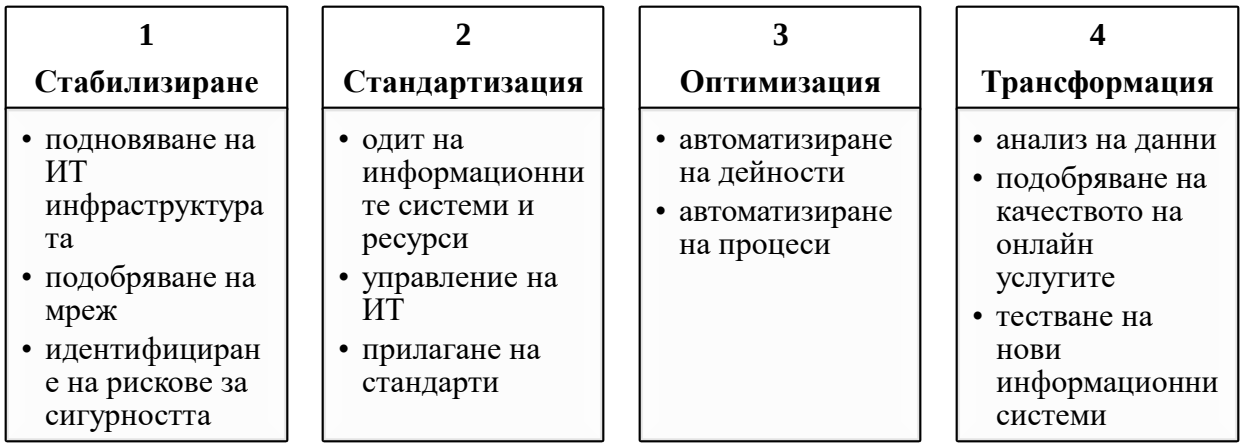
Създаването на референтен модел за киберсигурност за проектирането на онлайн услуги във ВУ изисква изясняване на етапите на ДТ. В книгата „Корпоративна сигурност" на катедра „Национална и регионална сигурност" е описано, че ДТ включва необходимостта от автоматизиране на контрола за сигурност на данните и разработване на стабилна ИТ инфраструктура [7].

Докладът „Какво означава дигиталната трансформация за висшето образование" посочва четири основни етапа, през които трябва да преминат университетите[8]. Те са представени на *Фигура 1*.

[6] "OASIS," Oasis open, 2022, https://www.oasis-open.org/.

[7] Атанас Димитров, Георги Павлов, Димитър Димитров, Екатерина Богомилова, Константин Пудин, Никола Иванов, Нончо Димитров, Теодора Гечкова, Тилчо Иванов, Цветан Цветков, Юри Ценков et al., "Корпоративна сигурност."

[8] Dania McDermott, "What Digital Transformation Means for Higher Education," Processmaker.com, 2020, https://www.processmaker.com/blog/what-digital-transformation-means-for-higher-education/.



Фигура 1. Етапи на дигиталната трансформация във висшето образование

Източник: Larissa Lewis, „Creating a Digital Transformation Roadmap“, Processmaker.com, 2020, https://www.processmaker.com/blog/digital-transformation [9]

Етапът на *стабилизиране* включва подновяване на ИТ инфраструктурата, подобряване на мрежа, идентифициране на рискове за сигурността. По време на *стандартизацията* се извършва одит на информационните системи и ресурси, управление на ИТ и прилагане на стандарти за киберсигурност. *Оптимизацията* включва автоматизиране на всички дейности и процеси. *Трансформацията* е свързана с анализ на данни, подобряване на качеството на онлайн услугите, както тестване на нови информационни системи.

Нормативна рамка за киберсигурност в ЕС и България

За целите на изследването е анализирана нормативната рамка на ЕС и е сравнена с действащата в Република България.

Европейската комисия представи програма за цифрово бъдеще на Европа, която включва Стратегия за цифровото бъдеще на Европейския съюз, Бяла книга за развитието на изкуствения интелект и Стратегия за създаването на единен цифров пазар и други.

Стратегия на ЕС за киберсигурност има за цел да засили устойчивостта на Европа срещу кибер заплахи и да гарантира, че всички граждани и институции могат да се възползват от надеждни услуги.

През декември 2020 г. Европейската комисия прие директива за киберсигурност на мрежите и информационните системи, в отговор на динамично променящата се цифровата трансформация. В нея е записано, че съдържанието на образователните системи трябва да е в съответствие с нормативните документи на държавите-членки, както се има предвид споделянето на добри практики в областта на дигиталното образование. За да се прецени до каква степен регулаторната рамка за висшето образование в България е подходяща за прехода към дигиталната ера, са

[9] Larissa Lewis, “Creating a Digital Transformation Roadmap,” Processmaker.com, 2020, https://www.processmaker.com/blog/digital-transformation/.

идентифицирани основни нормативни документи свързани с ДТ и киберсигурност във ВУ.

Съветът и Европейският парламент постигнаха съгласие относно мерки за високо общо ниво на киберсигурност в целия Съюз, за да подобрят допълнително устойчивостта и капацитета за реагиране при инциденти както на публичния, така и на частния сектор и на ЕС като цяло.

Целта на новата директива, наречена „NIS2“, е да премахне различията в изискванията за киберсигурност и в прилагането на мерките за киберсигурност в различните държави членки[10].

Нормативни документи на ЕС:

- Стратегия на ЕС за киберсигурност 2020-2025;
- План за действие за цифрово образование на ЕС 2021-2027;
- Разпоредба за култура на киберсигурност в организациите на Агенцията по киберсигурност на ЕС (ENISA)[11].

Подобряването на университетската култура чрез методологията “Политики за киберсигурност” на Агенцията на Европейския съюз за киберсигурност, е ключово за всички етапи на ДТ. Политиките обхващат създаването на програми, фокусирани върху конкретни дейности, тяхното изпълнение и измерване на въздействието им. Големият брой студенти, преподаватели и служители, различните нива на ИТ компетентност и сложна мрежова свързаност на всички устройства правят създаването и управлението на киберсигурността изключително сложно.

България участва във всички инициативи на ЕС, включително програмите "Хоризонт Европа" и "Цифрова Европа" и по-долу са разгледани нормативни документи на България, свързани с дигитализацията във ВУ и киберсигурността.

Нормативни документи на България:

- Стратегия за развитие на висшето образование в България (2021-2030)[12];
- Стратегия за ефективно прилагане на информационните и комуникационните технологии в образованието и науката на България (2014-2020);
- Националната програма за развитие „България 2030“;
- Националната програма „Цифрова България 2025“;
- Национална стратегия „Кибер устойчива България 2020”.

Нормативните документи подкрепят проблемите и предизвикателствата от областта киберсигурността на ВУ. Техните основни цели са повишаване на осведомеността и компетентностите, развитие на стимулираща среда за изследвания, достъп до данни, информация и знания. Прилагането на ДТ в образованието ще осигури

[10] NIS, “NIS 2 Directive,” Nis-2-directive.com, 2022, https://www.nis-2-directive.com/.

[11] ENISA Europa, “Cyber Security Culture in Organisations,” 2020, https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport.

[12] Strategy.bg, “Стратегията За Развитие На Висшето Образование в Република България (2019 – 2030),” 2020, http://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=962.

достъпност, актуалност и управление на образователните ресурси, които са в основата на качествено образование.

Основното предизвикателство пред университетите е постигането на по-високи общи нива на сигурност при използването и поддръжката на информационните системи за контрол на достъпа и информация. Политиките за висше образование не засягат пряко иновациите, но те имат връзка с двигателите на иновации, се посочва в изследване направено в университети от ЕС[13]. Основни фактори за развитие на иновациите могат да бъдат общата регулаторна рамка, съществуването на натрупани знания, научноизследователската и развойна дейност, фактори, специфични за определен пазар или продукт, като нивото на търсене и структура на разходите, вида на правителството, социалната инфраструктура, съществуването на права на собственост, правителственото потребление, международната отвореност, инфлацията и др.

В раздел 1.2 е направено изследване на чуждият опит в областта на киберсигурността на ВУ. Методът за събиране на данни включва подробно търсене в интернет страниците на университети от цял свят.

Сравнени са практиките на 17 университета, седем от България (Софийския Университет, УНСС, Икономически университет – Варна, Висше транспортно училище "Тодор Каблешков", Американски университет в България – Благоевград, Нов български университет, Варненски свободен университет "Черноризец Храбър") и десет водещите европейски, британски и американски университети (Виена, Любляна, Станфорд, Оксфорд, Харвард, Граз, Мазарик, Берлин, Тесалоники).

Университетите предоставят множество онлайн услуги като кандидатстване и семестриални изпити, уеб студент, електронни библиотеки, портал за преподаватели и др. Приоритетни направления са администриране и поддръжка на бази данни, съществуващи приложения и системи за онлайн обучение, актуализиране на университетския уебсайт, мрежовата свързаност, дейности, свързани с поддръжка на крайните потребители и др.

Търсени са показатели, имащи връзка с киберсигурността и даващи информация за броят на домейни, поддомейни, информационни системи, предлагани онлайн услуги и политики за информационна сигурност.

Сайтовете са сканирани чрез онлайн платформата Урлскан (www.urlscan.io). Методът за сканиране се базира на автоматизиран процес за преглеждане на Интернет адреса и записване на дейността, която навигация на страницата създава.

Анализът включва сравняването на следните показатели: популярност (ранг); глобален ранг; заявките показват общия брой трансфери идващи от други домейни; HTTPS протокол; под домейни, които работят като самостоятелни уеб сайтове; IP адресите (IPv6, IPsec); изходящият брой връзки; размер на сайта; X-XSS-Protection;

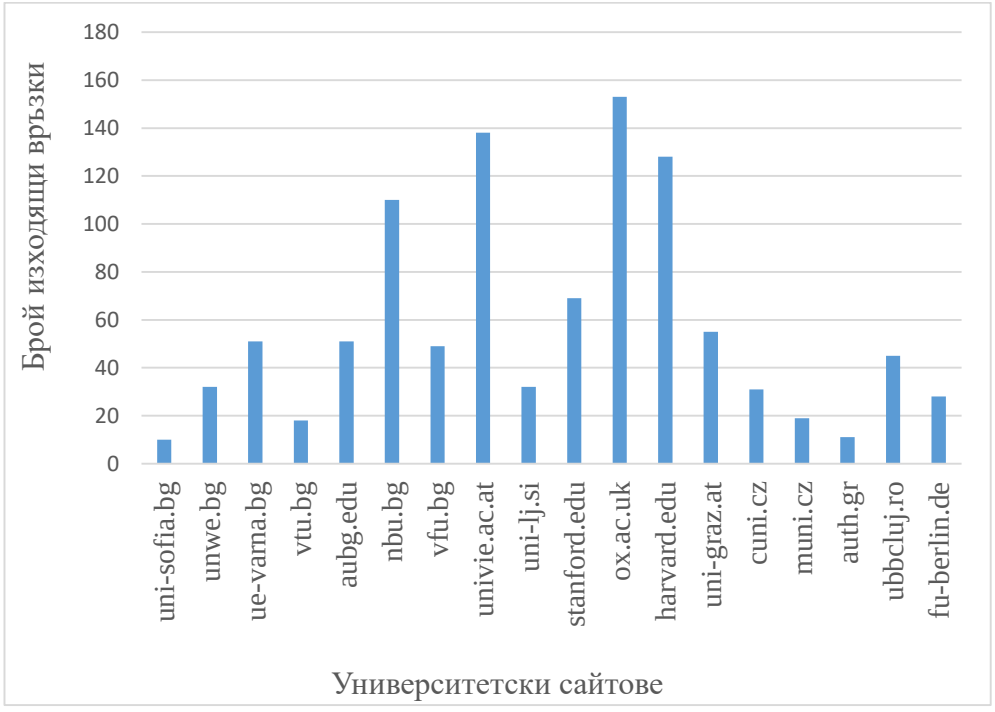
[13] Roger G. Baldwin, “Technology in Higher Education,” Education.stateuniversity.com, 2021, https://education.stateuniversity.com/pages/2496/Technology-in-Education-HIGHER-EDUCATION.html.

Strict-Transport-Security; X-Frame-Options; X-Content-Type-Options; X-Xss-Protection; Content-Security-Policy, както и допълнителна информация за самата страница.

От направеният анализ се вижда, че разгледаните университети в България имат приблизително еднакъв Гугъл ранг 4 или 5, докато при университетите в света той варира от 6 до 8. Използването на протокол HTTPS в международните университети е малко по-висок спрямо този в България и гарантира, че транзакциите се пазят поверително и всеки пакет данни е криптиран и защитен. Броят домейни, поддомейни и изходящият брой връзки дават информация за свързаните чрез интернет страници и предоставяните онлайн услуги. Университета във Виена, Оксфорд и Харвард имат над 120 изходящите връзки. Прави впечатление, че при повечето университети използването на IPv6 е около 80%.

В университетските сайтове изходящите връзки често пъти водят към поддомейни на главният сайт и представляват предлагани онлайн услуги. Големият брой под домейни показва, че университетските сайтове са изградени като портални и водят към различни под сайтове в Интернет или Интранет.

На Фигура 2 е представена графика на изходящите връзки в анализираните университетски сайтове. Броят им варира в много широк диапазон от 43 до 178. Софийският университет има най-малък брой изходящи връзки 10, докато Нов български университет има повече от 100. Сайтовете на Икономическият университет във Варна и Американският университет имат еднакъв брой 50. Сайтът на университетът в Станфорд, който винаги има най-високи показатели, има едва 69 изходящи връзки, спрямо университетите във Виена, Оксфорд и Харвард, които имат повече от 120 изходящи връзки.



Фигура 2. Изходящи връзки в университетски сайтове в България и света

Източник: Собствено проучване

Направеният анализ дава представа за организационни структури, съдържание, свързаност към социални мрежи и платформи, брой посещения, информационни системи, мобилни приложения, структурата на ИТ отдела, стратегия и политики за киберсигурност, актуализация на информацията и други параметри, пряко зависещи от ИТ управлението във университета. Анализът показва, че има много области, които трябва да бъдат изследвани и подобрени в българските университети. Готовността за промяна и внедряване на иновации е пряко свързана с броя и видовете на предоставяните ИТ услуги.

На базата на направените проучвания са идентифицирани четири основни групи информационни системи: Административни, Информационни, Учебна дейност и Наука.

В изследването "Заплахи за киберсигурността 2022" са представени най-често срещаните уязвимости при онлайн услугите[14]. От него се вижда, че основна заплаха за сигурността представлява мащабното извличане на данни. Лекотата с която могат да се събират и обобщават данни, прави тази атака широко разпространена.

Докладът „Дигитална трансформация във висшето образование" описва проблемите, пред които са изправени ВУ[15]. Повечето университети декларират като трудности липсата на средства за инвестициите в нови технологии, бавно променящата се организационна култура, несигурната интернет инфраструктура, недостатъчната готовност за обучение по киберсигурност и квалифициран ИТ персонал. ВУ използват технологично остарели информационни системи, които не са защитени правилно и трябва да ги адаптират към променящите се нужди на студентите и нормативните разпоредби.

Изследването на чуждият опит показва, че модерния университет е ориентиран към интернационализация, конкурентоспособност и иновации. Приоритетни теми са дигиталната трансформация, киберсигурността, както и законово нормативната база свързана с тях. Решение на базата на направения анализ включва прилагането на стандартизиран подход при проектирането на онлайн услуги във ВУ, защото справянето със съществуващите уязвимости и тяхното отстраняване в реално време може да бъде трудно.

В раздел 1.3 са анализирани предизвикателствата и проблемите в областта на киберсигурността пред университетите в България.

Университетите често възприемат реактивен подход към киберсигурността като предприемат мерки едва при настъпила атака. Проучване за киберсигурността показва, че през 2021 висшите образователни институции модернизират инструментите за сигурност на съществуващите ИТ системи като маркират елементи от контролни списъци за съответствие вместо да вграждат киберсигурността в своите нови системи

[14] Ptsecurity, "Cybersecurity Threatscape: Q2 2022," 2022, https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2022-q2/.

[15] Lina María Castro Benavides et al., "Digital Transformation in Higher Education Institutions: A Systematic Literature Review," *Sensors* 20, no. 11 (January 2020): 3291, https://doi.org/10.3390/s20113291.

и услуги[16]. Надеждността на мрежовите и информационните системи е ключова за безпроблемно функциониране на всички платформи и университетски сайтове, провеждане на кандидатстудентски кампании, електронни изпити, записвания, обучение и др.

Справка в базата данни за световното висше образование показва, че 63% от университетите управляват изцяло онлайн процеса на записване и съхранение на данните за студентите[17].

Международната асоциация на университетите подчертава, че няма единен модел за цифрова трансформация, който да пасва на всички висши учебни заведения. Справката предоставя общ преглед на националните стратегии и политики за използване на нови технологии в преподаването и ученето. Архитектурата на приложенията включва прилагане на ориентиран към потребителя дизайн, реинженеринг на информационните системи, единен вход, дигитално работно място и осигуряване на възможност за вътрешна оценка на процесите и подобряване на услугите.

Новите тенденции свързани с киберсигурността включват разработване на базирана на риска стратегия за сигурност, облачна инфраструктура и високоскоростни мрежи, дефинирани процеси за киберсигурност, системи за откриване и реагиране на кибератаки и др.

Действащата в момента нормативна уредба в областта на ИКТ в България обхваща: Закон за електронните съобщения; Закон за киберсигурност; Закон за електронните съобщителни мрежи и физическата инфраструктура; Закон за електронно управление; Закон за електронния подпис и електронните удостоверителни услуги; Закон за киберсигурност; Закон за търговския регистър; Закон за електронната търговия; Закон за защита на личните данни, както и други разпоредби.

Националната програма „Цифрова България“ има за цел хармонизиране на българското законодателство в съответствие с това на ЕС в рамките на Стратегията за цифров единен пазар в Европа. Целта на Европейската комисия е да подпомага държавите членки при идентифицирането на области, изискващи приоритетни действия, като една от тях е до 2030 г. най-малко 80% от гражданите да имат основни цифрови умения.

Данните в Рейтинговата система на висшите училища в България (РСВУ) за 2021 година показва увеличаване на броя на студентите и броя на научните публикации в международните библиографски бази данни.

[16] Dave Burg, Mike Mason, and Richard Watson, “Cybersecurity: How Do You Rise above the Waves of a Perfect Storm?,” EY, 2021, https://www.ey.com/en_bg/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm.

[17] WHED, „World Higher Education Database“.

Основните предизвикателства, описани в изследването „Университетите в дигиталния свят“[18] са:

- Висока степен на възрастова диференциация по отношение на възможностите за работа с дигитални технологии.
- Реформиране на ВО, целящо комбинирането на писмено-слуховата информация с визуална информация.
- Липса на стратегическите визии по отношение на основните функции на университетите, свързани с обучението, с развитието на науката и иновациите.
- Постигане на баланс между увеличаващите се обществени изисквания и очаквания към висшето образование.
- Недостатъчна конкурентоспособност по отношение на бързото развитие на пазара на образователни услуги и липса на гъвкавост в предлаганите форми на обучение.

Предизвикателствата пред ВО в България са свързани с липата на цялостен модел за дигитализация по който да бъде оценена степента на дигитализация на всяко висше училище, както и единна автентикация на потребителите за достъп до всички платформи.

Киберсигурността във ВУ се осигурява чрез процеси, които ръководството следва за да идентифицира, анализира и реагира по подходящ начин на рискове, които могат да влияят неблагоприятно на организацията. По време на конференцията „Дигитализация на висшето образование в България“, която се проведе тази година в УНСС, бяха обсъдени възможните заплахи, оценка на риска и начините за противодействие им. В нея се каза, че, университетите са уязвими към кибератаки поради своята децентрализирана структура, разнообразна група потребители (изследователи, студенти, докторанти, преподаватели, служители и други), различни нива на ИТ компетентност и сложна мрежова свързаност на всички устройства. В центъра на вниманието са хората и възможностите за тяхното обучение, с което да бъде снижена уязвимостта от кибератаки, загубата на данни или репутация.

България участва в няколко големи международни проекти, единият от които е мрежата "Европейски университети". В него дигитализацията е основен приоритет, именно затова редица технологични компании партнират на българските университети за осигуряване на тяхната информационна сигурност и киберсигурност.

Доклад за сигурността на софтуера от 2021 г. отбелязва, че повече от 85% от уеб приложенията имат уязвимости в сигурността[19]. Разбирането на тези уязвимости е от ключово значение за откриването им и защитата на данните. Стандартизацията и сертифицирането на дейностите, свързани с киберсигурността, не са достатъчно съобразени със съвременните нуждите на ВО. Ключовите послания, които ENISA отправя към организациите в тази връзка включват повече в информираност и образование относно сигурността на всички нива, управление на риска, сътрудничество

[18] Link Springer, “A University Landscape for the Digital World,” Link Springer, 2022, https://link.springer.com/chapter/10.1007%2F978-3-030-44897-4_1.

[19] Veracode, “State of Software Security,” Veracode, 2021, https://www.veracode.com/state-of-software-security-report.

с академичните среди, за да гарантира, че научните изследвания водят до качествени продукти и услуги.

Една от възможните стратегии за противодействие на рисковете за киберсигурността е обучението на служителите. „Обучението следва да е непрекъснато и съдържанието да се актуализира редовно, като обхваща възникващите заплахи за сигурността и контролите за сигурност, които са приложени за защита на информацията.“, се посочва в статията „Какво представлява обучението по сигурност и защо е важно“[20].

Университетите трябва да разработят програмите за информираност в съответствие с различните роли на служителите в организацията. Програмата трябва да включва различни форми на обучение – информационни бюлетини, компютърно базирано обучение за сигурност, симулирани фишинг упражнения, сигнали и съвети за киберсигурност.

Изводи

В *Глава първа* са анализирани състоянието и проблемите при управлението на киберсигурността на ВУ в България. Решение на базата на направения анализ включва проектирането на защитата, като важна част за разработването на онлайн услуги, защото справянето със съществуващите уязвимости и тяхното отстраняване в реално време може да бъде трудно. Киберсигурността трябва да бъде заложена в началните етапи на планиране, а не като процес за смекчаване или възстановяване след кибератака.

Изяснени са понятията, които са нужни за изследването: дигитална трансформация, киберсигурност, контроли за сигурност и референтен модел.

Идентифицирани са основните етапи на дигиталната трансформация – стабилизиране, стандартизация, оптимизация и трансформация, като и сътрудничество на европейско ниво за развитието на високоефективна екосистема за цифрово образование.

Анализът на най-често срещаните рискове за сигурността на онлайн услугите включва мащабно извличане на данни, фалшифициране на заявки между сайтове, атака за отказ на услуга или подправяне на идентификационни данни.

Направен е преглед на нормативната рамка на ЕС и България. Разгледаните нормативни документи подкрепят проблемите и предизвикателствата от областта на киберсигурността и очертава ключовите приоритети свързани с повишаване на качеството на образованието, въвеждане на съвременни методи на обучение, сигурна среда за изследвания, достъп до данни и информация.

Данните от анализираните университетски сайтове в България и в света дават информация за броят информационни системи, мобилни приложения, организационни структури, стратегия и политики за киберсигурност, както и други параметри, пряко

[20] Mimecast, “What Is Security Awareness Training and Why Is It Important?,” Mimecast, 2022, https://www.mimecast.com/content/what-is-security-awareness-training/.

зависещи от ИТ управлението във университета. От него става ясно, че има много области, които трябва да бъдат изследвани и подобрени. Броят на предлаганите онлайн услуги нараства, а заедно с тях и необходимостта от обща концепция за киберсигурност във ВО.

Анализиран е чуждият опит в областта на киберсигурността и е установено, че ВУ в България имат нужда от цялостен модел за киберсигурност при проектирането на онлайн услуги, какъвто вече има работещ в много други университети от ЕС. Прилагането на ДТ във ВУ ще осигури достъпност, актуалност и управление на образователните ресурси, подобряване на инфраструктурата, администрацията и контролът на достъп.

Глава II. Подходи и стандарти за управление на информационни технологии и киберсигурност във висшето образование

В Глава II са изпълнени следните поставени задачи:

1. На базата на преглед на литературата, посветена на управлението на киберсигурността, да бъдат идентифицирани успешните решения и добри практики за проектиране на сигурни онлайн услуги.

В раздел 2.1 на настоящата глава за целите на изследването са разгледани основни подходи и рамки за управление на ИТ и киберсигурност.

Пълният списък с описание и предназначение на всеки стандарт и подход е представен в *Приложение 8*. Повечето от тях успешно се използват във ВУ по света и затова са разгледани по-подробно.

COBIT 2019 подход за управление на информационни технологии. Обща рамка

Общата рамка за управление на информационните технологии в организацията е приета като стандарт (COBIT 2019[21]) и е разработена от Асоциацията за одит и контрол на информационните системи. Рамката е глобално признатата и се използва от над 188 държави и има над 200 000 признати сертификата. Основни принципи в COBIT 2019 са нуждите на заинтересованите страни и създаване на бизнес стойност, чрез използването на ИТ. COBIT 2019 поддържа високо ниво на съответствие и включва части от други стандарти за информационна сигурност, чрез ясно разграничаване между нивата стратегическо управление и оперативно управление (мениджмънт).

Подхода предлага обща рамка, включваща няколко стандарта, обвързвайки целите на управлението като цяло и целите на управлението на ИТ.

Основни стъпки при използване на подхода са: определяне на обектната област; дефиниране на фактори на проектирането; каскадиране на цели; приоритизиране на целите на управление и мениджмънта; установяване на добавената стойност.

[21] ISACA, „COBIT | Control Objectives for Information Technologies“, isaca.org, 2022, https://www.isaca.org/resources/cobit.

Каскадирането на цели поддържат приоритизирането на целите на управлението въз основа на приоритизирането на целите на организацията. Те включват култура на обслужване, ориентирана към клиента, оптимизиране на функционалността на вътрешния бизнес процес, постигане на оперативни съвършенства на услугата, управление на бизнес риска.

Описание на подхода в графичен вид може да бъде видян на Фигура 3.

Фигура 3. Основни процеси на подхода COBIT 2019

Източник: IEA, 2022, публикация на Enterprise Architecture, iea.wikidot.com/cobit

Основните елементи в COBIT 2019 са области, цели и показатели за ефективност. *Областите* следват общия жизнен цикъл на развитието на системите. *Целите на управление* описват практическите цели за управление на ИТ процеси. *Показателите за ефективност* описват активността.

Матрицата RACI[22] позволява да се идентифицират ролите и отговорностите, пряко свързани с организационната структура при управлението на киберсигурността, и ще бъдат разгледани подробно в Глава 3, раздел 3.3.

Четирите области, които следват общия жизнен цикъл на развитието на системите са[23]: *Обвързване, планиране и организиране (ОПО)*; *Изграждане, придобиване и внедряване (ИПВ)*; *Доставка, обслужване и поддръжка (ДОП)*; *Мониторинг, оценяване и анализ (МОА)*. Подробно описание на процесите и свързаните рамкови елементи в областите Планиране и организация и Придобиване и внедряване, могат да бъдат разгледани в ***Error! Reference source not found.***.

За всяка цел на управлението COBIT 2019 установява компонентите, които трябва да бъдат мащабирани, поддържани и удовлетворени, за постигането на всяка цел и те са:

- процеси
- организационни структури;

[22] RACI - Responsible, Accountable, Consulted, Informed

[23] Coursehero, „COBIT has several strengths that make it a worthy framework for IT“, www.coursehero.com, 2021, https://www.coursehero.com/file/p4pvm3s/COBIT-COBIT-has-several-strengths-that-make-it-a-worthy-framework-for-IT/.

- информационни потоци и елементи;
- хора, умения и компетенции;
- политики и процедури;
- култура, етика и поведение;
- услуги, инфраструктура и приложения.

Целите на стратегическото и оперативното управление са разделени в области, в който се разработват добри практики, така че ръководният орган да може да оцени наличните стратегически опции, да насочи организацията към стратегически цели и да наблюдава изпълнението на стратегическия план.

COBIT 2019 дава възможност за постигане на организационните цели, чрез балансиране и насочване на риска и мерки за контрол. Внедряването му ще позволи да се намали рискът за сигурността, управлението на данните, подобряване на ИТ услугите и достъпа на всички заинтересовани страни.

Стандарт ISO/IEC 27001:2022 система за управление на информационната сигурност. Обща рамка.

Стандартът е задължителен в България, като внедряването му е обусловено от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност, издадена на основание чл. 43, ал. 2 от Закона за електронното управление. Сертифицирани по него трябва да бъдат държавната, териториалната и местната администрации, съдебната власт, лица осъществяващи публични функции, както и за организациите предоставящи обществени услуги, каквито са образователните институции.

Стандартът обхваща следните области на информационната сигурност: Оценка на риска за информационната сигурност; Сигурност на човешките ресурси; Физическа сигурност; Компютърна и мрежова сигурност; Сигурност при разработването на софтуер и хардуер; Управление на инциденти; Управление на непрекъсваемостта.

ISO/IEC 27001:2022 има 93 контроли структурирани в четири контролни групи: A.5 Организационни контроли - съдържа 37 контроли; A.6 Контроли за хора - съдържа 8 контроли; A.7 Физически контроли - съдържа 14 контроли; A.8 Технологични контроли - съдържа 34 контроли.

В Приложение А са добавени следните 11 нови контроли:

- Разузнаване на заплахите
- Информационна сигурност при използване на облачни услуги
- ИКТ готовност за непрекъснатост на бизнеса
- Мониторинг на физическата сигурност
- Управление на конфигурацията
- Изтриване на информация
- Маскиране на данни
- Предотвратяване на изтичане на данни

- Мониторингови дейности
- Уеб филтриране
- Сигурно кодиране

Разделът с изисквания, ориентирани към системата за управление в Приложение А на стандарта ISO/IEC 27001:2022 съдържа списък от 35 контроли с 114 конкретни мерки за сигурност.

Контролите описват как трябва да изглежда един съответстващ на стандарта резултат от мерки и са представени в *Приложение 11*.

Основното предимство на внедряването на стандарта ISO/IEC 27001:2022 е, че е приложим за всякакви видове организации и гарантира, че информационната сигурност се управлява ефективно и ефикасно. Определя и оценява процесите по управление на сигурността на информацията, като същевременно осигурява непрекъсваемост на процесите във всички бизнес направления. Внедряването му отнема време и трябва да бъдат изпълнени всички негови препоръки и политики. Стандартът използва подход, основан на риска и това изисква от организациите да идентифицират рисковете за информационната сигурност и да изберат подходящи контроли за справяне с тях.

Библиотека на ИТ инфраструктурата ITIL. Обща рамка.

Библиотеката на ИТ инфраструктурата (ITIL) е подход, описващ най-добрите практики за управление на ИТ услуги. Основният фокус на ITIL е определянето на функционални, оперативни и организационни атрибути. Те са разделени в две ключови категории – *управление на поддръжката на услуги* и *управление на доставката на услуги*, като всяка от тях има редица поддържащи подкатегории.

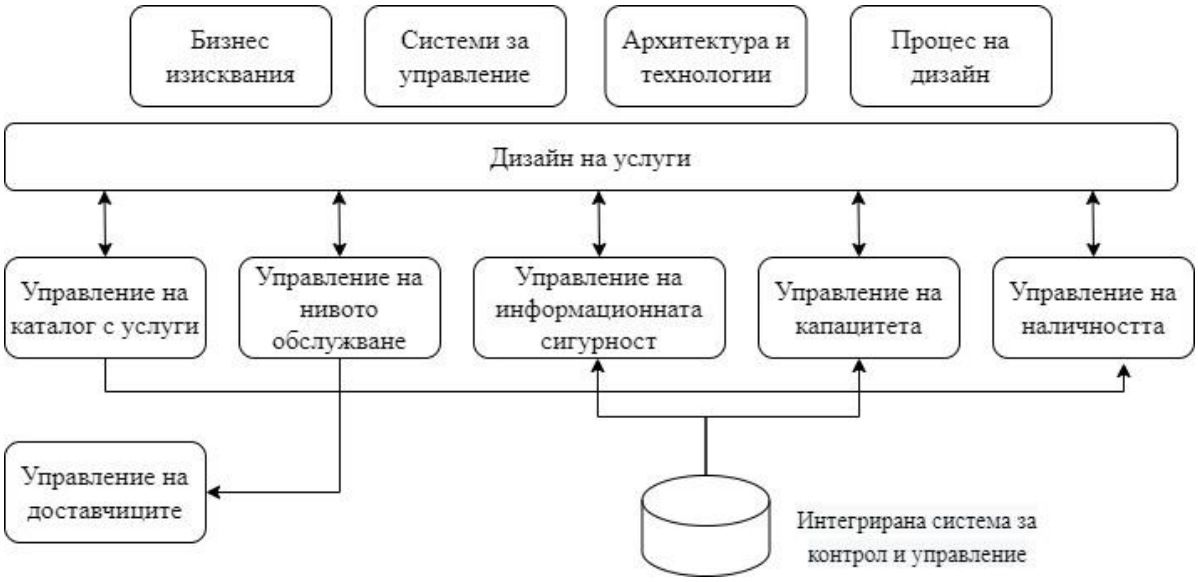
Библиотеката на ИТ инфраструктурата е широко използвана, защото се фокусира върху непрекъснатото подобряване на качеството, ефективността и осигурява пълен жизнен цикъл на ИТ услугите. Процесът на обслужване на проекти включва насоките за проектиране и развитие на услуги и процеси, свързани с управление на ИТ.

Процесът на проектиране на услугата ще бъде разгледан подробно, защото той е важна част от проектирането на онлайн услугите. Този процес включва управление на каталог с услуги; наличност; капацитет; продължителност; сигурност; доставчици.

Библиотеката предлага насоки за развитието и подобряването на преходния период, превръщайки процесите в стандартизирани документално операции. Преходът към услуги изброява изискванията на стратегията за обслужване, анализира проекта за услуги и контролиране на рисковете за отказ. Операцията на услугата съдържа практиките на обслужване на целите и поддръжка за гарантиране на стойността на тези услуги.

С цел унифицирано прилагане на изисквания за киберсигурност е предложено групирането на услугите на ITIL, така че в една група да бъдат услуги със сходни базови конфигурации за проектиране и изисквания към киберсигурността.

На Фигура *4* е показан процеса на проектиране на услуга в ITIL.



Фигура 4. Процеса на проектиране на услуга в ITIL

Източник: Tutorialspoint, ITIL - Service Design Overview, 2021, www.tutorialspoint.com/itil/service_design_overview.htm

Проектирането на услуги включва: обща част, изискванията, концепции за експлоатация и подобряване на услугата, технически и организационен план за внедряване на нова услуга и планиране на прехода. Всички етапи, елементи и описание към тях са представени в *Приложение 10*.

Предимства на подхода са подобрено качество на ИТ услугите, цялостен поглед върху доставката на продукти и услуги, управление на търсенето и увеличаване удовлетвореността на клиентите, намаляване риска от неспазване на бизнес изискванията, както и намаляване разходите при разработване на процедури и практики. Създаването на каталог на услугите е пряко свързано със задачите на изследването.

Рамка за киберсигурност на Национален институт за стандарти и технологии NIST CSF. Обща рамка.

Рамката за киберсигурност (NIST CSF)[24] не въвежда нови стандарти или концепции, а интегрира водещи практики в областта на киберсигурността, които са разработени от организации като Национален институт на САЩ за стандарти и технологии и международната организация по стандартизация. Тя се прилага успешно в по-малки организации и се използва като инструмент за докладване на сигурността на ръководството.

Петте функции на рамката са: Идентифициране, Откриване, Защита, Реагиране и Възстановяване, които осигуряват стратегия за жизнения цикъл на управлението на риска, възможности за подобряване на киберсигурността и комуникацията.

[24] Keller Nicole, “Cybersecurity Framework,” NIST, 2013, https://www.nist.gov/cyberframework.

„Идентифициране“ включва управление на активи; бизнес среда; управление; оценка на риска; стратегия за управление на риска; управление на риска по веригата на доставки. *„Откриване“* включва откриване на инциденти, както и събиране и споделяне на информация за кибер престъпления и заплахи. Връзката със съществуващите процеси в рамките на организациите е силно предимство. Целта на *функцията „Защита“* е разработване и прилагане на подходящи предпазни мерки, за да се гарантира предоставянето на критични инфраструктурни услуги. Тя е разделена на шест категории: Контрол на достъпа, Осведоменост и обучение, Сигурност на данните, Процеси и процедури за защита на информацията, Поддръжка и ремонт, Защитна технология. Определянето на риска е от ключово значение, поради бързо променящия се характер на заплахите за киберсигурност и необходимостта от непрекъсната актуализация.

Пълното описание на функцията „Защита“ е показано в *Приложение 12*.

Критични контроли за сигурност (*CIS CSC*)

Критичните контроли за киберсигурност (ККС) на Центъра за интернет сигурност на САЩ се фокусират върху конкретни практики, които значително увеличават защитата от най-често срещаните кибератаки[25]. ККС показват областите за създаване на програма за управление на риска, защитни стъпки, блокирането на неоторизиран достъп, идентифициране на атаки и инструменти за защита. Препоръчителните насоки за определяне на приоритетите при прилагане на контрола са разделени на три групи. Всяка група за изпълнение определя набор от предпазни мерки.

Основни групи (контроли от 1 до 6), познати като „базисна киберхигиена“, имат за цел да осуетят автоматизираните атаки от външен или вътрешен източник.

Основополагащи групи (контроли от 7 до 16) осигуряват на екипите за сигурност да се справят с повишената оперативна сложност и могат да зависят от специализирания опит за правилното инсталиране и конфигуриране.

Организационни групи (контроли от 17 до 20) представляват съвкупност от най-добри практики за идентификация и контрол на хардуерни и софтуерни активи; непрекъснато управление на уязвимости; защита на имейли и уеб браузъри; сигурност на приложния софтуер; тестове за проникване и други.

Всички критични контроли за киберсигурност са представени в *Приложение 13*.

На базата на направените проучвания и анализи може да обобщим, че всеки един от разгледаните стандарти намира място при проектирането на онлайн услуги. Подхода COBIT 2019 подпомогнат създаването на добавена стойност чрез използването на ИТ. ITIL включва насоките за проектиране и развитие на услуги и процеси. ISO 27001 стандарта използва подход за управление на сигурността основан на риска, което изисква от висшите училища да идентифицират рисковете за информационната

[25] Cisecurity, “The 18 CIS Controls,” Cisecurity, 2022, https://www.cisecurity.org/controls/cis-controls-list/.

сигурност и да изберат подходящи контроли за справяне с тях. Рамка за киберсигурност на Национален институт за стандарти и технологии осигурява стратегия за жизнения цикъл на управлението на риска от киберсигурността, докато ККС могат да бъдат използвани за блокиране на неоторизиран достъп, идентифициране атаките и инструменти за защита.

В раздел 2.2 е направен сравнителен анализ на подходите и стандартите за управление на ИТ и киберсигурност.

Управлението на информационните технологии е инструмент за контрол и управление на информационните ресурси“[26] и е пряко свързано с множество уеб-базирани приложения или специализирани програми за чието функциониране са нужни ясни процеси и процедури.

Много международни рамки и стандарти се занимават с киберсигурността от сходни, но различни позиции, всяка от които предоставя принципи, процедури и практики за ефективно управление на рисковете от киберсигурността. Агенцията на Европейския съюз за киберсигурност публикува доклад, който представя съпоставяне на основните цели за сигурност. В него се дават насоки за оценка на сигурността на данните и спазването на изискванията на директивата за сигурността на мрежите и информационните системи, като предоставя рамка за управление на киберсигурността. Стандартът ISO/IEC 27001:2022 помага на организацията да установява, внедрява, поддържа и непрекъснато подобрява системата за управление на информацията. COBIT и ITIL предлагат подход за оценка на нивото на сигурност, но не и механизми за защита на киберпространството. Отправната точка във разгледаните подходи в раздел 2.1 е определянето на изисквания за информационна сигурност.

За целите на изследването е направен сравнителен анализ на COBIT 2019 и ITIL от гледна точка на връзката им с ISO/IEC 27001:2022, включващ описание, обем, потребители, обхват и приложение. Задачата е да се установят основните предпоставки за модел на базата на общите фундаментални положения в основният подход COBIT 2019.

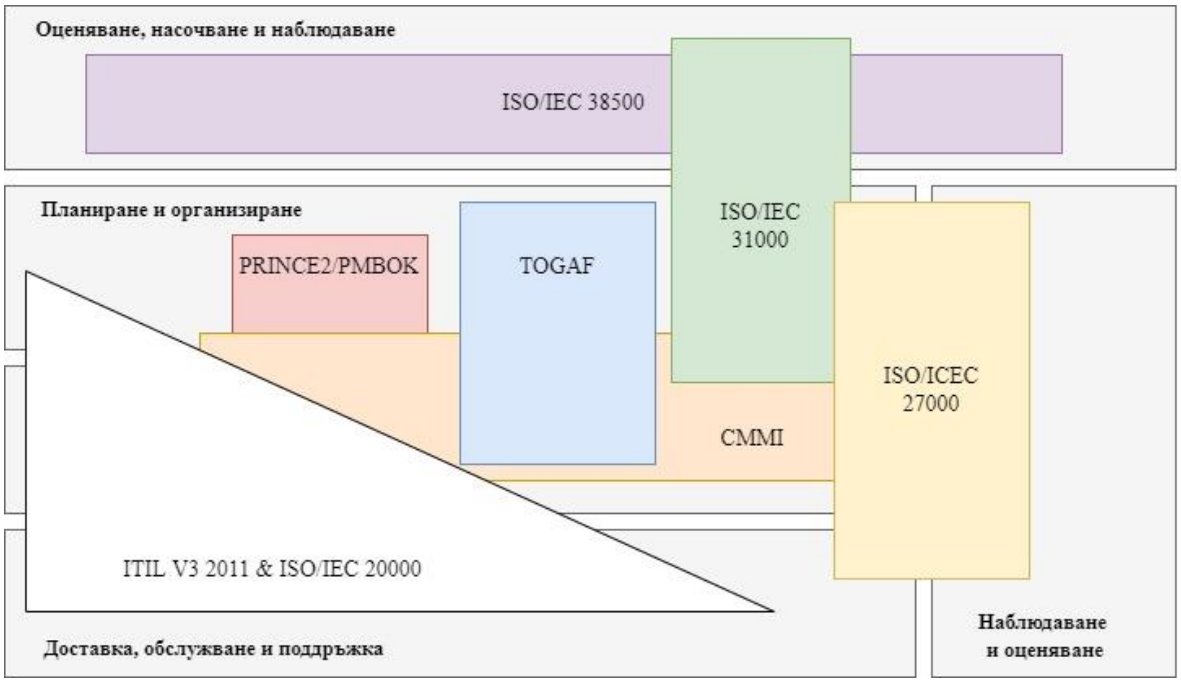
Пълна таблица с подробна информация, за съпоставянето между COBIT 2019 и ISO/IEC 27001:2022 е представена в *Приложение 13*.

Подходът на COBIT 2019 определя нуждите на заинтересованите страни, преобразувани в резултати или влияещи на бизнес целите, които са разпределени в четири категории. COBIT не съответства на еквивалент на методологията на ITIL, но прилагането на комбинация от двата подхода, намалява критичните заплахи за киберсигурността. ISO/IEC 27001:2022 има функции за запазване на поверителността, целостта и достъпността на информацията. Тази наличност на информация се

[26] Isaias Bianchi и Rui Sousa, „IT Governance Mechanisms in Higher Education“, *Procedia Computer Science*, International Conference on enterprise Information Systems, 100 (01 Януари 2016): 941–46, https://doi.org/10.1016/j.procs.2016.09.253.

обработва в рамките на ITIL и COBIT 2019 с аспекти на качеството, надеждността и поддръжката на ИТ[27].

На Фигура 5Фигура 5 е показано съпоставяне на международните стандарти и подходи на информационна сигурност. COBIT 2019 ще бъде по-ефективен избор, ако искаме да подобрим качеството и измеримостта на управлението на ИТ в целия им жизнен цикъл на прилагане. От друга страна, ако търсим непрекъснато подобряване на ефективността на онлайн услугите, ITIL би бил по-добрият избор, защото неговата методика има разлика в структурата си, която се занимава с управление на инциденти и няма еквивалентен раздел в подхода на COBIT 2019[28].



Фигура 5. Съпоставяне на международни стандарти и подходи на информационна сигурност

Източник: ISACA, 2022, www.isaca.org/resources/news-and-trends/industry-news/2017/using-cobit-5-to-assess-it-processes-capabilities-and-evaluate-compliance-with-the-world-lottery-ass

Разликата между ISO/IEC 27001:2022 и COBIT 2019 е, че първият е единствено за целите на информационната сигурност, а вторият е за управление на бизнес процесите в областта на ИТ. COBIT не само отговаря за сигурността в дадена организация, но включва начина, по който организацията подрежда и контролира ИТ операциите. Той има всички контроли, мерки и процеси на информационните технологии и помага на организацията да свърже собствените бизнес цели към своите

[27] Shamsul Sahibuddin и Mohammad Sharifi, „Combining ITIL, COBIT and ISO/IEC 27002“, ResearchGate, б.д., https://www.researchgate.net/publication/325846466_Combining_ITIL_COBIT_and_ISOIEC_27002_in_Order_to_Design_a_Comprehensive_IT_Framework_in_Organizations.

[28] advisera.com, „COBIT vs. ITIL vs. ISO 20000: A comparison“, 20000Academy, б.д., https://advisera.com/20000academy/blog/2019/09/25/cobit-vs-itil-vs-iso-20000-a-comparison/.

ИТ цели. ISO/IEC 27001:2022 се фокусира върху извършване на оценка на риска и след това прилагане на специфични контроли за сигурност за защита на критичните информационни активи. Може да бъде свързан както с COBIT, така и с ITIL.

Направено е съпоставяне между COBIT процесите и цели за контрол на ISO/IEC 27001:2022, свързани с информационната сигурност и проектирането на онлайн услуги.

Важна част от тези процеси са разработването на нови ИТ системи и услуги, работа от разстояние и управлението на непрекъснатостта на бизнеса. Именно затова в изследването по-нататък е разгледан единствено домейна Планирай и организирай в COBIT 2019, защото той има връзка към проектирането на онлайн услуги във ВУ и е разгледан подробно в раздел 2.1. Пълният анализ е представен в *Приложение 15*.

Докладът „Фактори, влияещи върху информираността и отношението към прилагането на ИТ управлението във висшето учебно заведение“[29] показва, че в зависимост от своите стратегии и цели, университетите избират различни подходи за управление на ИТ. Някой се фокусират към управление на услуги, други залагат на управлението и процесите или пък комбинират няколко стандартизирани метода за да имат цялостно управление на ИТ. ВУ в Австрия използват комбинация от COBIT, ITIL и ISO/IEC 27001:2022. Британското висше образование има разработена своя система за управление на ИТ[30], която се използва и от университетите в Испания[31].

В раздел 2.3 са разгледани различните референтни модели за управление на киберсигурността и изискванията към тях.

Ползите от възприемането на подхода на референтния модел включват постигне на оперативна съвместимост в и между различни инфраструктури и подобряване на комуникацията между множеството заинтересовани страни. Предоставя отлични инструменти за дефиниране на обхват по отношение на функционалност или област от включени бизнес процеси. Едно от най-честите предизвикателства, пред които са изправени дизайнерите на информационни системи, е да позиционират нова или съществуваща система по отношение на други подобни или свързани системи. Референтни модели от различни видове са особено полезни за тази цел.

Референтните модели се използват широко в секторите на телекомуникациите и отбраната, както и в корпоративните и публичните организации. Всички те се характеризират с множество доставчици, които трябва да работят с обща рамка от принципи и концепции, за да осигурят оперативна съвместимост.

В международните стандарти[32] референтния модел обозначава “референтните точки“ между функционалните блокове. Обхватът на стандарта произтича от познаването на референтните точки (т.е. възможните области), в които стандартът може

[29] Uky Yudatama и съавт., „Factors affecting awareness and attitude of IT governance implementation in the higher education institution“, в *2017 3rd International Conference on Science in Information Technology (ICSITech)*, 2017, 588–92, https://doi.org/10.1109/ICSITech.2017.8257181.

[30] JISC, “Jisc,” Jisc, 2021, https://www.jisc.ac.uk/.

[31] Universitat de les Illes Balears, “ITG4AU - Universitat de Les Illes Balears,” ITG4AU, 2022, https://itg4au.uib.eu/Project/Mission/.

[32] ISO, NIST, CIS, COBIT 19, ITIL и други

да се прилага. Разбирането как различните стандарти са свързани един с друг се подпомага от наличието на концептуална рамка, в която те са разположени.

Референтните модели обединяват стандарти и тяхното използване улеснява работата на инженерите и разработчиците, които трябва да създават обекти отговарящи на даден стандарт.

В зависимост от своята функционалност референтните модели са: бизнес референтен модел; референтният модел на компонентите (софтуерни и хардуерни); технически референтен модел (компютърно и комуникационно оборудване); референтен модел на данни; референтен модел на производителност; референтен модел за сигурност.

С цел изясняване на структурата на референтен модел са разгледани някои от най-популярните референтни рамки и модели.

Модела на данни на основната архитектура (CADM – Core Architecture Data Model) съдържа в себе си три основни вида архитектурни модели: концептуални, логически и физически.

NIST Enterprise Architecture Model е пет-слоен модел за корпоративна архитектура, предназначен за организиране, планиране и изграждане на интегриран набор от информационни архитектури. Йерархията в модела се основава на това, че една организация има редица бизнес функции, като всяка от тях изисква информация от много източници. Всеки източник може да управлява една или повече информационни системи, които съдържат данни, организирани и съхранявани в произволен брой системи.

Референтния модел отворена архивна информационна система (OAIS – Open Archival Information System) служи за управление на данни. Неговите основни функции са да запази информацията и да осигури достъп до архивираната информация по последователен начин за нуждите на потребителите или на определена общност.

Ориентирана към услуги архитектура (SOA – Service Oriented Architecture) е абстрактна рамка за разбиране на значими обекти и връзки между тях в рамките на ориентирана към услуги среда, както и за разработване на последователни стандарти или спецификации, поддържащи тази среда.

Ориентирана към услуги архитектура предоставя четири различни вида услуги: функционални; услуги за приложения; инфраструктурни, които са инструмент за процеси като сигурност и удостоверяване.

Всяка услуга се състои от интерфейс, договор и внедряване. Интерфейсът определя как доставчикът на услуга ще изпълнява заявки от потребителя на услуга. Договорът определя как трябва да си взаимодействат доставчикът и потребителят на услугата. Внедряването е свързано с управлението на услугата, което контролира жизнения цикъл за разработка и публикуването и в регистър на услугите. Регистъра позволява на разработчиците бързо да ги намират и използват повторно за сглобяване на нови приложения или бизнес процеси.

От изследването по-горе става ясно, че структурата на референтен модел съдържа различни нива на области, функции свързани с тях, обекти към които е насочен моделът, както и множество процеси и процедури. Моделът OSI например, осигурява обща основа за координиране на разработването на ISO стандарти за целите на взаимното свързване на системите.

Основна цел на референтния модел при проектирането на онлайн услуги във ВУ е сигурността. За да бъде постигната е необходимо да има ясна структура и взаимовръзки между отделните части на модела. Всички приложения трябва синхронно да получават и променят данни директно в техния първичен източник, което ще намали необходимостта от поддържане на сложни модели за синхронизиране на данни. Определянето на риска както за информационните системи, така и за всяка онлайн услуга е от ключово значение поради бързо променящия се характер на заплахите за киберсигурност и необходимостта от непрекъсната актуализация.

Изискванията към *киберсигурността* се основават на множество стандарти и добри практики. В статията „Проектиране на киберсигурността“[33] са описани базовите изисквания: *минимизиране площта на атаката, сигурност по подразбиране, най-малка привилегия, защита в дълбочина, доказани модели на проектиране и защитени компоненти, документация за сигурност, поверителност*.

Всички горе изброени добри практики и насоки следва да бъдат част от изискванията на референтния модел за проектиране на онлайн услуги във ВО.

Референтният модел трябва да се основава на бизнес изисквания, а не на съществуваща системна функционалност и да обхваща всички възможни функции в оценяваната функционална област. Ограниченията при прилагането му са свързани със съответствие с нормативните документи в България и в ЕС.

Структура на референтен модел

Референтни модели са абстрактни модели за организация на бизнеса, разработени за конкретни отрасли на база реален опит от внедрявания и включващи проверени на практика процедури и методи за управление. В тях са определени типови бизнес-процеси, хоризонтални и вертикални връзки и бизнес правила, действащи в различни области или върху обекти.

Структурата на референтния модел съдържа: области и обекти; функции; организационна структура; процеси и процедури.

Подобни структури има в редица референтни модели, като техните части се различават в зависимост от функционалността на дадения референтния модел. Областите и обектите могат да бъдат бизнес цели; софтуерни и хардуерни компонентите; компютърно и комуникационно оборудване; информационни активи и данни и други.

Референтните модели позволяват на организациите да започнат разработка на

[33] Ashim Dutta and Prateek Singh, “Cybersecurity Design Principles,” Eaton, 2021, https://www.eaton.com/us/en-us/company/news-insights/cybersecurity/cybersecurity-design-principles.html.

собствени модели на база вече готов набор от функции и процеси, и са предназначени за осигуряване на стандартно описание на моделирането на бизнес процесите и техния анализ.

Широкото приложение на референтните модели е свързано с това, че те предоставят стандартен език, позволяващ използването на единна терминология. Почти всички имат стандартна пътна карта, която осигурява рамка за подобряване на процесите, от създаване на стратегия до прилагане на нови управленски практики, както и набор от най-добри практики, които се асоциират с всеки процес. Референтните модели представят стандартни определения на ключови показатели за ефективност, като по този начин спомагат за измерването на постигнатите резултати и усъвършенстването на бизнес процесите.

В раздел 2.4 са идентифицирани на основни характеристики на референтен модел за кибер сигурност на висшите училища, както и методиката за разработването му.

Стандартизирането на процесите при проектиране и управление на онлайн услугите във ВУ в България изисква разпределяне на отговорности, управление на ИТ и докладване на рисковете. Процесите на оценка и управление на кибер сигурността трансформират политиките за сигурност в конкретни планове, имащи за цел намаляването на заплахите и уязвимостите.

За да бъдат изпълнени общите изисквания за сигурност към референтния модел, описани в раздел 2.3, той трябва да обхване функции и контроли от разгледаните стандарти в раздел 2.1 (COBIT 2019, ITIL, ISO/IEC 27001:2022, NIST CSF и CIS CSC), като се фокусира върху вграждането на киберсигурността в етапите при проектиране на онлайн услуги във ВУ.

Изискването за минимизирането на площта на атаката може да бъде постигната чрез прилагане на рамката за киберсигурност (NIST CSF) и критичните контроли за киберсигурност (CIS CSC). Определянето на риска е от ключово значение и при двата подхода, поради бързо променящия се характер на заплахите за киберсигурност.

Критичните контроли за киберсигурност ще бъдат използвани, защото те представляват съвкупност от най-добрите практики за идентификация на хардуерни и софтуерни активи, непрекъснато управление на уязвимости, защита срещу злонамерен софтуер, възстановяване на данни и други.

Изискването за сигурност по подразбиране може да бъде изпълнено, както при проектирането на нови услуги, така и при препроектирането на съществуващи такива, чрез използването на COBIT 2019. Подходът поддържа високо ниво на съответствие и включва части от други стандарти за информационна сигурност, чрез ясно разграничаване между нивата стратегическо управление и оперативно управление (мениджмънт).

Изискването за защита в дълбочина може да бъде изпълнено, чрез прилагане на контролите за сигурност от Приложение А на стандарта ISO/IEC 27001:2022.

Изискването за използване на доказани модели на проектиране и защитени компоненти може да бъде изпълнено, чрез прилагането на библиотеката на ИТ инфраструктурата (ITIL).

Изискванията за най-малка привилегия, документация за сигурност и поверителност се покриват от горе разгледаните стандарти и затова няма да бъдат разглеждани подробно.

Структура и взаимовръзки в предлагания референтен модел за кибер сигурност

На базата на направеният анализ на чуждият опит в раздел 1.2 и след преглед на референтните модели за управление на киберсигурността в раздел 2.3 е избрано референтният модел да се състои от обекти, функции, профили и процеси, пряко зависещи от контролът на достъп.

На Фигура 6 е представена структура и взаимовръзки в предлагания референтен модел.

Фигура 6. Структура и взаимовръзки в предлагания референтен модел

Структурата на предлагания референтен модел покрива определените области описани в раздел 2.3.

Референтният модел за киберсигурност при проектирането на онлайн услуги във ВУ се състои от обекти, функции, процедури и организационна структура. Всички елементи са обединен от процесите на управление на ИТ и използваните стандарти, и рамки за управление на ИТ и киберсигурността.

Политики и стратегии за управление на ИТ, базирани на стандарти се постига чрез прилагане на областите „Обвързване, планиране и организиране“, „Изграждане, придобиване и внедряване“ от COBIT 19. Тези две области следват общия жизнен цикъл на развитието на системите и ще бъдат включени в референтният модел. Първата обхваща стратегическото ИТ планиране, създаване на корпоративна информационна архитектура и управление на проекти, а втората е свързана с внедряването на нови информационни системи и услуги. Определяне на процесите и взаимоотношенията трябва да съответства на вътрешна организация, оперативни процедури и свързаните с

тях роли и отговорности.

В изследването е разгледан единствено домейна Планирай и организирай в COBIT 2019, защото той има връзка към проектирането на онлайн услуги във ВУ.

Контрол на достъп в референтния модел е свързан с препоръчителните контроли за сигурност към различни обекти и процеси. От анализа на стандартите раздел 2.1. и сравнителният анализ в 2.2 видяхме, че COBIT съдържа в себе си ITIL ISO и е приложим за големи организации, каквито са университетите.

Обектите в предлаганият референтен модел са основните информационни системи и произлизащите от тях онлайн услуги. От анализа на чуждия опит в раздел 1.2 беше направен извода, че основните системи във ВУ са: административни, информационна сигурност, учебна дейност и научно изследователски системи. Те имат нуждата от специфични контроли за сигурност и към тях в раздел 3.2 трябва да бъдат реферирани документи от използваните стандарти.

Функциите са пряко свързани с управлението на обектите и се избират в зависимост от рисковия профил на информационната система или онлайн услуга. В референтния модел се използва функцията „Защита“ от стандарта NIST CSF, която очертава подходящите предпазни мерки за предоставяне на критични инфраструктурни услуги и поддържа възможността за ограничаване на въздействието на потенциално събитие за киберсигурност.

Процедурите са представени като модел съгласно цели, действия и документи от стандарти, защото проектирането на онлайн услуги или промяна на съществуващи, изисква установяването на общи процеси и процедури. Те са свързани с проектирането на нова онлайн услуга, взимат се от стандарта ITIL, като референтният модел показва всеки описан от стандарта процес и свързаният рамков елемент към него.

Организационната структура е добавена поради разнообразните потребителски групи в университетите и показва уникално привеждане на административните роли в съответствие с контрола на достъп.

Матрицата RACI от подобие на референтния модел COBIT 19 се използва за да се идентифицират ролите и отговорностите, пряко свързани с организационната структура и управлението на киберсигурността. Матрицата RACI е разгледана подробно в раздел 3.3.

Изводи

В *Глава втора* са анализирани подходите и стандартите за управление на информационни технологии и киберсигурност във ВО.

Представени са най-често използваните референтни модели за управление на ИТ услуги и киберсигурност. Идентифицирани са техните основни характеристики и възможности за използването им при проектирането на онлайн услуги.

ВУ имат различни организационни структури и специфични изисквания за осигуряване на пълния набор от процедури за киберсигурност при проектирането на онлайн услуги. Университетите в България, като образователни институции,

предоставящи обществени услуги трябва да бъдат сертифицирани по ISO/IEC 27001:2022. Използването на ITIL ще спомогне за непрекъснато подобряване на ефективността на онлайн услугите.

В предлагания референтен модел ще бъдат използвани следните пет стандарта: Цели за контрол на информацията и свързаните с тях технологии (COBIT 19), Стандарт за управление на информационната сигурност (ISO/IEC 27001:2022), Библиотеката на инфраструктурата на информационните технологии (ITIL), Рамка за киберсигурност на Национален институт за стандарти и технологии (NIST CSF) и Критични контроли за киберсигурност (CIS CSC). Избраните стандарти, покриват целият жизнен цикъл при проектирането на онлайн услуги, имат контроли за киберсигурност и успешно се използват в много ВУ по света.

Референтният модел се състои от обекти, функции, процедури и организационна структура, обединени от политики и стратегии за управление на ИТ и контрол на достъпа.

Определени са изискванията и ограниченията към предложеният референтния модел, които са свързани със запазване на поверителността, целостта и достъпността на информационните ресурси, намаляване на критичните заплахи и създаване на добър управленски модел за ИТ във ВУ.

Глава III. Приложение на методиката за разработване на референтния модел

Настоящата глава описва процеса на разработване на референтния модел.

В Глава III са изпълнени следните поставени задачи:

1. Да бъде създаден референтен модел за киберсигурност и стандартизиране на процесите на управление на онлайн услугите във ВУ в България.

Направен е анализ на университетските сайтове, за да се види как различните университети са организирали каталога на предлаганите от тях онлайн услуги. На базата на направеното проучване, и с цел унификация на различните онлайн услуги, е приет подхода те да са групирани в същите категории към които информационните системи спадат. Идентифицирана е оценката на риска на университетските системи в зависимост от въздействието и вероятността от уязвимости за сигурността им.

Контролите за сигурност са реферирани към документи от изследваните стандарти и са представени подробно в раздел 3.2.

Раздел 3.1 обхваща събиране и анализ на данни. Използвани са данните от платформа за сканиране на уеб сайтове. Анализът обхваща първата страница на сайта на университета и показва броят заявки, трансфери, домейни и поддомейни, използвани протоколи, както и различните настройки за сигурност на хедъра на страницата.

Много стандарти за киберсигурност подчертават важността на точното определяне на риска чрез систематичен процес на управление на риска.

Идентифицирането, количественото определяне и смекчаването на риска са съществени фази на управление на риска. Намаляването на риска чрез адекватен контрол е свързано с прилагането на строги мерки за киберсигурност.

На базата на направеното изследване в Глава първа, раздел 1.2 са определени основните информационни системи във ВУ.

Използвайки COBIT 19 е направена оценка на риска на университетските системи, като е взето предвид въздействието и вероятността им от уязвимости. Те са отчетени по скала от 1 до 5 (1 е ниско, 5 е много високо).

Таблица 1. Оценка на риска на университетските системи, на базата на COBIT 19

Информационни системи	Въздействие (1-5)	Вероятност (1-5)	Оценка на риска
Административни системи	5	3	Много висок
Информационни системи	5	4	Много висок
Поддръжка и обучение	4	3	Висок
Научни изследвания	2	2	Нормален

Източник: www.isaca.org/resources/cobit

От Таблица 1 се вижда, че Административните и Информационните системи имат много висока оценка на риска. Рискът при системи свързани с „Поддръжка и обучение“ се определя като висок, а при системите свързани с „Научни изследвания“ е нормален.

Каталог на услугите представлява пълен списък на услугите, управлявани от университета. Някои от тези услуги са видими за клиентите, докато други не са. Контролите за сигурност към информационните системи за твърдо зададени, докато контролите към услугите се променят в зависимост от това дали са видими или не (имат ли достъп до интернет или не), както и в съответствие с техният моментен статус.

Направен е преглед на университетските сайтове, за да се види в какви категории са организирани услугите. Различните университети са възприели различни начини за организация на каталога на предлаганите от тях услуги. Много от категориите се припокриват по съдържание, но са именувани по различен начини.

В Таблица 2 могат да бъдат видени университетските информационни системи и категориите услуги към тях. Всяка категория включва услуги със сходни технологични процеси и изисквания за киберсигурност в съответствие с използваната информационна система.

Таблица 2. Информационни системи и категории услуги във ВУ

Информационни системи	Категории услуги
	Профили и удостоверяване

Административни системи	Архивиране и съхранение
	Информационна сигурност
	Комуникация и сътрудничество
Информационни системи	Мрежи и инфраструктура
	Сървъри и данни
	Уеб разработка и хостинг
	Хардуер, софтуер и приложения
Учебна дейност	Осведоменост и обучение
Наука	Научни изследвания

Източник: Собствено проучване

В някой сайтове, услугите могат да бъдат филтрирани не само по категория, но и по вид потребители (напр. студенти, преподаватели, служители и други).

Описание на категориите услуги във ВУ:

Профили и удостоверяване – услуги, свързани с удостоверяване, оторизация и управление на акаунти, системи за контрол на достъпа и др.

Архивиране и съхранение – услуги, свързани със съхранение, споделяне и управление на университетски данни с умерен и висок риск.

Информационна сигурност – услуги, свързани със сигурността на информационните активи, мрежова свързаност, дисково криптиране и др.

Комуникация и сътрудничество – услуги, свързани с кандидат-студентски и магистърски кампании, организиране на събития и конференции и др.

Мрежи и инфраструктура – услуги, свързани с управлението на информационните системи, поддръжка и изграждане на мрежи за данни и др.

Сървъри и данни – услуги, свързани със системно администриране, управление на конфигурацията на крайна точка, миграция на данни, виртуални сървъри и др.

Уеб разработка и хостинг – услуги, свързани с уеб инфраструктурата и ресурсите на университета, уеб хостинг, домейни и др.

Хардуер, софтуер и приложения – услуги, свързани с управление на настолни компютри, лаптопи, мобилни телефони и периферни устройства, лицензиран софтуер, програми и модули, облачни услуги и др.

Поддръжка и обучение – услуги, свързани със създаването на дигитални образователни ресурси, участие в стажантски програми, обучение, консултации и др.

Научни изследвания – услуги, свързани с изследователски административни системи, съхранение на научни данни и публикации, техническа поддръжка и др.

На базата на направената оценка на риска на университетските системи, използвайки подхода COBIT 19, към тях са отнесени произлизащите от тях услуги, като е взето предвид въздействието и вероятността им от уязвимости. Те са отчетени по скала от 1 до 5 (1 е ниско, 5 е много високо).

Таблица 3. Оценка на риска на онлайн услуги, чрез методологията на COBIT

Информационни системи	Онлайн услуги	Въздействие (1-5)	Вероятност (1-5)	Оценка на риска
Административни системи	Профили и удостоверяване	5	3	Много висок
	Архивиране и съхранение	4	2	Висок
	Информационна сигурност	5	4	Много висок
	Комуникация и сътрудничество	2	2	Нормален
Информационни системи	Мрежи и инфраструктура	4	4	Висок
	Сървъри и данни	5	4	Много висок
	Уеб разработка и хостинг	3	3	Нормален
	Хардуер, софтуер и приложения	4	5	Много висок
Поддръжка и обучение	Осведоменост и обучение	4	3	Нормален
Научни изследвания	Научни изследвания	2	2	Нормален

Източник: Собствен анализ на базата на направено изследване.

От таблица Таблица 3 се вижда, че услугите в категория „Профили и удостоверяване“, „Архивиране и съхранение“ и „Информационна сигурност“ имат високо въздействие. Услугите от „Комуникация и сътрудничество“ има нормален риск, тъй като към нея няма високи изисквания за сигурност.

Услугите в категория „Мрежи и инфраструктура“, „Сървъри и данни“ и Хардуер, софтуер и приложения“ се характеризират с високо въздействие и много голяма вероятност от риск за сигурността. Оценката на риска при услугите „Уеб разработка и хостинг“ е нормален. Рискът при услугите свързани с „Поддръжка и обучение“ и „Научни изследвания“ се определя като нормален.

Групирането на услугите е важна стъпка, свързана със създаването на каталог на услугите във ВУ. Управлението на каталога на услугите включва всички процеси от жизненият цикъл на проектиране на услугата, нейната защита и архивиране. ITIL идентифицира изискванията за услуги и разработва нови предложения за услуги, както и промени и подобрения на съществуващите.

Всички услуги трябва да имат изисквания за киберсигурност за да се гарантира, че потребителите и процесите ще получат достъп само до информация или ресурси за които имат права. Изисквания трябва да има и относно неразрешеното създаване, изменение или изтриване на информация. Това включва всички функции, предназначени да контролират потока от информация и използването на ресурси от потребители, процеси и обекти. Услугите, свързани с административни системи трябва да имат изисквания за осигуряване на специфични функции, предназначени да гарантират, че данните няма да бъдат модифицирани по неоторизиран начин.

Функцията надеждност на услугата гарантира, че достъпът до ресурси е възможен, когато е необходимо, и че ресурсите не се искат или задържат ненужно. Обмен на данни обхваща всички функции, предназначени да гарантират сигурността на данните по време на предаване по комуникационни канали. Функциите за откриване и възстановяване на грешки свеждат до минимум прекъсванията или загуба на услуга.

В раздел 3.2 е направено отнасяне (реферираne) на контролите за сигурност към функциите на модела.

Контрол на достъпа във връзка с функциите

Контролът на достъп обхваща всички идентификационни данни, които се издават, управляват, проверяват, отменят и одитират за оторизирани устройства, потребители и процеси. Той се прилага към административните и информационните системи и контролите за киберсигурност към него са най-много.

Осведоменост и обучение: Тази област е определяща за това дали преподавателите и служителите получават обучение за киберсигурност и дали могат да изпълняват своите задължения и отговорности в съответствие със съответните политики, процедури и споразумения. Тя има три подкатегории - Обучение по сигурността, Привилегировани потребители и служители и Заинтересовани лица от трети страни.

Сигурност на данните: Данните се управляват в съответствие с рисковата стратегия на организацията за защита на поверителността, целостта и наличността на информацията. Тази област има пет подкатегории: Сигурност на данни, Управление на активи, Защита на данни, Проверка на целостта на софтуера и информацията и Среда за разработка и тестване.

Защита на информацията: Политиките за сигурност се поддържат и използват за защитата на информационните системи и активи. Тази област има седем подкатегории - Базова конфигурация на информационни технологии/системи. Жизнен цикъл на развитие на системата за управление на системите, Процеси за контрол на промяната на конфигурацията, Архивиране на информацията, Разпоредби относно физическата работна среда за организационните активи, Процеси на защита и Киберсигурността в практиките за човешки ресурси.

Защитна технология: Техническите решения за сигурност се управляват, за да гарантират сигурността и устойчивостта на системите и активите, в съответствие със съответните политики, процедури и споразумения.

Най-важните характеристики на съвременните инструменти за защита на онлайн услугите включват видимост и защита, покритие на различни архитектури, интеграция с DevOps инструменти, автоматизация и непрекъснати актуализации.

Видимостта на използваните услуги, трафикът, който тече към тях, и свързаността на крайни точки са критични. За да защитят услугите, базирани както в локалната, така и в облачната инфраструктура, ВУ трябва да осигурят съвременни решения и гъвкавост при внедряването.

Възможността за интегриране, с балансиращи натоварването шлюзове или използването на софтуер, като услуга осигурява избор и последователност, независимо от типа на защитената услуга. Динамичният пейзаж на заплахите прави ръчното актуализиране, тестване и внедряване на набори от правила и контроли за сигурност невъзможна задача. Именно затова са необходими инструменти и модели, които могат да осигуряват автоматизация и да позволяват оркестрация в цялата инфраструктура на приложенията. Важно е инструментите и контролите за сигурност на уеб приложенията да пасват на техните процеси и да се интегрират с инструментите, които екипите на ИТ отдела използват. За да постигнат това, университетските уеб приложения и онлайн услуги трябва да имат широк набор от функции и възможности, сигурност по дизайн, вграждане на киберсигурността във всички процеси и поддръжка за нови технологии.

В раздел 3.3 са разработени процедурите в референтния модел.

Структурата на референтния модел описана в раздел 2.4 включва организационна структура, роли, отговорности и процедури.

Организационната структура представлява отдели, в които са формирани ролите, отговорностите и техните взаимовръзки според избраните критерии за структуриране. Организационните роли са свързани с изпълнителите на задачи постигането на бизнес целите.

ВУ нямат идентични организационни структури на ИТ дирекции и отдели. Всеки университет се е развил и променил въз основа на множество фактори с течение на времето, а организационната структура е различна в зависимост от големината и дейността. ИТ дирекциите могат да бъдат интегрирани в институцията, докладвайки чрез декани или ръководители на отдели, но те също могат да бъдат административни звена, докладващи директно на ректорите, чрез главни информационни служители, или в редки случаи чрез главни финансови или административни служители.

Стандарта ISO 27001:2022 има разработени шаблони за организационна структура на информационната сигурност на малки, средни и големи организации. В малките организации е характерно, че един човек съвместява няколко длъжности, докато в големите организации, работят експерти отговарящи за определена сфера от ИТ. Служителите в ИТ дирекциите управляват широка гама от дейности, понякога с двойни роли за административни и академични функции.

Някои ВУ може да имат специални комисии на борда, фокусирани върху информационните ресурси, докато други са склонни да диверсифицират

информационната подкрепа в други по-централни функции като записване, обучение и студентски живот.

Стандарта COBIT 19 има определена организационна структура, свързана с каскадирането на целите и процесите в него.

Изпълнението на процедурите в референтния модел е свързано с разпределението на ролите и отговорностите за управление на ИТ. За изясняването им е разгледана организационна структура в COBIT 19, както и ролите и отговорностите свързани с проектирането на услуги в ITIL.

Ролите се основават на процесите на проектиране на онлайн услуги, както и на общи ИТ практики, а имената и комбинациите може да варират в зависимост от организационната структура на ВУ. Ключово за всеки университет е да гарантира, че въз основа на неговата структура, предлагани услуги и процеси, може лесно да се идентифицират, документират, присвояват и преглеждат съответните роли.

Понятието процедура е набор от последователност на установени действия за изпълняването на специфична задача. Наличието на процедура при проектирането на онлайн услуги гарантира, че всяка предложена услуга и приета промяна се оценява в последователен и повтарящ се начин от гледна точка на кибер сигурността.

Процедурите за работа с референтния модел описват стъпките, които трябва да се следват и включват всички етапи, свързани със създаването на нова услуга от координация на проектирането до избор на реферирани контроли за сигурност.

Описание на процедурите

1. *Координация на проектирането* - При тази процедура се използват графиките от COBIT 19 за да разпределят ролите на изпълнителното ръководство свързани с разработката на новата услуга.
2. *Преглед на класификацията на информационни системи* – определяне с кои тип информационна система ще работи бъдещата услуга.
3. *Преглед на класификацията на услуги* – определяне към коя група услуги може да бъде причислена новата услуга.
4. *Преглед на функциите на киберсигурност* – гарантиране, че са включени всички функции на киберсигурност, които са необходими за конкретната услуга.
5. *Избор на системни компоненти* – определяне на кои системни компоненти трябва да бъдат включени архитектурни ограничения, критични точки за сигурността и защитни механизми.
6. *Управление на базовата конфигурация* – гарантиране, че всяка предложена и приета промяна се оценява в последователен и повтарящ се начин от гледна точка на кибер сигурността и систематичност.
7. *Управление на каталог на услуги* – предоставяне на информация за услугата, текущо състояние и взаимозависимостите й с други услуги.
8. *Управление на контроли за сигурност* – гарантиране, че приложените стандарти и свързаните към тях контроли за сигурност от референтните документи

отговаря на предвиденото ниво на риск за новата услуга. За определен тип услуги може да бъде по-удачно да се използва стандарта ISO/IEC 27001:2022, докато за друг тип да е по-подходящо използването на ITIL.

Често пъти организационните политики, процедури и стандарти се разработват много преди завършването на проектирането на услугата. Контролите, които са удовлетворени от тези политики, процедури и стандарти, могат да бъдат оценени преди пускането на услугата.

На базата на сравнителният анализ между COBIT 2019 и ITIL в раздел 2.2 стана ясно, че прилагането на комбинация от двата подхода намалява критичните заплахи за киберсигурността. Именно затова ролите са взети от подхода COBIT 19, а процесите свързани с проектиране на услуга от стандарта ITIL.

Подходът COBIT 19 определя множество роли, свързани с организационната ИТ структура. Те включват главен директор, натоварен с ДТ и киберсигурността; главен директор по риска отговорен за всички аспекти на управлението на риска в организацията; главен директор ИТ, отговорен за цялостното управление на ИТ; главен оперативен директор, отговорен за бизнес стратегии, планиране и управление на предоставянето на услуги и решения за ИТ; главен служител по сигурността, отговорен за всички аспекти на управлението на информационната сигурност.

Всички роли и отговорности в COBIT 19 са показани в *Приложение 17*.

Матрицата RACI в COBIT 2019 позволява да се идентифицират ключовите тематични области, изискващи ясни роли и отговорности за вземане на решения. RACI има четири вида асоциации: отговорни, отчетни, консултирани и информирани. Електронната таблица, публикувана на страницата COBIT предоставя насоки, които показват процесите подходящи за всяка длъжност[34]. Матрицата разбива всеки един процес и предоставят гъвкави насоки за това коя роля в организацията е „Отговорна“ или „Отчетна“ за всеки процес. След като бъдат определени тези две ключови роли, могат да се определят ролите за „Консултирани“ и „Информирани“ въз основа на уникалните изисквания на всяко ВУ. Предимство от събирането на всички процеси в RACI е, че лесно може да се филтрират всички практики по отчетност на една роля и след това да се сравнят показателите, отчитащи тези практики.

В ITIL има определени мениджърски позиции, свързани с проектирането на услуги, непрекъснатост, сигурност, капацитет, наличност, съответствие, управление на каталог на услуги, доставчиците и други.

Всички роли, свързани с проектирането на услугите на ITIL изискват специфични умения, качества и компетенции от участващите хора, за да могат да работят ефективно и ефикасно и са показани в *Приложение 18*.

[34] ISACA, “COBIT | Control Objectives for Information Technologies,” ISACA, 2022, https://www.isaca.org/resources/cobit.

Всяка организация определя подходящи длъжностни характеристики, които отговарят на техните нужди и лицата, заемащи тези длъжности, могат да изпълняват една или повече от необходимите роли.

Структурите на ВУ включват общо събрание, академичен съвет, ректор и ректорско ръководство, контролен съвет, комисия за академична етика, факултети, дирекции, институти, центрове и други. В държавните институции тези основни организационни единици си сътрудничат с външни органи като държавни, обществени и бизнес организации. Външните организации ежедневно взаимодействат и оформят политиките и процедурите на вътрешните организационни структури на университета.

Според стандарта ISO 27001:2022 организационната структура на информационната сигурност във ВУ би трябвало да има Комисия по сигурност, включваща мениджър информационна сигурност и комисия по сигурността в различните отдели.

Изводи

В *Глава трета* е структурирано приложението на методиката за разработване на референтния модел. Анализът на най-често срещаните уязвимости в инфраструктурата и уеб приложенията показва, че университетите се съсредоточават върху контроли за сигурност и процеси, които са предимно базови и това често води до пропуски в сигурността.

Направената оценка на риска на университетските информационни системи и услуги по методологията на COBIT 2019 показва, че административните услуги и услугите свързани с информационната сигурност имат най-висок риск за сигурността.

Университетите са възприели различни начини за организация на каталога на предлаганите от тях услуги. На базата на направеното проучване е приет подход онлайн услугите да бъдат групирани в съответствие с изисквания към киберсигурността на използваната от тях информационна система.

Предложеният референтен модел описва основните информационни системи и услуги във ВУ, както и начините, по които се свързват и взаимодействат помежду си. Модела обединява няколко стандарта за управление на ИТ и киберсигурност и задава стандарти както за обектите в модела, така и за техните взаимоотношения един с друг. Реферирани са контролите за сигурност към функциите на модела.

Процедурите за работа с референтният модел включват ясно дефинирани процеси при проектирането на услуги, за да се гарантира, че всяка предложена услуга и приета промяна се оценява в последователен и повтарящ се начин от гледна точка на киберсигурността.

Установени са ролите и отговорностите, свързани с управлението на ИТ във ВУ. Използването на референтния модел ще помогне на мениджърите в разработката на онлайн услуги да разделят проблемното пространство на по-малки части, които могат да бъдат разбрани, решени и усъвършенствани.

Глава IV. Верификация и валидация на референтен модел

В Глава IV са изпълнени следните поставени задачи:

1. Моделът да бъде верифициран и валидиран чрез анализ на документи и интервюта с експерти. Референтният модел да бъде внедрен чрез създаване на онлайн приложение.

В раздел 4.1 е направен избор на платформа за разработване на тестово софтуерно приложение. Разгледани са най-популярните системи за управление на съдържанието с отворен код - WordPress, TYPO3, Joomla!, Drupal, Contao, Neos, WooCommerce, OpenCart, AbanteCart, PrestaShop[35]. Направено е сравнение на техните специфични функционалности в областите на инсталация и конфигурация, управление на потребители, каталог на услуги, създаване на съдържание, филтриране на данни, възможности за промени на изходния код и адаптиране на системата към индивидуалните изисквания за кибер сигурност.

С цел намиране на най-доброто софтуерно решение е направено задание към платформата, разделено в областите: администриране, управление на съдържанието, каталог на услуги, известия и коментари, проследяване и отчитане, съобразено с изследователските анализи направени в глава Втора, раздел 2.3.

За целите на дисертационния труд е избрана OpenCart платформа, която дава възможност да се създадат множество администраторски роли с различни права на достъп, добавяне на неограничен брой услуги, създаване на връзки към избрана категория или под категория (напр. информационни системи, области на киберсигурност, контроли за киберсигурност), статус на услугата (активна, неактивна, в процес на разработка), сходни и свързани услуги, както и добавяне на информационни страници.

В административния панел има общ преглед на всички услуги, потребители, последни редакции, инструменти за запазване и възстановяване на данни, отворен за редакция код и богата документация. Специфична функционалност е добавяне на групи атрибути и атрибути към група. Групите атрибути са използвани за въвеждането на използваните стандарти, а атрибутите към всяка група за въвеждане на контроли за киберсигурност от съответният стандарт. Създадена е и възможност за филтриране и сортиране на услугите по специфични функции (напр. критичност на услуга).

Описание на приложението – потребителски интерфейс

Лентата с основното меню е разположена хоризонтално в горната част на сайта. Бутоните са както следва: Начало, Референтен модел, Стандарти, Информационни системи, Киберсигурност и Онлайн услуги. На Фигура 7 е представена екранна снимка на първата страница на сайта.

[35] "3 Open Source Content Management Systems Compared," Opensource, 2021, https://opensource.com/business/14/6/open-source-cms-joomla-wordpress-drupal.

Фигура 7. Екранна снимка на първа страница на платформата - https://csservices.online

Частта „Референтен модел" включва четири подменюта: описание, процес на работа, верификация и валидиране, екип. На страницата Описание на модела е направено и качено видео, показващо работата с основните функционалности на платформата.

Частта Верификация и валидиране (*https://csservices.online/верифициране-и-валидиране*) съдържа информация от одита на уеб платформата, направен през сайта www.semrush.com/siteaudit. Създадена е галерия „Тестване на уеб платформата" с екранни снимки от одита. Страницата съдържа линк към анкетата и казуса във Формс за верифициране на референтния модел.

Частта „Стандарти" обхваща използваните стандарти (ISO/IEC 27001, COBIT 2019, ITIL, NIST CSF, CIS CSC), като за всеки един от тях е дадено кратко описание, контроли за сигурност и полезни връзки към официалните сайтове.

Частта „Информационни системи" обхваща четирите основни типа системи: административни, информационни, учебна дейност и наука.

Частта „Киберсигурност" обхваща петте области: контрол на достъп, сигурност на данните, осведоменост и обучение, защита на информацията и защитни технологии.

Частта „Уеб услуги" обхваща основни видове университетски услуги свързани към типовете информационни системи: административни, информационни, поддръжка и обучение, научни изследвания.

Навигацията във вътрешните страници в уебсайта има последователно именуване, оформяне и позициониране. Сайтът има адаптивен дизайн, показващ съдържанието в различни размери на екрана (напр. мобилни устройства и таблети).

Описание на приложението - административен интерфейс

Административния панел е разделен на следните части: обзор, журнал, каталог, галерия, клиенти, системни, отчети, файлов мениджър и визуален редактор.

Обзор е частта, която дава информация за потребителите и нови заявени услуги. *Журнал* е частта, отговорна за стилове, изгледите на отделните видове страници, информацията, която да бъде включена в горната и долната част на сайта, управление на модули, както и всички системни настройки. *Каталог* е основната част, свързана с управлението на категориите и услугите и включва: продуктови етикети, филтри, атрибути, опции, файлове за теглене, коментари и обща информация.

Галерията **дава** възможност **за** добавяне на албуми с екранни снимки от различните етапи на разработване на дадена уеб услуга или тестване, като прави прегледа на дизайн, функционалности и одит на услуги много лесни. *Дизайн*ът е отговорен за изгледи, редактор на тема, банери, SEO URL адреси. От *Системни* се определят всички настройки, потребители, база данни, хостинг панел, поддръжка (архивиране, регистър на грешките). В *Отчети* могат да бъдат разгледани различни статистики. В *Файлов мениджър е* организирането на всички качени файлове в персонализирани папки.

Предимства са различните интерфейси за управление на шаблони и модули, автоматично оразмеряване на изображения, редактиране на услуги, доклади и статистика улесняват управлението на каталога на услугите.

Въвеждане или редакция на услуга има следните полета:

- Общи – име на услугата и автоматично генериране на SEO адрес, описание;
- Данни - статус, подредба по азбучен ред или ръчно номериране
- Връзки – доставчик на услугата, връзка с категории, филтри, файлове за теглене, свързани услуги
- Атрибути – контроли за сигурност и описание, които се извикват от предварително зададен списък
- Опции
- Период – време, в което услугата е активна и достъпна
- Изображение – снимки от процесите на проектиране на услугата

Платформата има възможност за добавяне на неограничен брой атрибути (стандарти използвани в референтния модел), както и тяхното подреждане по приоритет.

Одита и тестване на софтуерното приложение е направен през сайта www.semrush.com. От него се вижда, че няма проблеми с дублирано съдържание или неработещи вътрешни връзки. Направена е галерия, показваща всички етапи на одита: https://csservices.online/index.php?route=gallery/album.

Верификацията на референтния модел има за цел провери дали техническо задание, програмния код и документация, създадени в хода на разработката, съответстват на правилата и стандартите на ИТ. Посредством формална верификация е

направен преглед на коректността на програмното осигуряване, като са избрани ключови информационни системи и база данни.

Сценарии за разработване на онлайн услуги, свързани с различни типове информационни системи

В уеб платформата са качени примерни услуги, за които е определено с кои информационни системи работят, типовете услуги, към които спадат, както и реферираните контроли за сигурност към тях. *Например: отдалечен достъп VPN, услуги за студентски общежития, промяна на забравена парола в Уеб Студент, регистрация в Уеб Студент, онлайн записване на новоприети бакалаври, планиране и отчитане на НИД, предоставяне на уеб хостинг за изследователски цели.* Някои от услугите са обозначени като „в процес на разработка“ и към тях може да бъде приложен референтният модел. *Например: заявка за избор на спорт, справка за годишен отпуск, информационна кампания, администриране на изследователски системи, архивиране и съхранение.*

На базата на създадените процедури за работа с референтния модел в Глава 3, раздел 3.3 се попълва таблица шаблон с информация за новата услуга. В нея се вписват потребителите на услугата, определя се с кой тип информационни системи ще работи бъдещата услуга, към коя група услуги може да бъде причислена. Разглеждат се областите на киберсигурност и се включват само тези областите, които са необходими за конкретната група услуги и се прилагат контроли за сигурност от референтните документи, които отговаря на предвиденото ниво на риск за проектираната услуга.

Анкета, описание и казус за работа с референтния модел

С цел да се валидира предложения модел и за да бъдат установени възможностите за усъвършенстването му е направено проучване, базирано на експертно мнение на хора от ИТ сектора. Проучването е структурирано в три раздела, като включва анкета с информация за участниците, въпроси свързани с информационната сигурност при проектирането на онлайн услуги и практически казус, имащ за цел създаването на примерна услуга и определяне на контроли за киберсигурност към нея. Решаването на казуса и изказването на експертно мнение по проблемите, обхванати в научното изследване са с най-голяма тежест.

Анкетата и описание за работа с референтния модел бяха изпратени на повече от 50 експерти, работещи в ВУ, както и в други сфери, свързани с киберсигурност и онлайн услуги. Отговорили на анкетата и изпълнили казуса са 28 експерта.

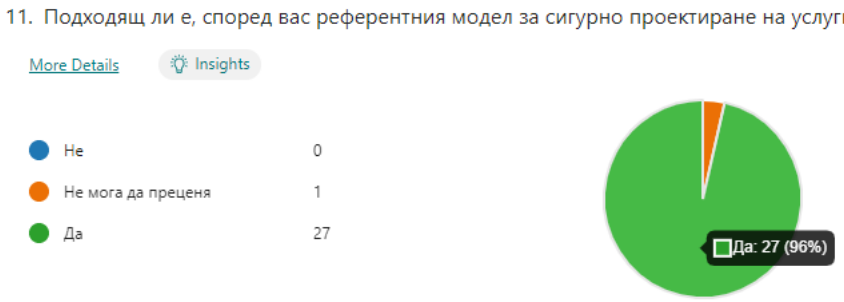
Заеманите длъжности на респондентите са в различни сфери на ИТ. В анкетата са включени мениджъри на отдели и ръководители екипи, свързани с управлението на ИТ и киберсигурността, мрежови инженери, отговарящи за конфигурирането и управлението на защитни стени, експерти по проектиране и програмиране на софтуерни приложения, графични дизайнери, експерти по уеб оптимизация, тестьори на софтуер, мрежови и системни администратори, както и професори, доценти и пост докторанти от университети, работещи в сферата на киберсигурността.

На въпросът „Прилага ли вашата организацията сертифициран подход за управление на информационната сигурност?“ 75% са отговорили „Да“, а 21% са отговорили „Не“. Близки по стойност са и отговорите на въпроса „Съществува ли политика за използването на криптографска защита на критична информация?“ Това е така, защото голяма част от респондентите работят в големи корпорации и банковият сектор, където управлението на ИТ и киберсигурността е базирано на стандарти.

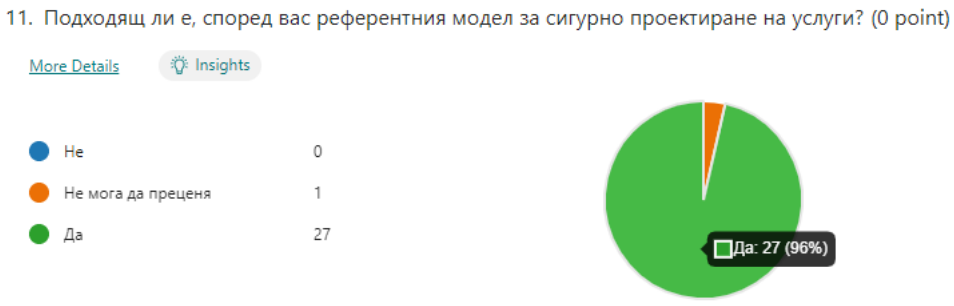
От анкетата става ясно, че служителите, работещи в големи организации, задължително преминават обучение по киберсигурност, което е обвързано с политиките за информационна сигурност. На въпроса „Служителите преминават ли обучение по осведоменост за киберсигурност?“ 71% са отговорили „Да“, 4% „Не мога да преценя“ и 25% „Не“.

На въпросите, свързани с разработването на собствен софтуер, информационни системи и услуги и политиките, налагащи прилагането и оценката на контроли за киберсигурност, отговорите са близки по стойност, като 75% са отговорили „Да“, 7% „Не мога да преценя“ и 18% „Не“.

Подходящ ли е според вас референтния модел за сигурно проектиране на услуги? 96% са отговорили „Да, и само 4% са отговорили „Не мога да преценя“. 64% са споделили, че според тях той обхваща всички области на киберсигурност, което е показано на



Фигура 8.



Фигура 8. Екранна снимка 2 от анкетата към референтния модел

Въпросът „Бихте ли използвали контроли от различни стандартизирани подходи при проектирането на една онлайн услуга?“ е изключително важен, защото той дава информация от какъв тип са услугите в организацията и има ли работещ каталог на услугите. На този въпрос 61% са отговорили „Да“ и 36% „Не мога да преценя“.

Анализирайки отговорите и коментарите към анкетата и казуса може да заключим, че предлаганият референтен модел разглежда проблемите, свързани с киберсигурността в дълбочина и гарантира сигурността на класифицираната информация, свързана с дейността на съответното ВУ. Респондентите са единодушни, че предложеният референтен модел е добре структуриран, логически свързан и предлага гъвкав подход. Някой от тях изтъкват, че референтния модел дава възможност за избор на контроли за сигурност между стандартите и дава решение на множество предизвикателства и проблеми пред ВО. Малка част от анкетираните са изразили мнение, че модела е твърде подробен и използването на различни подходи за киберсигурност би объркало служителите.

Казусът, който респондентите трябваше да разработят е свързан с работа със софтуерното приложение и изисква създаването на нова онлайн услуга, като се премине през всички процедури на работа с референтния модел описани в раздел 3.3.

Изпълнението на казуса обхваща координация на проектирането на услуга, избор на информационни системи, с които работи, класификация на услугата, преглед на областите на киберсигурност, избор на стандарти и контроли за сигурност, които да бъдат приложени. Препоръките за подобряването на референтния модел след изпълнението на казуса включват към потребителският интерфейс на софтуерното приложение да бъдат добавени повече бутони и падащи менюта, показващи вътрешното съдържание. Друго предложение е свързано с нови функционалности и филтри, които да улеснят работата с референтния модел – филтър за критичност на услугата, статус на услугата, както и добавяне на ролите и отговорностите на хората, свързани с проектирането и управлението на дадена онлайн услуга.

Изводи

В Глава четвърта е верифициран и валидиран на референтния модел. Апробацията на модела е направена посредством софтуерно приложение, базирано на система за управление на съдържанието достъпно на адрес www.csservices.online. Функционалните възможности на платформата са свързани със следните области: администриране, управление на съдържанието, каталог на услуги, известия / коментари, проследяване и отчитане.

Платформата дава възможност да се създадат множество администраторски роли с различни права на достъп. Предимства са добавянето на неограничен брой услуги, създаване на връзки към избрана категория или по категория, статус на услугата, сходни или свързани услуги и др.

Специфична функционалност е добавяне на групи атрибути и атрибути към група. Групите атрибути са използвани за въвеждането на използваните стандарти, а атрибутите към всяка група за въвеждане на контроли за киберсигурност от съответният стандарт. Създадена е и възможност за филтриране и сортиране на услугите по специфични функции (напр. критичност на услуга).

Сайтът има адаптивен дизайн, показващ съдържанието в различни размери на екрана (напр. мобилни устройства и таблети).

Направената верификацията показва, че техническо задание и програмния код, създадени в хода на разработката съответстват на добрите практики в ИТ.

С цел да се валидира предложения модел и да бъдат установени възможностите за усъвършенстването му е направено проучване базирано на експертно мнение на хора от ИТ сектора. Валидирането показва, че приложените контроли за кибер сигурност към дадена услуга, не противоречат на класификацията на този тип услуга.

Предложеният модел ще бъде полезен, защото ВУ предлагат множество онлайн услуги, част от които са свързани с основните университетски дейности. Проектирането на сигурни онлайн услуги е свързано с прилагането на защитени базови конфигурации, строги контроли за сигурност, както и надеждна мрежова инфраструктура.

ЗАКЛЮЧЕНИЕ

Актуалността на избрания за разработване и изследване проблем е определена от необходимостта за дигитална трансформация и управление на ИТ във висшето образование. Настоящото изследване е свързано с липсата на единни подходи за управление на ИТ, сложната структура на университетите, високите изисквания към тях и бързо променящата се среда. Управлението на ИТ във висшите училища в България обхваща структури и процеси, роли и отговорности, ИТ политики, характеристики и специфични особености на съществуващите управленски модели, добри практики за управление на ИТ.

Разработваният референтен модел е специфичен за българското висше образование и се основава на стандарти на ИТ услуги като отчита, особеностите на организацията на висшите училища. Внедряването му трябва да доведе до подобряване и модернизация на процесите, повишаване на зрелостта на организацията, постигане на стратегическите цели и задачи на институцията, добавянето на стойност и придобиване на стратегически предимства, както и подходящи мениджърски практики и ефективно управление на информационните технологии.

Прилагането на комбинация от ITIL и COBIT, ще помогне за създаването на добър управленски модел за ИТ във висшите училища. COBIT, е фокусиран върху перспективата на одит и контрол, докато ITIL поема управлението на услугите. Двата подхода се допълват и могат да осигурят качество, надеждност, запазване на поверителността, целостта и достъпността на информацията в университетите. Целта на докторантурата е ясно дефинирана и има достатъчно широк спектър от възможности за реализация и развитие. Референтният модел трябва да спомогне за подобряване на комуникацията и обмена на информация между различните структурни звена, създаване на условия за бързо въвеждане на нови електронни процедури и услуги, дигитализация на научните изследвания, както и стандартизирани критерии за анализ и повишаване на сигурността на обмена на данни и информация.

Предлаганите за използване методи и стандарти имат повишена мащабируемост и проследимост по време на проектирането за киберсигурност на сложни, свързани в мрежа информационни системи.

Създаването на общ процес за управление на ИТ, който може да се използва при разработването на нови услуги би увеличило ефективността и би улеснило процеса на одит на услуги. Събирането на данни за киберсигурността е решаваща стъпка, която формира свързваща връзка между проблемите със сигурността в кибер инфраструктурата и съответните стъпки за решение, управлявани от данни в тази рамка.

IV. НАУЧНИ И НАУЧНО-ПРИЛОЖНИ ПРИНОСИ

Научни приноси

1. Модифицирана е методология за проектиране на онлайн услуги, която отговаря на стандартите и изискванията за киберсигурност. Предложените методи и средства за тяхното приложение предлагат повишена мащабируемост и проследимост по време на проектирането за киберсигурност на сложни, свързани в мрежа информационни системи.

Научно-приложни приноси

2. Идентифицирани са основните информационни системи използвани в организации от висшето образование и са структурирани от гледна точка на киберсигурността на предлаганите услуги. Предложена е класификация на информационните системи от гледна точка на рисковете за киберсигурността.
3. Разработен е референтен модел за киберсигурност при проектирането на онлайн услуги във висши учебни заведения в Република България. Моделът е разработен на базата на използването на стандарти за управление на ИТ и на киберсигурността.
4. Разработен е процес за проектиране на нови онлайн услуги, който включва всички дейности от проектирането до избора на контроли за кибер сигурност и позволява постигането на по-висока ефективност и разширява възможностите за контрол и одит на онлайн услугите.

Приложни приноси

5. Разработеният референтен модел е верифициран и валидиран, чрез създаване на онлайн приложение, даващо възможност за създаване на каталог на онлайн услуги с реферирани контроли за сигурност към всяка услуга, съгласно международно признатите стандарти в областта.

V. ПУБЛИКАЦИИ И НАУЧНО-ИЗСЛЕДОВАТЕЛСКИ ПРОЕКТИ

Публикации

1. Pavlova “Enhancing the Organisational Culture related to Cyber Security during the University Digital Transformation”, Second International Scientific Conference "Digital Transformation, Cyber Security and Resilience" (DIGILIENCE 2020), magazine Information&Security, vol.46, no.2 (2020): 239-249, https://doi.org/10.11610/isij.5006, ISSN 0861-5160 (print), ISSN 1314-2119 (online).
2. Pavlova “Increasing cybersecurity in the process of digitization in higher education institutions in Bulgaria”, 10th International Conference on application of information and communication technology and statistics in economy and education (ICAICTSEE 2020), november 27-28th, 2020, UNWE, Sofia, page 474-481, ISSN 2367-7635 (print), ISSN 2367-7643 (online).
3. Павлова „Инфраструктура и управление на достъпа до информационни ресурси в УНСС“, Доклади от десетата юбилейна международна научна конференция за докторанти и студенти „Инфраструктура: бизнес и комуникации“, стр. 33-43, 21 април 2021, УНСС.
4. Павлова „Предизвикателства за киберсигурността при използването на лични устройства в УНСС“, 2021, Научни трудове на УНСС, ISSN 2534-8957 (online).
5. Pavlova “Implementation of Federated Cyber Ranges in Higher Education in Bulgaria: Challenges, Requirements and Opportunities”, Third International Scientific Conference "Digital Transformation, Cyber Security and Resilience" (DIGILIENCE 2021), magazine Information&Security, vol.50, no.2 (2021): 149-159, https://doi.org/10.11610/isij.5006, ISSN 0861-5160 (print), ISSN 1314-2119 (online)
6. Павлова „Икономически аспекти на киберсигурността във висшите училища“. Участие в конференция „Икономически предизвикателства: криза, възстановяване, устойчивост“, 19 ноември 2021, УНСС.
7. Pavlova “Reference model for cybersecurity in the design of online services in higher education institutions in Bulgaria”, 11th International Conference on application of information and communication technology and statistics in economy and education (ICAICTSEE 2021), November 25-26th, 2021, UNWE, Sofia.
8. Павлова "Осведоменост и обучение по киберсигурност във университетите в България. Съответствие с ISO 27001", конференция „Икономически предизвикателства 2022“, 17 юни 2022, УНСС.

Участие в научно-изследователски проекти

- 2021, НИД НИ: Изисквания и концептуален модел за създаване на лаборатория

за обучение в ОКС „Магисър“ по киберсигурност в УНСС

- 2022, НИП Fulbright Poland: Изграждане на киберклиника в УНСС

- 2023, НИП по програма "Хоризонт- Европа": Създаване на прототип на система за автентификация на потребители на защитени информационни системи, базирана на мозъчно-компютърен интерфейс

- 2023, НИП по програма "Хоризонт- Европа": Изграждане на база данни и разработване на специализиран софтуер за автоматизирана обработка и анализ на Big data за осигуряване функционалността на Национален ситуационен център (НСЦ) и Център за управление на кризи (ЦУК)

UNIVERSITY OF NATIONAL AND WORLD ECONOMY

Faculty of Infrastructure Economics

Department of "National and Regional Security"

Eng. Elitsa Georgieva Pavlova

"REFERENCE MODEL FOR CYBERSECURITY IN THE DESIGN OF ONLINE SERVICES IN HIGHER EDUCATION INSTITUTIONS IN BULGARIA"

ABSTRACT

of a dissertation work for the educational and scientific degree "doctor"

by professional direction 3.8. Economics scientific specialty "Economics and Management" (Economics of Defense and Security)

Research supervisor: Assoc. Dr. Georgi Penchev

Reviewers: Prof. Dr. Dimitar Velev

Assoc. Dr. Rosen Kirilov

Sofia, 2023

The dissertation was discussed and referred for defense by the Department of "National and Regional Security" at the Faculty of "Infrastructure Economics" at UNWE at a meeting held on 28.02.2023.

The work consists of 137 pages of main text. It consists of an introduction, an exposition in four chapters, a conclusion, a list of references, 18 tables, 32 figures, 18 appendices (70 pages).

The literature used contains 60 titles in Bulgarian and English, including normative documents and official sources, books, monographs, articles in scientific and periodicals, reports and analyzes of international organizations, as well as electronic sources with specific information.

The public defense of the dissertation work will take place on 02.05.2023
from 10:00 a.m., in the Hall of Scientific Councils of UNWE.

The defense materials are available in the "Scientific Councils and Competitions" sector at the "Science" Directorate and on the UNWE website www.unwe.bg.

TABLE OF CONTENTS OF THE AUTHOR REFERENCE

I. GENERAL CHARACTERISTICS OF THE DISSERTATION

Digital transformation (DT) in higher education institutions (HEIs) and research organizations is related to the use of information technology, organizational structure and processes that provide the link between the university's goals and its IT policy. Universities are adopting a host of new technologies and teaching methods, using various distance learning applications and portals needed to support an online or blended learning environment.

The growing combination of new challenges and risks in the sector make cyber security a strategic priority to protect information assets, and DT a critical necessity.

The relevance of the problem is related to the need for structured security management in the design of new electronic procedures and services in HE.

In the process of DT, universities increase the online services they offer and with them the risks of cyber attacks increase. This will require new standards and infrastructure for digital learning, as well as additional legislation that ensures secure online services on the one hand and encourages innovation on the other. During DT, online services and the processes related to their design change at the same time, which makes it imperative to review information security strategies and policies. The transition to a virtual and cloud architecture poses a number of questions related to the cybersecurity of stored data.

That is why the development and implementation of a cybersecurity model in the design of online services in higher education (HE) will help to ensure effective and continuous management of all important administrative and learning processes.

The research problem of the dissertation is the identified lack of a model for cyber security in higher education covering the stages of designing online services, which would increase the quality of education, and would help to identify the main directions for increasing information and cyber security. The problem is related to the management of online services and cyber security, as well as the complex structure of universities, the high demands on them and the rapidly changing IT environment.

In the process of DT, universities increase the online services they offer and with them the risks of cyber attacks increase. This will require new standards and infrastructure for digital learning, as well as additional legislation that ensures secure online services on the one hand and encourages innovation on the other. During DT, online services and the processes related to their design change at the same time, which makes it imperative to review information security strategies and policies. The transition to a virtual and cloud architecture poses a number of questions related to the cybersecurity of stored data.

That is why the development and implementation of a cybersecurity model in the design of online services in higher education (HE) will help to ensure effective and continuous management of all important administrative and learning processes.

The research problem of the dissertation is the identified lack of a model for cyber security in higher education covering the stages of designing online services, which would increase the quality of education, and would help to identify the main directions for increasing information and cyber security. The problem is related to the management of online services and cyber security, as well as the complex structure of universities, the high demands on them and the rapidly changing IT environment.

The following tasks have been defined for the implementation of the set goal:

1. To analyze the activities and processes of higher education institutions in the field of IT technologies and online services, to identify the main characteristics related to cyber security management.

2. Based on a review of the literature dedicated to cyber security management, to identify successful solutions and good practices for designing secure online services.

3. To create a reference model for cyber security and standardization of online service management processes in higher education institutions in Bulgaria.

4. The model should be verified and validated through document analysis and interviews with experts. The reference model to be implemented by creating an online application.

In order to establish the state of cyber security management, a review was made of the websites of the leading universities in Bulgaria and the world.

Data and research related to cyber security in higher education in the European Union (EU) were used. Relevant literature related to general cyber security, best practices and cyber security frameworks are reviewed. The research includes interviews, document analysis and expert opinion for verification and validation of the reference model.

The methods used in the dissertation include document and comparative analysis, as well as the application of international approaches and standards for IT management, information security and cyber security: the Framework for Controlling Information and Related Technologies (COBIT 2019), the IT Infrastructure Library (ITIL) is an approach describing best practices for IT service management, the Information Security Management Standard (ISO/IEC 27001:2022), the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), and the Controls for Effective Cybersecurity (CIS CSC).

The research is limited to the design stage of new online services, without going into details of the stages of their implementation and improvement.

Users of the results of the dissertation can be the Ministry of e-Government and the Ministry of Education and Science of the Republic of Bulgaria, all higher education institutions, as well as researchers, students and the public in general.

Unclassified sources of data and information were used - monographs, textbooks, scientific publications, articles and data from the Internet.

The dissertation covers four chapters:

In *Chapter one*, the state and problems in the management of cyber security of higher education institutions in Bulgaria are analyzed. The concepts needed for the study are clarified. The main stages of DT have been identified and the regulatory framework of the EU and Bulgaria has been reviewed. The foreign experience in the field of cyber security in higher education institutions was analyzed.

In *Chapter two*, the approaches and standards for managing information technology and cyber security in HE are analyzed. The most commonly used reference models for IT service management and cybersecurity are presented. Their main characteristics and possibilities for their use in the design of online services are identified. The requirements and limitations of the reference model are defined.

In *Chapter three*, the application of the methodology for developing the reference model is structured. A risk assessment was made according to the impact and probability of vulnerabilities of university systems and online services derived from them. Referenced security controls to model functions. The procedures for working with the reference model have been developed and the roles and responsibilities related to IT management in higher education institutions have been established.

In *Chapter Four*, the reference model is verified and validated. The model validation was done using a software application based on a content management system. In order to validate the proposed model and to establish the possibilities for its improvement, a study was conducted based on the expert opinion of people from the IT sector.

II. VOLUME AND STRUCTURE

The dissertation consists of 137 pages of main text. It consists of an introduction, an exposition in four chapters, a conclusion, a list of the literature used, 18 tables, 32 figures, 18 appendices.

The literature used contains 60 titles in Bulgarian and English, including normative documents and official sources, books, monographs, articles in scientific and periodicals, reports and analyzes of international organizations, as well as electronic sources with specific information.

The dissertation has the following structure:

List of abbreviations

Introduction

Chapter I. Status and problems in the management of cyber security of higher education institutions in Bulgaria

1.1. Basic concepts and stages of digital transformation. Cybersecurity regulatory framework

1.2. Study of foreign experience in the field of cyber security of higher education institutions

1.3. Challenges and problems in the field of cyber security for universities in Bulgaria

Conclusions to Chapter I

Chapter II. Approaches and Standards for Information Technology Management and Cybersecurity in Higher Education

2.1. Basic approaches. IT and Cybersecurity Management Framework

2.2. Benchmarking IT and Cybersecurity Management Approaches and Standards

2.3. Cybersecurity Management Reference Models. Requirements.

2.4. Identifying key features of a cyber security reference model for HEIs. Development methodology.

Conclusions to Chapter II

Chapter III. Application of the reference model development methodology
3.1. Data collection and analysis
3.2. Referencing security controls to model functions
3.3. Procedures in the reference model
Conclusions to Chapter III

Chapter IV. Reference model verification and validation
4.1. Choosing a platform for developing a test software application
4.2. Auditing and testing of the software application
4.3. Verification of the reference model
Conclusions to Chapter IV
Conclusion

References
List of tables
List of figures
List of applications

III. SYNTHESIZED STATEMENT

Chapter I. Status and problems in the management of cyber security of higher education institutions in Bulgaria

Universities in Bulgaria are at different stages of their digital transformation in relation to the available infrastructure and funds at their disposal. Digitization includes changing the schedule and conducting the study programs, changing the organizational structure, creating interactive content, transforming the university infrastructure. Achieving a successful DT is related to a consistent and purposeful policy for improving the services provided, building new structural units, linking the strategic goals of the university with the goals of IT development, awareness and staff training.

In Chapter I, the following set tasks are completed:

1. To analyze the activities and processes of higher education institutions in the field of IT technologies and online services.

2. To highlight the main characteristics of online services related to cyber security management.

Section 1.1 describes basic concepts and stages of digital transformation and the regulatory framework for cybersecurity. The approach used to analyze the main concepts and define them for the needs of the research is based on one of the most influential sources for international scientific citation Web of Science[36]. The terms used as search keywords in the

[36] Web of Science, "Web of Science," Webofscience.com, 2022, https://www.webofscience.com/wos/woscc/basic-search.

database were digital transformation, information security, cybersecurity, cybersecurity controls, and reference model.

These concepts are found in the titles of 463 scientific studies for the last three years, with the largest number of them in the category "Education" (45%), followed by "Governance" (8%) and "Economics" (7%) . Cybersecurity in HEIs has been investigated in 110 reports.

The most cited concepts necessary for the study are discussed below.

Digital transformation

One of the most popular concepts related to IT management is "digital transformation". It is important when changing the activities of organizations or when there is a significant change in technologies and their full implementation.

In the monograph "Digital Transformation in Higher Education", the authors describe digitization in five areas[37]: IT strategic planning, IT value addition, risk management, results measurement and IT resource management.

The concept of digital transformation in higher education institutions, for the purposes of the study, is defined as a series of deep and coordinated changes that enable new educational models and transform the activity of the institution using secure and fast access to information resources, applications and services at any time and from any device.

Information security

The report "Modern Security Assessment Toolkit" by Prof. Dr. Tsvetan Tsvetkov states that security assessment and the management process are connected and interdependent, and security issues affect the long-term prosperity of the organization and affect vital goals of the organization[38].

For the purposes of the study, information security is defined as the ability to protect the internal resources of a higher education institution from threats, and its management includes the protection of information assets through the application of policies, procedures, organizational structures, infrastructure and audits. The governance framework defines who is empowered to make decisions and how accountability for results will be established. Management processes ensure that all critical assets are protected and risks are adequately mitigated.

Cyber security

Cyber security is a component of information security and related to it are: IT protection measures; the degree of protection resulting from the application of these measures; data and information processed and transmitted; connected virtual and physical elements of the systems.

In the report "A training model in the field of cyber security" of Ch. Assistant Professor Nedko Tagarev said that the main goal of training in the field of cyber security is related to the establishment and improvement of programs for the protection of computer systems,

[37] Mark McCormack Christopher Brooks, "Defining Digital Transformation," Educause.edu, 2020, https://www.educause.edu/ecar/research-publications/driving-digital-transformation-in-higher-education/2020/defining-digital-transformation.

[38] Цветан Цветков, "Съвременен инструментариум за оценяване на сигурността," Journal Issues - Economic Alternatives, Unwe.bg, 2016, https://www.unwe.bg/alternativi/bg/journalissues/article/8948.

networks and other digital systems, which are of crucial importance in preventing theft, sabotage and other malicious acts.

For the purposes of the study, cybersecurity is defined as a set of practices and guidelines that are used to protect computer networks, software programs, and information assets from unauthorized access, resilience, and recovery from a cyber attack. Cybersecurity priorities are deterrence, prevention, detection and response.

Cyber Security Controls

Cybersecurity encompasses the controls that must be created and implemented to protect information stored in information systems.

For the purposes of the study, cybersecurity controls are defined as safeguards or countermeasures to avoid, detect, counter, or minimize cybersecurity risks - viruses, malware, cyber attacks, hackers, phishing attempts, and others.

Reference model

According to the Organization for the Advancement of Structured Information Standards, a reference model is "an abstract framework for understanding meaningful relationships between objects of a given environment, and for developing consistent standards or specifications supporting that environment . In other sources, a reference model is described as "a conceptual framework establishing a common language for communication and understanding of system elements and their meaningful relationships within a given community." [39]

For the purposes of the study, the concept of a reference model is defined as a conceptual framework establishing a common language between standardized approaches and good practices for cyber security that can be used in the daily work of HE sector organizations.

Stages of digital transformation

Creating a cyber security reference model for the design of online services in higher education requires clarification of the stages of IT. The Department of National and Regional Security's Corporate Security book says that IT includes the need to automate data security controls and develop a robust IT infrastructure[40].

The report "What Digital Transformation Means for Higher Education" identifies four main stages that universities must go through[41]. These are presented in Figure 1.

Figure 1. Stages of digital transformation in higher education

[39] "OASIS," Oasis open, 2022, https://www.oasis-open.org/.

[40] Атанас Димитров, Георги Павлов, Димитър Димитров, Екатерина Богомилова, Константин Пудин, Никола Иванов, Нончо Димитров, Теодора Гечкова, Тилчо Иванов, Цветан Цветков, Юри Ценков et al., "Корпоративна сигурност."

[41] Dania McDermott, "What Digital Transformation Means for Higher Education," Processmaker.com, 2020, https://www.processmaker.com/blog/what-digital-transformation-means-for-higher-education/.

1 Stabilization	2 Standardization	3 Optimization	4 Transformation
• Renewing the IT infrastructure • Network improvement • Identify security risks	• Audit of information systems and resources • IT management • enforcement of standards	• Automation of activities • process automation	• Data analysis • improving the quality of online services • Testing of new information systems

Source: Larissa Lewis, "Creating a Digital Transformation Roadmap," Processmaker.com, 2020, https://www.processmaker.com/blog/digital-transformation[42]

The stabilization phase includes renewing the IT infrastructure, improving the network, identifying security risks. During standardization, information systems and resources are audited, IT management and cyber security standards are implemented. Optimization includes automating all activities and processes. The transformation is related to data analysis, improving the quality of online services, as well as testing new information systems.

Regulatory framework for cyber security in the EU and Bulgaria

For the purposes of the study, the regulatory framework of the EU was analyzed and compared with the one in force in the Republic of Bulgaria.

The European Commission presented a program for Europe's digital future, which includes a Strategy for the Digital Future of the European Union, a White Paper on the Development of Artificial Intelligence and a Strategy for the Creation of a Digital Single Market and others.

An EU cybersecurity strategy aims to strengthen Europe's resilience against cyber threats and ensure that all citizens and institutions can benefit from reliable services.

In December 2020, the European Commission adopted a directive on the cybersecurity of networks and information systems, in response to the dynamically changing digital transformation. It says that the content of education systems should be in line with the regulatory documents of the Member States, as is the sharing of good practices in the field of digital education. In order to assess to what extent the regulatory framework for higher education in Bulgaria is suitable for the transition to the digital era, basic normative documents related to IT and cyber security in higher education institutions have been identified.

The Council and the European Parliament agreed on measures for a high common level of cybersecurity across the Union to further improve the resilience and incident response capacity of both the public and private sectors and the EU as a whole.

The aim of the new directive, called 'NIS2', is to remove differences in cybersecurity requirements and the implementation of cybersecurity measures across Member States[43].

[42] Larissa Lewis, "Creating a Digital Transformation Roadmap," Processmaker.com, 2020, https://www.processmaker.com/blog/digital-transformation/.

[43] NIS, "NIS 2 Directive," Nis-2-directive.com, 2022, https://www.nis-2-directive.com/.

EU regulatory documents:

• EU Cyber Security Strategy 2020-2025;

• EU Digital Education Action Plan 2021-2027;

• Provision for a culture of cyber security in the organizations of the EU Cyber Security Agency (ENISA) [44].

The improvement of the university culture, through the "Cybersecurity Policies" methodology of the European Union Agency for Cybersecurity, is key to all stages of DT. Policies cover the creation of programs focused on specific activities, their implementation and the measurement of their impact. The large number of students, faculty and staff, varying levels of IT competence, and complex network connectivity of all devices make creating and managing cybersecurity extremely complex.

Bulgaria participates in all EU initiatives, including the "Horizon Europe" and "Digital Europe" programs, and Bulgarian normative documents related to digitization in higher education institutions and cyber security are discussed below.

Normative documents of Bulgaria:

• Strategy for the development of higher education in Bulgaria (2021-2030) [45];

• Strategy for effective application of information and communication technologies in education and science in Bulgaria (2014-2020);

• The National Development Program "Bulgaria 2030";

• The National Program "Digital Bulgaria 2025";

• National Strategy "Cyber Sustainable Bulgaria 2020".

Normative documents support the problems and challenges in the field of cyber security of higher education institutions. Their main objectives are to raise awareness and competences, develop a stimulating environment for research, access to data, information and knowledge. The application of DT in education will ensure accessibility, relevance and management of educational resources, which are the basis of quality education.

The main challenge for universities is to achieve higher general levels of security in the use and maintenance of information systems for access control and information. Higher education policies do not directly affect innovation, but they do have a link with the drivers of innovation, according to a study carried out in EU universities[46]. Key factors for the development of innovation can be the general regulatory framework, the existence of accumulated knowledge, research and development, factors specific to a certain market or product, such as the level of demand and cost structure, the type of government, social infrastructure, the existence of property rights, government consumption, international openness, inflation, etc.

In section 1.2, a study of foreign experience in the field of higher education cyber security is made. The data collection method involved a detailed search of the websites of universities around the world.

---

[44] ENISA Europa, "Cyber Security Culture in Organisations," 2020, https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport.

[45] Strategy.bg, "Стратегията За Развитие На Висшето Образование в Република България (2019 – 2030)," 2020, http://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=962.

[46] Roger G. Baldwin, "Technology in Higher Education," Education.stateuniversity.com, 2021, https://education.stateuniversity.com/pages/2496/Technology-in-Education-HIGHER-EDUCATION.html.

The practices of 17 universities were compared, seven from Bulgaria (Sofia University, UNSS, University of Economics - Varna, Higher Transport School "Todor Kableshkov", American University in Bulgaria - Blagoevgrad, New Bulgarian University, Varna Free University "Chernorizets Hrabar") and ten the leading European, British and American universities (Vienna, Ljubljana, Stanford, Oxford, Harvard, Graz, Mazarik, Berlin, Thessaloniki).

Universities provide many online services such as application and semester exams, web student, e-libraries, faculty portal, etc. Priority areas are database administration and maintenance, existing online learning applications and systems, updating the university website, network connectivity, end-user support activities, etc.

Indicators related to cyber security and providing information on the number of domains, sub-domains, information systems, online services offered and information security policies were sought.

The sites were scanned using the online platform Urlscan (www.urlscan.io). The scanning method is based on an automated process to scan the Internet address and record the activity that page navigation creates.

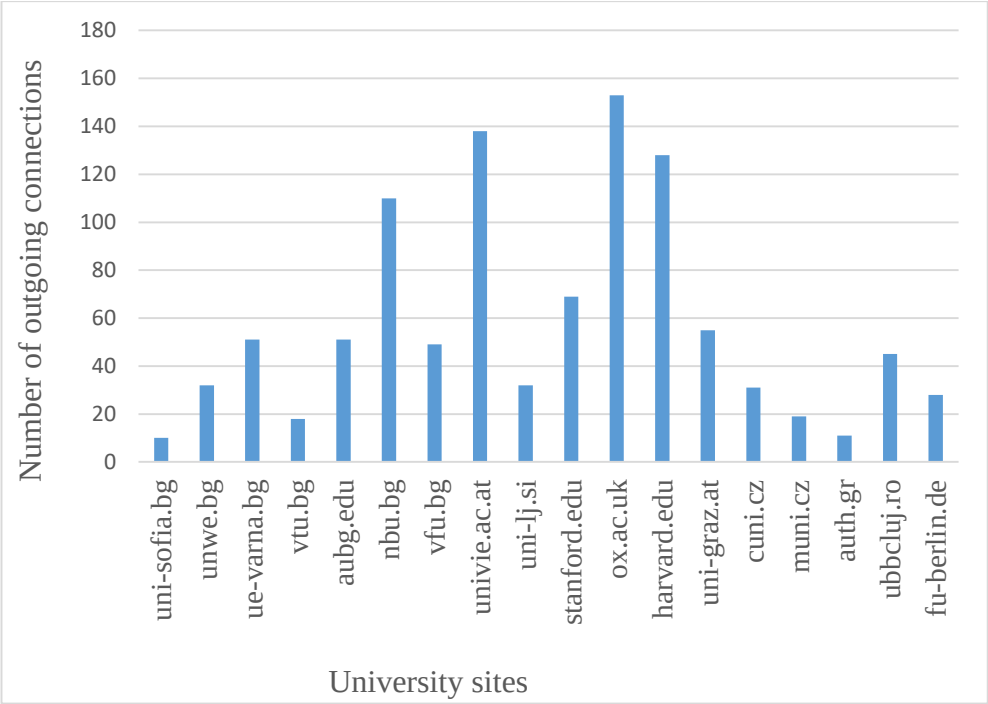
The analysis includes the comparison of the following indicators: popularity (rank); global rank; requests show the total number of transfers coming from other domains; HTTPS protocol; under domains that operate as stand-alone websites; IP addresses (IPv6, IPsec); the outgoing number of connections; site size; X-XSS-Protection; Strict-Transport-Security; X-Frame-Options; X-Content-Type-Options; X-Xss-Protection; Content-Security-Policy as well as additional information about the page itself.

The analysis shows that the considered universities in Bulgaria have approximately the same Google rank of 4 or 5, while for universities in the world it varies from 6 to 8. The use of the HTTPS protocol in international universities is slightly higher than in Bulgaria and guarantees , that transactions are kept confidential and every packet of data is encrypted and secure. The number of domains, subdomains and the number of outbound links provide information about the connected web pages and the online services provided. The University of Vienna, Oxford and Harvard have over 120 outgoing links. It is noteworthy that for most universities the use of IPv6 is around 80%.

On university sites, outbound links often lead to subdomains of the main site and represent online services offered. The large number of subdomains indicates that university sites are built as portals and lead to various subsites on the Internet or Intranet.

Figure 2 presents a graph of outbound links in the analyzed university sites. Their number varies in a very wide range from 43 to 178. Sofia University has the least number of outbound links 10, while New Bulgarian University has more than 100. The sites of Varna University of Economics and American University have the same number of 50. The site of the university in Stanford, which always ranks highest, has just 69 outbound links, compared to the universities of Vienna, Oxford and Harvard, which have more than 120 outbound links.

Figure 2. Outbound links in university sites in Bulgaria and the world



Source: Own research

The analysis provided provides insight into organizational structures, content, connectivity to social networks and platforms, number of visits, information systems, mobile applications, IT department structure, cyber security strategy and policies, information update and other parameters directly dependent on IT management in the university. The analysis shows that there are many areas that need to be investigated and improved in Bulgarian universities. Readiness to change and implement innovations is directly related to the number and types of IT services provided.

Based on the studies, four main groups of information systems have been identified: Administrative, Information, Educational and Science.

In the study "Cybersecurity Threats 2022" the most common vulnerabilities in online services are presented[47]. It shows that large-scale data mining is a major security threat. The ease with which data can be collected and aggregated makes this attack widespread.

The report "Digital Transformation in Higher Education" describes the problems faced by higher education institutions[48]. Most universities declare as difficulties the lack of funds for the investment in new technologies, the slow changing organizational culture, the insecure internet infrastructure, the insufficient readiness for training in cyber security and qualified IT staff. Higher education institutions use technologically outdated information systems that are not properly secured and must adapt them to the changing needs of students and regulatory regulations.

The study of foreign experience shows that the modern university is oriented towards internationalization, competitiveness and innovation. Priority topics are digital transformation, cyber security, as well as the legal framework related to them. A solution

[47] Ptsecurity, "Cybersecurity Threatscape: Q2 2022," 2022, https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2022-q2/.

[48] Lina María Castro Benavides et al., "Digital Transformation in Higher Education Institutions: A Systematic Literature Review," *Sensors* 20, no. 11 (January 2020): 3291, https://doi.org/10.3390/s20113291.

based on the analysis made involves the application of a standardized approach in the design of online services in higher education institutions, because dealing with existing vulnerabilities and their elimination in real time can be difficult.

Section 1.3 analyzes the challenges and problems in the field of cyber security for universities in Bulgaria.

Universities often take a reactive approach to cyber security, taking action only when an attack occurs. A cybersecurity study shows that in 2021, higher education institutions are modernizing the security tools of existing IT systems by marking compliance checklist items instead of building cybersecurity into their new systems and services[49]. The reliability of network and information systems is key to the smooth functioning of all platforms and university sites, conducting candidate student campaigns, electronic exams, enrollments, training, etc.

A query in the World Higher Education Database shows that 63% of universities manage the enrollment and storage of student data entirely online[50].

The International Association of Universities emphasizes that there is no single model for digital transformation that fits all higher education institutions. The brief provides an overview of national strategies and policies for the use of new technologies in teaching and learning. Application architecture includes implementing user-centered design, information systems reengineering, single sign-on, digital workplace, and enabling internal process evaluation and service improvement.

New cybersecurity trends include risk-based security strategy development, cloud infrastructure and high-speed networks, defined cybersecurity processes, cyber attack detection and response systems, and more.

The currently effective regulatory framework in the field of ICT in Bulgaria covers: Law on Electronic Communications; Cyber Security Act; Law on Electronic Communications Networks and Physical Infrastructure; e-Governance Act; Law on electronic signature and electronic authentication services; Cyber Security Act; Trade Register Law; Electronic Commerce Act; Personal Data Protection Act and other regulations.

The national program "Digital Bulgaria" aims to harmonize Bulgarian legislation in accordance with that of the EU within the framework of the Digital Single Market Strategy in Europe. The aim of the European Commission is to support Member States in identifying areas requiring priority action, one of which is that by 2030 at least 80% of citizens have basic digital skills.

The data in the Ranking System of Higher Schools in Bulgaria (RSVU) for 2021 shows an increase in the number of students and the number of scientific publications in international bibliographic databases.

The main challenges described in the "Universities in a Digital World" study are[51]:

[49] Dave Burg, Mike Mason, and Richard Watson, "Cybersecurity: How Do You Rise above the Waves of a Perfect Storm?," EY, 2021, https://www.ey.com/en_bg/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm.

[50] WHED, „World Higher Education Database".

[51] Link Springer, "A University Landscape for the Digital World," Link Springer, 2022, https://link.springer.com/chapter/10.1007%2F978-3-030-44897-4_1.

• A high degree of age differentiation regarding the possibilities of working with digital technologies.

• Reforming HE aimed at combining written-auditory information with visual information.

• Lack of strategic visions regarding the main functions of universities related to training, the development of science and innovation.

• Achieving a balance between increasing societal demands and expectations for higher education.

• Insufficient competitiveness in relation to the rapid development of the educational services market and lack of flexibility in the offered forms of education.

The challenges facing HE in Bulgaria are related to the need for a comprehensive digitization model to assess the degree of digitization of each higher education institution, as well as uniform user authentication for access to all platforms.

Cybersecurity in HEIs is ensured through processes that management follows to identify, analyze and respond appropriately to risks that may adversely affect the organization. During the "Digitalization of Higher Education in Bulgaria" conference, which took place this year at UNSS, possible threats, risk assessment and ways to counter them were discussed. It said that universities are vulnerable to cyber-attacks due to their decentralized structure, diverse group of users (researchers, students, PhD students, teachers, staff and others), different levels of IT competence and complex network connectivity of all devices. The focus is on people and opportunities to train them to reduce vulnerability to cyber attacks, loss of data or reputation.

Bulgaria participates in several large international projects, one of which is the "European Universities" network. In it, digitization is a top priority, which is precisely why a number of technology companies partner with Bulgarian universities to ensure their information security and cyber security.

A 2021 software security report notes that more than 85% of web applications have security vulnerabilities[52]. Understanding these vulnerabilities is key to detecting them and protecting data. Standardization and certification of activities related to cyber security are not sufficiently adapted to the modern needs of HE. ENISA's key messages to organizations in this regard include more security awareness and education at all levels, risk management, collaboration with academia to ensure that research leads to quality products and services.

One possible strategy for countering cybersecurity risks is employee training. "Training should be ongoing and the content updated regularly, covering emerging security threats and the security controls that are implemented to protect information," says the article "What is security training and why is it important"[53].

Universities should develop the awareness programs according to the different roles of the employees in the organization. The program should include various forms of training – newsletters, computer-based security training, simulated phishing exercises, cyber security alerts and tips.

[52] Veracode, “State of Software Security,” Veracode, 2021, https://www.veracode.com/state-of-software-security-report.

[53] Mimecast, “What Is Security Awareness Training and Why Is It Important?,” Mimecast, 2022, https://www.mimecast.com/content/what-is-security-awareness-training/.

Conclusions

In Chapter one, the state and problems in the management of cyber security of higher education institutions in Bulgaria are analyzed.

The concepts necessary for the study are clarified: digital transformation, cyber security, security controls, reference model.

The main stages of DT have been identified and the regulatory framework of the EU and Bulgaria has been reviewed. Foreign experience in the field of cyber security has been analyzed and it has been established that universities in Bulgaria need a comprehensive model for cyber security in the design of online services, such as is already operating in many other EU universities.

Chapter II. Approaches and Standards for Information Technology Management and Cybersecurity in Higher Education

In Chapter II, the following set tasks are completed:

1. Based on a review of the literature dedicated to cyber security management, to identify successful solutions and good practices for designing secure online services.

In section 2.1 of this chapter, major approaches and frameworks for managing IT and cyber security are discussed for the purposes of the study.

The complete list with a description and purpose of each standard and approach is presented in Appendix 8. Most of them are successfully used in higher education institutions around the world and are therefore discussed in more detail.

COBIT 2019 approach to information technology management. General framework

The common framework for managing information technology in the organization is accepted as a standard (COBIT 2019[54]) and was developed by the Association for Auditing and Control of Information Systems. The framework is globally recognized and used by over 188 countries and has over 200,000 recognized certificates. Key principles in COBIT 2019 are stakeholder needs and business value creation through the use of IT. COBIT 2019 maintains a high level of compliance and includes parts of other information security standards, by clearly distinguishing between the levels of strategic management and operational management (management).

The approach offers a common framework, including several standards, linking the goals of management in general and the goals of IT management.

Basic steps in using the approach are: defining the object area; defining design factors; cascading goals; prioritization of governance and management objectives; establishing the added value.

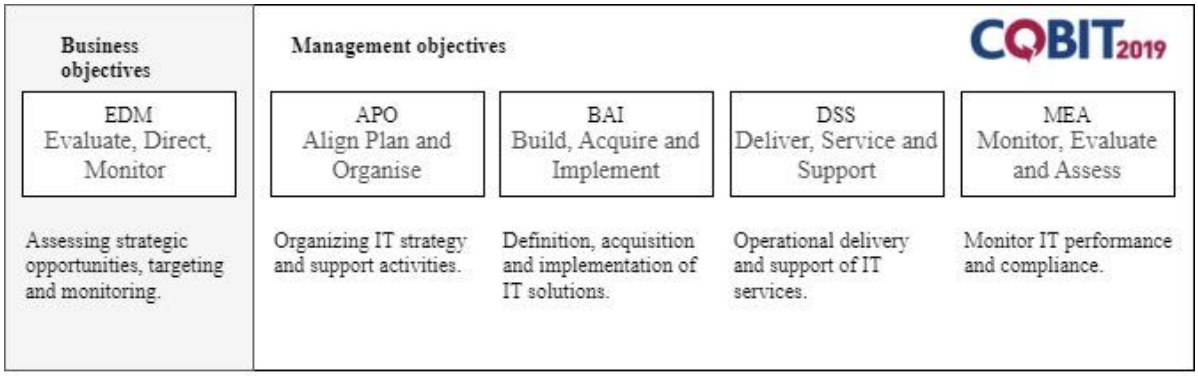
Goal cascading supports the prioritization of management goals based on the organization's goal prioritization. These include a customer-oriented service culture,

[54] ISACA, „COBIT | Control Objectives for Information Technologies“, isaca.org, 2022, https://www.isaca.org/resources/cobit.

optimization of internal business process functionality, achievement of service operational excellence, business risk management.

A graphical description of the approach can be seen in Figure 3.

Figure 3. Core processes of the COBIT 2019 approach



Source: IEA, 2022, Enterprise Architecture publication, iea.wikidot.com/cobit

The main elements in COBIT 2019 are areas, objectives and performance indicators. The domains follow the common development life cycle of the systems. Management objectives describe the practical goals for managing IT processes. Performance indicators describe activity.

The RACI[55] matrix allows to identify the roles and responsibilities directly related to the organizational structure in the management of cyber security and will be discussed in detail in Chapter 3, Section 3.3.

The four areas that follow the general life cycle of systems development are[56]: Binding, Planning and Organizing (BPO); Construction, Acquisition and Implementation (CAI); Delivery, Service and Support (SS); Monitoring, Evaluation and Analysis (MEA). A detailed description of the processes and related framework elements in the areas of Planning and Organization and Acquisition and Implementation can be found in *Appendix 9*.

For each management objective, COBIT 2019 identifies the components that must be scaled, maintained and satisfied to achieve each objective and they are:

- processes
- organizational structures;
- information flows and elements;
- people, skills and competencies;
- policies and procedures;
- culture, ethics and behavior;
- services, infrastructure and applications.

The objectives of strategic and operational management are divided into areas in which good practices are developed so that the governing body can assess the available strategic

[55] RACI - Responsible, Accountable, Consulted, Informed

[56] Coursehero, „COBIT has several strengths that make it a worthy framework for IT“, www.coursehero.com, 2021, https://www.coursehero.com/file/p4pvm3s/COBIT-COBIT-has-several-strengths-that-make-it-a-worthy-framework-for-IT/.

options, direct the organization to strategic goals and monitor the implementation of the strategic plan.

COBIT 2019 enables the achievement of organizational goals by balancing and targeting risk and control measures. Its implementation will reduce security risk, data management, improve IT services and access for all stakeholders.

Standard ISO/IEC 27001:2022 information security management system. General framework.

The standard is mandatory in Bulgaria, and its implementation is conditioned by the Ordinance on the general requirements for interoperability and information security, issued on the basis of Art. 43, para. 2 of the Law on Electronic Government. State, territorial and local administrations, the judiciary, persons performing public functions, as well as organizations providing public services, such as educational institutions, must be certified according to it.

The standard covers the following areas of information security: Risk assessment for information security; Security of human resources; Physical security; Computer and network security; Security in software and hardware development; Incident Management; Continuity management.

ISO/IEC 27001:2022 has 93 controls structured into four control groups: A.5 Organizational controls - contains 37 controls; A.6 Human Controls - contains 8 controls; A.7 Physical controls - contains 14 controls; A.8 Technological controls - contains 34 controls.

The following 11 new controls have been added to Appendix A:

- Threat intelligence
- Information security when using cloud services
- ICT readiness for business continuity
- Physical security monitoring
- Configuration management
- Delete information
- Data masking
- Prevent data leakage
- Monitoring activities
- Web filtering
- Secure encryption

The management system-oriented requirements section of Annex A of the ISO/IEC 27001:2022 standard contains a list of 35 controls with 114 specific security measures.

The controls describe what a standard-compliant measurement result should look like and are presented in Appendix 11.

The main advantage of implementing the ISO/IEC 27001:2022 standard is that it is applicable to all types of organizations and ensures that information security is managed effectively and efficiently. Defines and evaluates information security management processes while ensuring process continuity across all business lines. Its implementation takes time and all its recommendations and policies must be implemented. The standard uses a risk-based approach and this requires organizations to identify information security risks and select appropriate controls to address them.

ITIL IT Infrastructure Library. General framework.

The IT Infrastructure Library (ITIL) is an approach describing best practices for managing IT services. The main focus of ITIL is the definition of functional, operational and organizational attributes. These are divided into two key categories – Service Support Management and Service Delivery Management, each with a number of supporting sub-categories.

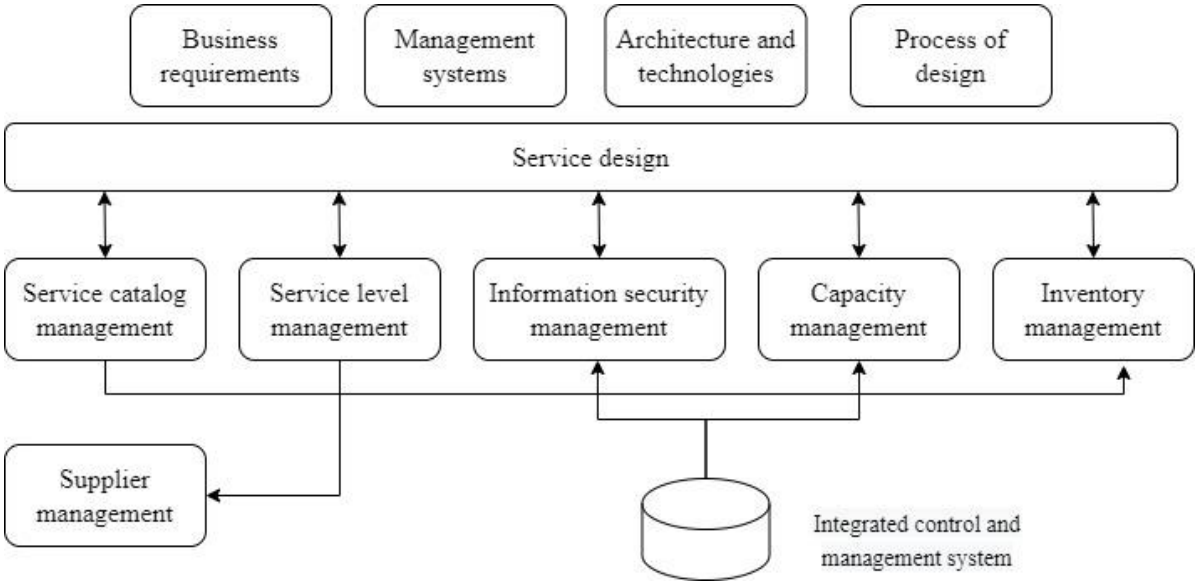
The IT infrastructure library is widely used because it focuses on continuous improvement of quality, efficiency and provides a complete life cycle of IT services. The project service process includes the guidelines for the design and development of services and processes related to IT management.

Service design will be discussed in detail because it is an important part of designing online services. This process includes service catalog management; availability; capacity; duration; security; providers.

The library offers guidelines for the development and improvement of the transition period, turning the processes into standardized documented operations. Transition to services lists the requirements of the service strategy, analyzes the design of services and controls the risks of failure. Service operation contains the practices of serving the objectives and support to ensure the value of these services.

For the purpose of uniform application of cybersecurity requirements, it is proposed to group ITIL services so that in one group are services with similar baseline design configurations and cybersecurity requirements.

Figure 4 shows the service design process in ITIL.



Source: Tutorialspoint, ITIL - Service Design Overview, 2021, www.tutorialspoint.com/itil/service_design_overview.htm

Service design includes: general part, requirements, concepts for service operation and improvement, technical and organizational plan for new service implementation and transition planning. All stages, elements and their description are presented in Appendix 10.

Advantages of the approach are improved quality of IT services, a comprehensive view of the delivery of products and services, demand management and increased customer

satisfaction, reduced risk of non-compliance with business requirements, as well as reduced costs in developing procedures and practices. The creation of a catalog of services is directly related to the tasks of the study.

National Institute of Standards and Technology NIST CSF Cybersecurity Framework. General framework.

The Cyber Security Framework (NIST CSF) [57] does not introduce new standards or concepts, but rather integrates best practices in cybersecurity that have been developed by organizations such as the US National Institute of Standards and Technology and the International Organization for Standardization. It has been successfully implemented in smaller organizations and is used as a security reporting tool for management.

The framework's five functions are: Identify, Detect, Protect, Respond and Recover, which provide a risk management lifecycle strategy, opportunities to improve cybersecurity and communication.

"Identification" includes asset management; business environment; management; Risk Assessment; risk management strategy; supply chain risk management. "Detection" includes detecting incidents as well as gathering and sharing information about cybercrime and threats. Linkage with existing processes within organizations is a strong asset. The purpose of the Protection function is to develop and implement appropriate safeguards to ensure the provision of critical infrastructure services. It is divided into six categories: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance and Repair, Protective Technology. Determining risk is key due to the rapidly changing nature of cyber security threats and the need for continuous updating.

A full description of the Protection feature is shown in *Appendix 12*.

Critical Security Controls (CIS CSC)

The US Center for Internet Security's Critical Security Controls (CIS CSC) focus on specific practices that significantly increase protection against the most common cyberattacks[58]. CIS show the areas for creating a risk management program, security steps, blocking unauthorized access, identifying attacks and protection tools. Recommended guidelines for prioritizing control implementation are divided into three groups. Each implementation group defines a set of safeguards.

Core groups (controls 1 through 6), known as “basic cyber hygiene,” aim to thwart automated attacks from an external or internal source.

Foundation groups (controls 7 through 16) enable security teams to handle increased operational complexity and can depend on specialized expertise for proper installation and configuration.

Organizational groups (controls 17 through 20) represent a collection of best practices for identifying and controlling hardware and software assets; continuous vulnerability management; email and web browser protection; application software security; penetration testing and more.

[57] Keller Nicole, “Cybersecurity Framework,” NIST, 2013, https://www.nist.gov/cyberframework.

[58] Cisecurity, “The 18 CIS Controls,” Cisecurity, 2022, https://www.cisecurity.org/controls/cis-controls-list/.

All critical cybersecurity controls are presented in *Appendix 13*.

Based on the studies and analysis, we can summarize that each of the considered standards finds a place in the design of online services. The COBIT 2019 approaches support the creation of added value through the use of IT. ITIL includes the guidelines for the design and development of services and processes. The ISO 27001 standard uses a risk-based approach to security management, which requires higher education institutions to identify information security risks and select appropriate controls to address them. The National Institute of Standards and Technology's Cybersecurity Framework provides a strategy for the lifecycle of cybersecurity risk management, while CCPs can be used to block unauthorized access, identify attacks, and protect against tools.

Section 2.2 provides a comparative analysis of IT and cyber security management approaches and standards.

Information technology management is a tool for controlling and managing information resources[59] and is directly related to many web-based applications or specialized programs that require clear processes and procedures to operate.

Many international frameworks and standards address cybersecurity from similar but different positions, each providing principles, procedures, and practices for effectively managing cybersecurity risks. The European Union Agency for Cybersecurity has published a report that presents a comparison of the main security objectives. It provides guidance on assessing data security and compliance with the NIS Directive, providing a framework for cybersecurity management. The ISO/IEC 27001:2022 standard helps an organization establish, implement, maintain and continuously improve an information management system. COBIT and ITIL offer an approach to assess the level of security, but not mechanisms to protect cyberspace. The starting point in the approaches discussed in section 2.1 is the definition of information security requirements.

For the purposes of the study, a comparative analysis of COBIT 2019 and ITIL was made from the point of view of their relationship with ISO/IEC 27001:2022, including description, scope, users, scope and application. The task is to establish the basic prerequisites for a model based on the common fundamentals in the COBIT 2019 core approach.

A complete table with detailed information on the mapping between COBIT 2019 and ISO/IEC 27001:2022 is presented in *Appendix 13*.

The COBIT 2019 approach defines stakeholder needs, translated into outcomes or influencing business objectives, which are divided into four categories. COBIT does not correspond to an equivalent of the ITIL methodology, but applying a combination of both approaches reduces critical cybersecurity threats. ISO/IEC 27001:2022 has functions to preserve the confidentiality, integrity and accessibility of information. This availability of information is handled within ITIL and COBIT 2019 with aspects of IT quality, reliability and support[60].

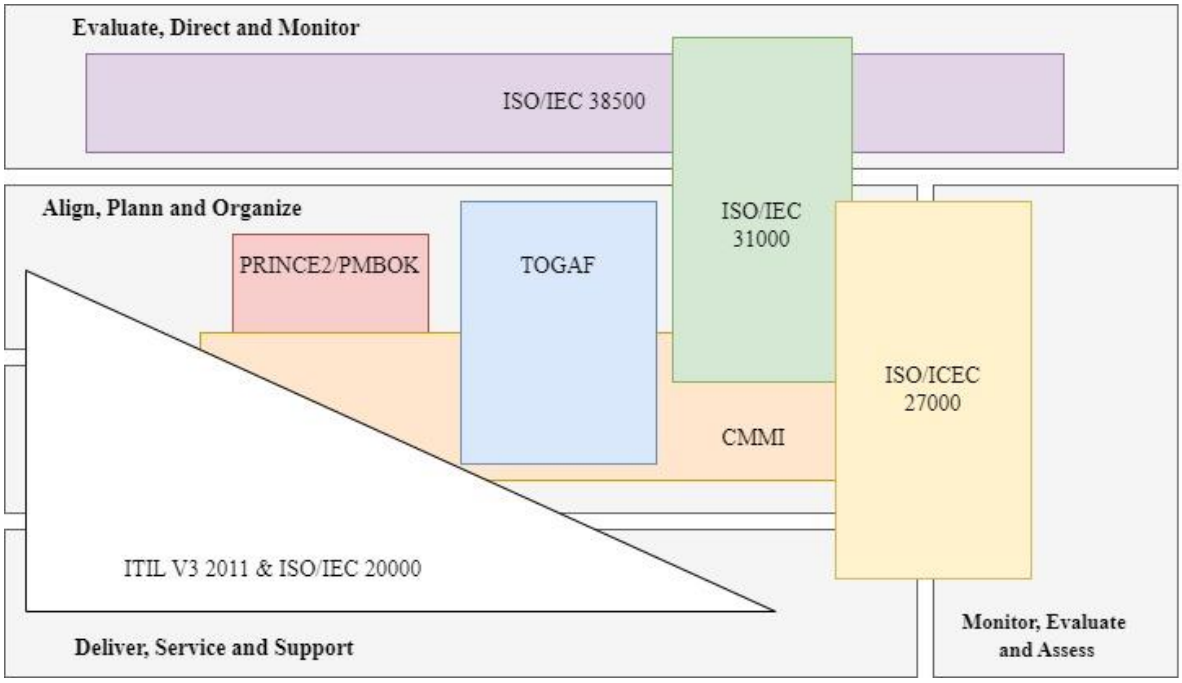
---

[59] Isaias Bianchi и Rui Sousa, „IT Governance Mechanisms in Higher Education“, *Procedia Computer Science*, International Conference on enterprise Information Systems, 100 (01 Януари 2016): 941–46, https://doi.org/10.1016/j.procs.2016.09.253.

[60] Shamsul Sahibuddin и Mohammad Sharifi, „Combining ITIL, COBIT and ISO/IEC 27002“, ResearchGate, б.д.,

Figure 5 shows a comparison of international information security standards and approaches. COBIT 2019 will be a more effective choice if we want to improve the quality and measurability of IT management throughout their implementation lifecycle. On the other hand, if we are looking to continuously improve the effectiveness of online services, ITIL would be the better choice because its methodology has a difference in its structure that deals with incident management and has no equivalent section in the COBIT 2019 approach[61].

Figure 5. Comparison of international standards and approaches of information security



Source: ISACA, 2022, www.isaca.org/resources/news-and-trends/industry-news/2017/using-cobit-5-to-assess-it-processes-capabilities-and-evaluate-compliance-with-the-world-lottery-ass

The difference between ISO/IEC 27001:2022 and COBIT 2019 is that the former is solely for information security purposes and the latter is for IT business process management. COBIT not only addresses security in an organization, but also includes how the organization arranges and controls IT operations. It has all IT controls, measures and processes and helps the organization link its own business goals to its IT goals. ISO/IEC 27001:2022 focuses on performing a risk assessment and then implementing specific security controls to protect critical information assets. It can be related to both COBIT and ITIL.

A mapping is made between COBIT processes and ISO/IEC 27001:2022 control objectives related to information security and the design of online services.

An important part of these processes are the development of new IT systems and services, remote work and business continuity management. That is why in the research, only the domain Plan and organize in COBIT 2019 is considered, because it is related to the design

https://www.researchgate.net/publication/325846466_Combining_ITIL_COBIT_and_ISOIEC_27002_in_Order_to_Design_a_Comprehensive_IT_Framework_in_Organizations.

[61] advisera.com, „COBIT vs. ITIL vs. ISO 20000: A comparison“, 20000Academy, б.д., https://advisera.com/20000academy/blog/2019/09/25/cobit-vs-itil-vs-iso-20000-a-comparison/.

of online services in higher education institutions and is discussed in detail in section 2.1. The full analysis is presented in *Appendix 15*.

The report "Factors influencing awareness and attitudes towards the implementation of IT governance in the higher education institution"[62] shows that depending on their strategies and goals, universities choose different approaches to IT governance. Some focus on service management, others focus on management and processes, or combine several standardized methods to have a comprehensive IT management. HEIs in Austria use a combination of COBIT, ITIL and ISO/IEC 27001:2022. British higher education has developed its own IT management system[63], which is also used by universities in Spain[64].

Section 2.3 discusses the different cybersecurity governance reference models and their requirements.

The benefits of adopting a reference model approach include achieving interoperability within and between different infrastructures and improving communication between multiple stakeholders. Provides excellent tools for defining scope in terms of functionality or area of business processes involved. One of the most common challenges information systems designers face is positioning a new or existing system in relation to other similar or related systems. Reference models of various kinds are particularly useful for this purpose.

Reference models are widely used in the telecommunications and defense sectors, as well as in corporate and public organizations. All of them are characterized by multiple vendors that must work with a common framework of principles and concepts to ensure interoperability.

In international standards[65], the reference model denotes the "reference points" between functional blocks. The scope of the standard derives from knowing the reference points (ie the possible areas) in which the standard can be applied. Understanding how different standards relate to each other is aided by having a conceptual framework within which they are situated.

Reference models unify standards and their use facilitates the work of engineers and developers who must create objects conforming to a given standard.

Depending on their functionality, the reference models are: business reference model; the reference model of the components (software and hardware); technical reference model (computer and communication equipment); reference data model; performance reference model; security reference model.

In order to clarify the structure of a reference model, some of the most popular reference frames and models are examined.

The Core Architecture Data Model (CADM) contains three main types of architecture models: conceptual, logical, and physical.

The NIST Enterprise Architecture Model is a five-layer enterprise architecture model designed to organize, plan, and build an integrated set of information architectures. The

---

[62] Uky Yudatama и съавт., „Factors affecting awareness and attitude of IT governance implementation in the higher education institution“, в *2017 3rd International Conference on Science in Information Technology (ICSITech)*, 2017, 588–92, https://doi.org/10.1109/ICSITech.2017.8257181.

[63] JISC, “Jisc,” Jisc, 2021, https://www.jisc.ac.uk/.

[64] Universitat de les Illes Balears, “ITG4AU - Universitat de Les Illes Balears,” ITG4AU, 2022, https://itg4au.uib.eu/Project/Mission/.

[65] ISO, NIST, CIS, COBIT 19, ITIL и други

hierarchy in the model is based on the fact that an organization has a number of business functions, each of which requires information from many sources. Each source can manage one or more information systems that contain data organized and stored in any number of systems.

The reference model Open Archival Information System (OAIS) serves for data management. Its main functions are to preserve information and provide access to archived information in a consistent manner for the needs of users or a particular community.

Service Oriented Architecture (SOA) is an abstract framework for understanding meaningful entities and relationships between them within a service-oriented environment, and for developing consistent standards or specifications supporting that environment.

A service-oriented architecture provides four different types of services: functional; application services; infrastructure, which are instrumental for processes such as security and authentication.

Each service consists of an interface, a contract, and an implementation. An interface defines how a service provider will fulfill requests from a service user. The contract defines how the service provider and user must interact. Deployment is about service management, which controls the development lifecycle and publishing to a service registry as well. The registry allows developers to quickly find and reuse them to build new applications or business processes.

From the above, it is clear that the structure of a reference model contains different levels of areas, functions related to them, objects to which the model is directed, as well as many processes and procedures. The OSI model, for example, provides a common basis for coordinating the development of ISO standards for the purpose of interconnecting systems.

The main goal of the reference model in the design of online services in higher education institutions is security. In order to achieve it, it is necessary to have a clear structure and interrelationships between the individual parts of the model. All applications should synchronously receive and modify data directly at their primary source, which will reduce the need to maintain complex data synchronization models. Determining the risk to both information systems and any online service is key due to the rapidly changing nature of cyber security threats and the need for continuous updating.

Cybersecurity requirements are based on multiple standards and best practices. The Cybersecurity Design article[66] describes the basic requirements: *attack surface minimization, security by default, least privilege, defense in depth, proven design patterns and secure components, security documentation, privacy*.

All the above listed good practices and guidelines should be part of the requirements of the reference model for designing online services in HE.

The reference model should be based on business requirements rather than existing system functionality and should cover all possible functions in the functional area being evaluated. The restrictions on its application are related to compliance with the regulatory documents in Bulgaria and the EU.

[66] Ashim Dutta and Prateek Singh, "Cybersecurity Design Principles," Eaton, 2021, https://www.eaton.com/us/en-us/company/news-insights/cybersecurity/cybersecurity-design-principles.html.

Structure of a reference model

Reference models are abstract models for business organization, developed for specific industries based on real experience from implementations and including practically verified procedures and management methods. They define typical business processes, horizontal and vertical connections and business rules acting in different areas or on objects.

The structure of the reference model contains: areas and objects; functions; organizational structure; processes and procedures.

Similar structures exist in a number of reference models, and their parts differ depending on the functionality of the given reference model. Fields and objects can be business objectives; software and hardware components; computer and communication equipment; information assets and data and others.

Reference models allow organizations to start developing their own models based on an already ready set of functions and processes, and are designed to provide a standard description of business process modeling and their analysis.

The wide application of reference models is related to the fact that they provide a standard language allowing the use of a uniform terminology. Almost all have a standard roadmap that provides a framework for process improvement, from creating a strategy to implementing new management practices, as well as a set of best practices that are associated with each process. Reference models present standard definitions of key performance indicators, thereby helping to measure the results achieved and improve business processes.

In section 2.4, the main characteristics of a cyber security reference model for HEIs are identified, as well as the methodology for its development.

The standardization of the processes in the design and management of online services in higher education institutions in Bulgaria requires allocation of responsibilities, IT management and risk reporting. Cyber security assessment and management processes transform security policies into concrete plans aimed at reducing threats and vulnerabilities.

To meet the general security requirements for the reference model described in section 2.3, it must cover functions and controls from the standards discussed in section 2.1 (COBIT 2019, ITIL, ISO/IEC 27001:2022, NIST CSF and CIS CSC), focusing on embedding cyber security in the design stages of online services in HEIs.

The requirement to minimize the attack surface can be achieved by applying the Cybersecurity Framework (NIST CSF) and Cybersecurity Critical Controls (CIS CSC). Defining risk is key to both approaches due to the rapidly changing nature of cybersecurity threats.

Critical cybersecurity controls will be used because they represent a collection of best practices for hardware and software asset identification, continuous vulnerability management, malware protection, data recovery, and more.

The default security requirement can be met, both when designing new services and when redesigning existing ones, by using COBIT 2019. The approach maintains a high level of compliance and incorporates parts of other information security standards by clearly delineating between the levels of strategic management and operational management (management).

The defense-in-depth requirement can be met by applying the security controls from Appendix A of the ISO/IEC 27001:2022 standard.

The requirement to use proven design patterns and secure components can be met by implementing the IT Infrastructure Library (ITIL).

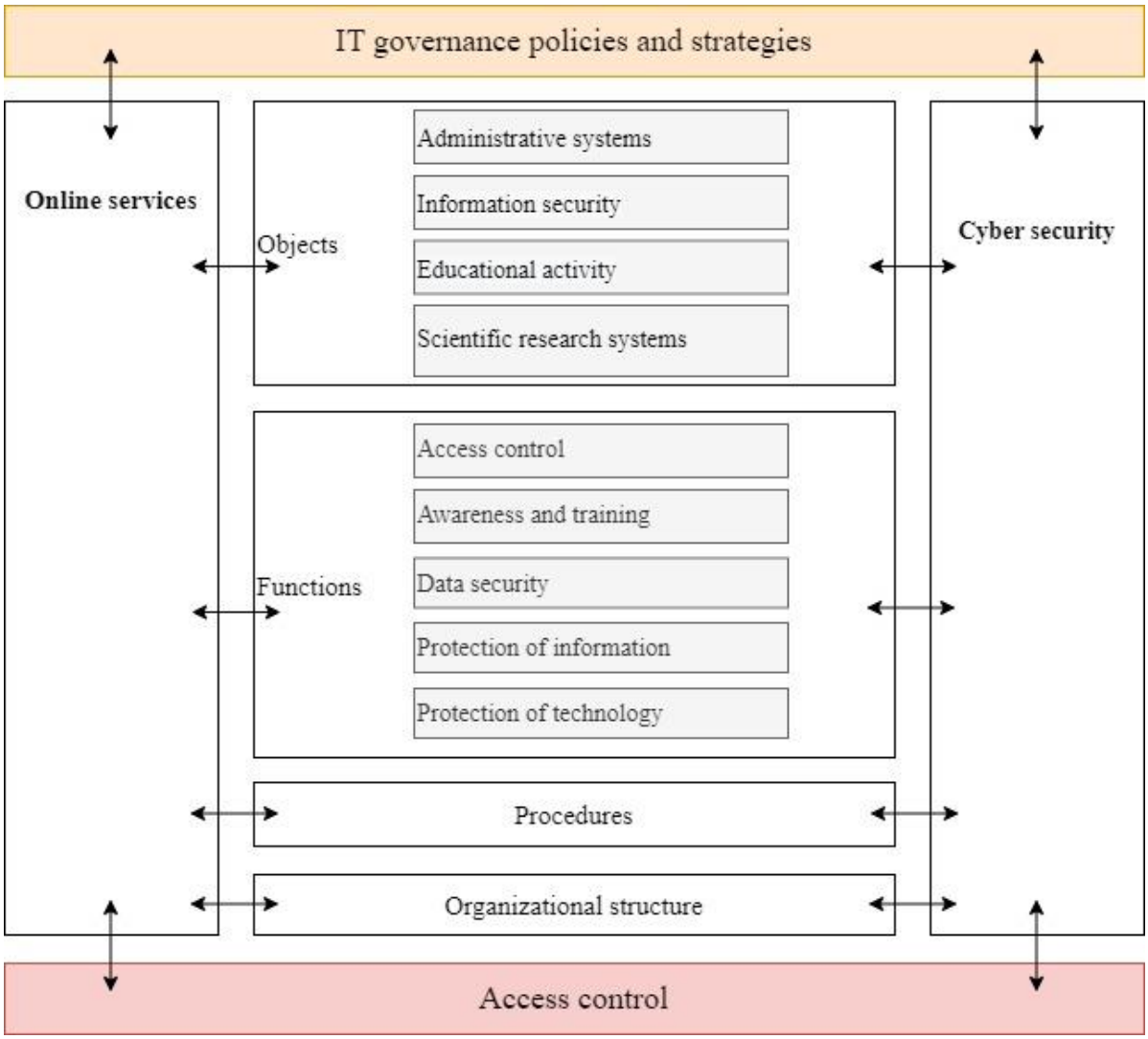
Least privilege, security documentation, and privacy requirements are covered by the standards discussed above and will therefore not be discussed in detail.

Structure and Interrelationships in the Proposed Cyber Security Reference Model

Based on the analysis of foreign experience in section 1.2 and after reviewing the reference models for cyber security management in section 2.3, it was chosen that the reference model consists of objects, functions, profiles and processes directly dependent on access control.

Figure 6 presents the structure and interrelationships in the proposed reference model.

Figure 6. Structure and relationships in the proposed reference model



The structure of the proposed reference model covers the defined areas described in section 2.3.

The reference model for cyber security in the design of online services in higher education consists of objects, functions, procedures and organizational structure. All elements

are united by the IT management processes and standards used, and frameworks for managing IT and cybersecurity.

Standards-based IT management policies and strategies is achieved by applying the areas of "Commit, Plan and Organize", "Build, Acquire and Implement" from COBIT 19. These two areas follow the common systems development life cycle and will be included in the reference model. The first covers strategic IT planning, creation of corporate information architecture and project management, and the second is related to the implementation of new information systems and services. Definition of processes and relationships should correspond to internal organization, operating procedures and related roles and responsibilities.

In the study, only the Plan and Organize domain in COBIT 2019 was considered, because it is related to the design of online services in higher education institutions.

Access control in the reference model is related to the recommended security controls to various objects and processes. From the analysis of standards section 2.1. and benchmarking in 2.2 we saw that COBIT incorporates ITIL ISO and is applicable to large organizations such as universities.

The objects in the proposed reference model are the main information systems and the online services derived from them. From the analysis of foreign experience in section 1.2, it was concluded that the main systems in higher education institutions are: administrative, information security, educational activity and scientific research systems. They need specific security controls and to them in section 3.2 documents from the used standards should be referenced.

The functions are directly related to the management of the objects and are selected depending on the risk profile of the information system or online service. The reference model uses the Protection feature of the NIST CSF standard, which outlines the appropriate safeguards to deliver critical infrastructure services and supports the ability to limit the impact of a potential cybersecurity event.

Procedures are presented as a model according to objectives, actions and standards documents, because the design of online services or the modification of existing ones requires the establishment of common processes and procedures. They are related to the design of a new online service, taken from the ITIL standard, with the reference model showing each process described by the standard and the related framework element to it.

The organizational structure was added due to the diverse user groups in the universities and shows a unique alignment of administrative roles with access control.

The RACI matrix, similar to the COBIT 19 reference model, is used to identify roles and responsibilities directly related to the organizational structure and governance of cybersecurity. The RACI matrix is discussed in detail in Section 3.3.

Conclusions

In Chapter two, the approaches and standards for managing information technology and cyber security in HE are analyzed.

The most commonly used reference models for IT service management and cybersecurity are presented. Their main characteristics and possibilities for their use in the design of online services are identified.

The requirements and limitations of the reference model are defined.

Chapter III. Application of the reference model development methodology

This chapter describes the process of developing the reference model.

In Chapter III, the following set tasks are completed:

1. To create a reference model for cyber security and standardization of online service management processes in higher education institutions in Bulgaria.

An analysis of university websites was done to see how different universities have organized the catalog of online services they offer. On the basis of the research done, and with the aim of unifying the various online services, the approach has been adopted that they are grouped in the same categories to which the information systems fall. The risk assessment of university systems is identified depending on the impact and probability of their security vulnerabilities.

The security controls are referenced to documents from the studied standards and are presented in detail in section 3.2.

Section 3.1 covers data collection and analysis. Data from a website scanning platform was used. The analysis covers the first page of the university site and shows the number of requests, transfers, domains and subdomains, protocols used, and the various security settings of the page header.

Many cybersecurity standards emphasize the importance of accurately determining risk through a systematic risk management process. Identifying, quantifying and mitigating risk are essential phases of risk management. Mitigating risk through adequate controls is linked to the implementation of strong cyber security measures.

Based on the research done in Chapter one, section 1.2, the main information systems in higher education institutions are defined.

Using COBIT 19, a risk assessment of university systems was made, taking into account their impact and likelihood of vulnerabilities. They are scored on a scale of 1 to 5 (1 being low, 5 being very high).

Table 1. Risk assessment of university systems based on COBIT 19

Information systems	Impact (1-5)	Probability (1-5)	Risk Assessment
Administrative systems	5	3	Very high
Information systems	5	4	Very high
Support and training	4	3	High
Research	2	2	Normal

Source: www.isaca.org/resources/cobit

Table 1 shows that Administrative and Information Systems have a very high risk assessment. The risk for systems related to "Maintenance and Training" is defined as high, and for systems related to "Research" it is normal.

The Service Catalog is a complete list of services managed by the University. Some of these services are visible to customers, while others are not. Security controls to information systems are fixed, while controls to services change depending on whether they are visible or not (whether they have access to the Internet or not) and according to their current status.

University websites were reviewed to see what categories services were organized into. Different universities have adopted different ways of organizing the catalog of services they offer. Many of the categories overlap in content but are named differently.

In Table 2, the university information systems and the categories of services to them can be seen. Each category includes services with similar technological processes and cybersecurity requirements in accordance with the information system used.

Table 2. Information systems and categories of services in higher education institutions

Information systems	Categories of services
Administrative systems	Profiles and Authentication
	Archiving and storage
	Information security
	Communication and collaboration
Information systems	Networks and infrastructure
	Servers and data
	Web development and hosting
	Hardware, software and applications
Learning activity	Awareness and training
Studies	Research

Source: Own research

On some sites, services can be filtered not only by category, but also by type of users (eg students, teachers, employees and others).

Description of the categories of services in the higher education institution:

Profiles and authentication – services related to authentication, authorization and account management, access control systems, etc.

Archiving and storage - services related to the storage, sharing and management of moderate and high risk university data.

Information security - services related to the security of information assets, network connectivity, disk encryption, etc.

Communication and cooperation - services related to candidate-student and master's campaigns, organization of events and conferences, etc.

Networks and infrastructure - services related to the management of information systems, maintenance and construction of data networks, etc.

Servers and Data - services related to system administration, endpoint configuration management, data migration, virtual servers, and more.

Web development and hosting - services related to the university's web infrastructure and resources, web hosting, domains, etc.

Hardware, software and applications - services related to the management of desktop computers, laptops, mobile phones and peripherals, licensed software, programs and modules, cloud services, etc.

Support and training - services related to the creation of digital educational resources, participation in internship programs, training, consulting, etc.

Scientific research – services related to research administrative systems, storage of scientific data and publications, technical support, etc.

Based on the risk assessment of the university systems, using the COBIT 19 approach, the resulting services are attributed to them, taking into account their impact and probability of vulnerabilities. They are scored on a scale of 1 to 5 (1 being low, 5 being very high).

Table 3. Risk assessment of online services, using the COBIT methodology

Information Systems	Online Services	Impact (1-5)	Probability (1-5)	Risk assessment
Administrative systems	Profiles and authentication	5	3	Very high
	Backup and Storage	4	2	High
	Information security	5	4	Very high
	Communication and cooperation	2	2	Normal
Information systems	Networks and Infrastructure	4	4	High
	Servers and data	5	4	Very high
	Web Development and Hosting	3	3	Normal
	Hardware, software and applications	4	5	Very high
Support and training	Awareness and training	4	3	Normal
Scientific Research	Scientific Research	2	2	Normal

Source: Own analysis based on research done.

From table Table 3, it can be seen that the services in the category "Profiles and authentication", "Archiving and storage" and "Information security" have a high impact.

"Communication and Collaboration" services have a normal risk, as they do not have high security requirements.

Services in the "Networks and Infrastructure", "Servers and Data" and "Hardware, Software and Applications" category are characterized by high impact and a very high probability of security risk. Web Development and Hosting Services risk rating is Normal. The risk for the services related to "Support and training" and "Research" is defined as normal.

The grouping of services is an important step related to the creation of a catalog of services in a higher education institution. Service catalog management includes all processes from the life cycle of service design, its protection and backup. Service design in ITIL identifies service requirements and develops new service offerings as well as changes and enhancements to existing ones.

All services must have cybersecurity requirements to ensure that users and processes will only access information or resources to which they are entitled. There should also be requirements regarding the unauthorized creation, modification or deletion of information. This includes all functions designed to control the flow of information and the use of resources by users, processes, and objects. Services related to administrative systems must have requirements to provide specific functions designed to ensure that data will not be modified in an unauthorized manner.

The service reliability feature ensures that access to resources is possible when needed and that resources are not unnecessarily requested or held. Data exchange covers all functions designed to ensure the security of data during transmission over communication channels. Error detection and recovery features minimize interruptions or loss of service.

In section 3.2, security controls are referenced to model functions.

Access control in relation to functions

Access control encompasses all credentials that are issued, managed, verified, revoked, and audited for authorized devices, users, and processes. It applies to administrative and information systems and has the most cybersecurity controls.

Awareness and Training: This area determines whether faculty and staff receive cybersecurity training and can perform their duties and responsibilities in accordance with relevant policies, procedures and agreements. It has three subcategories - Security Training, Privileged Users and Employees, and Third Party Stakeholders.

Data security: Data is managed in accordance with the organization's risk strategy to protect the confidentiality, integrity and availability of information. This area has five subcategories: Data Security, Asset Management, Data Protection, Software and Information Integrity Verification, and Development and Testing Environment.

Information Security: Security policies are maintained and used to protect information systems and assets. This area has seven subcategories - Basic IT/Systems Configuration. Systems Management System Development Lifecycle, Configuration Change Control Processes, Information Backing Up, Physical Work Environment Provisions for Organizational Assets, Security Processes, and Cybersecurity in HR Practices.

Security technology: Technical security solutions are managed to ensure the security and resilience of systems and assets, in accordance with relevant policies, procedures and agreements.

The most important features of modern online service security tools include visibility and protection, coverage of different architectures, integration with DevOps tools, automation and continuous updates.

Visibility of services in use, traffic flowing to them, and endpoint connectivity are critical. To protect services based on both on-premise and cloud infrastructure, HEIs must provide modern solutions and deployment flexibility.

The ability to integrate with load-balancing gateways or the use of software-as-a-service provides choice and consistency regardless of the type of service being protected. The dynamic threat landscape makes manually updating, testing and deploying policy sets and security controls an impossible task. This is precisely why tools and models are needed that can provide automation and enable orchestration across the entire application infrastructure. It's important that web application security tools and controls fit their processes and integrate with the tools that IT teams use. To achieve this, university web applications and online services must have a wide range of features and capabilities, security by design, embedding cybersecurity into all processes, and support for new technologies.

Section 3.3 elaborates the procedures in the reference model.

The structure of the reference model described in section 2.4 includes organizational structure, roles, responsibilities and procedures.

The organizational structure represents departments in which the roles, responsibilities and their interrelationships are formed according to the selected structuring criteria. Organizational roles are related to task performers achieving business goals.

Higher education institutions do not have identical organizational structures of IT directorates and departments. Each university has developed and changed based on many factors over time, and the organizational structure varies according to size and activity. IT directorates may be integrated into the institution, reporting through deans or department heads, but they may also be administrative units reporting directly to chancellors, through chief information officers, or in rare cases through chief financial or administrative officers.

The ISO 27001:2022 standard has developed templates for the information security organizational structure of small, medium and large organizations. In small organizations, it is characteristic that one person combines several positions, while in large organizations, experts responsible for a certain field of IT work. Staff in IT departments manage a wide range of activities, sometimes with dual roles for administrative and academic functions.

Some HEIs may have dedicated board committees focused on information resources, while others tend to diversify information support into other more central functions such as enrollment, learning, and student life.

The COBIT 19 standard has a defined organizational structure related to the cascading of goals and processes within it.

The implementation of the procedures in the reference model is related to the distribution of IT management roles and responsibilities. To clarify them, an organizational structure in COBIT 19, as well as the roles and responsibilities related to service design in ITIL, is considered.

Roles are based on online service design processes as well as common IT practices, and names and combinations may vary depending on the organizational structure of the HEI.

It is key for any university to ensure that, based on its structure, services offered and processes, relevant roles can be easily identified, documented, assigned and reviewed.

The concept of a procedure is a set of sequences of established actions for the performance of a specific task. Having a process in place when designing online services ensures that every proposed service and accepted change is evaluated in a consistent and repeatable manner from a cyber security perspective.

The procedures for working with the reference model describe the steps to be followed and include all stages related to the creation of a new service from design coordination to the selection of referenced security controls.

Description of procedures

1. *Design coordination* - creating a design for designing services, through the maintenance of policies, standards, necessary resources, etc. This procedure uses the charts from COBIT 19 to allocate executive management roles related to the design and development of the new service.

2. *Overview of the classification of information systems* - determining which type of information system the future service will work with.

3. *Review of the classification of services* - determining to which group of services the new service can be assigned.

4. *Review of cybersecurity features* – ensuring that all cybersecurity features that are required for the particular service are included.

5. *Selection of system components* – determining which system components should include architectural constraints, critical security points, and protection mechanisms.

6. *Baseline Configuration Management* – ensuring that every proposed and accepted change is evaluated in a consistent and repeatable manner from a cyber security and systematic perspective.

7. *Service catalog management* – provision of information about the service, its current status and its interdependencies with other services.

8. *Security Controls Management* - ensuring that the applied standards and related security controls from the reference documents meet the intended level of risk for the new service. For a certain type of service, it may be more appropriate to use the ISO/IEC 27001:2022 standard, while for another type, the use of ITIL is more appropriate.

Organizational policies, procedures and standards are often developed long before service design is completed. Controls that satisfy these policies, procedures, and standards may be evaluated prior to service release.

Based on the comparative analysis between COBIT 2019 and ITIL in section 2.2, it became clear that applying a combination of the two approaches reduces critical cybersecurity threats. That is why the roles are taken from the COBIT 19 approach, and the processes related to service design from the ITIL standard.

The COBIT 19 approach defines multiple roles related to the organizational IT structure. These include the chief director in charge of IT and cyber security; chief risk officer responsible for all aspects of risk management in the organization; Chief IT Officer responsible for overall IT management; chief operating officer responsible for business

strategies, planning and management of IT service delivery and solutions; chief security officer responsible for all aspects of information security management.

All roles and responsibilities in COBIT 19 are shown in *Appendix 17*.

The RACI matrix in COBIT 2019 allows to identify the key topic areas requiring clear decision-making roles and responsibilities. RACI has four types of associations: responsible, accountable, consulted and informed. The spreadsheet posted on the COBIT page provides guidelines that show the processes appropriate for each position[67]. The matrix breaks down each process and provides flexible guidelines for which role in the organization is "Responsible" or "Reportable" for each process. Once these two key roles are defined, the roles for 'Consulted' and 'Informed' can be defined based on the unique requirements of each HEI. An advantage of collecting all processes in RACI is that it is easy to filter all the accountability practices of a role and then compare the metrics reporting those practices.

In ITIL, there are certain management positions related to service design, continuity, security, capacity, availability, compliance, service catalog management, suppliers and others.

All ITIL service design roles require specific skills, qualities and competencies from the people involved to be able to work effectively and efficiently and are shown in Appendix 18.

Each organization defines appropriate job descriptions that meet their needs, and the individuals occupying these positions may perform one or more of the required roles.

The structures of the higher education institution include the general assembly, academic council, rector and rector's management, control board, commission for academic ethics, faculties, directorates, institutes, centers and others. In government institutions, these basic organizational units cooperate with external bodies such as government, community and business organizations. External organizations interact with and shape the policies and procedures of the university's internal organizational structures on a daily basis.

According to the ISO 27001:2022 standard, the organizational structure of information security in a university should have a Security Committee, including an information security manager and a security committee in the various departments.

Conclusions

In Chapter three, the application of the methodology for developing the reference model is structured. A risk assessment was made according to the impact and probability of vulnerabilities of university systems and online services derived from them. Referenced security controls to model functions. The procedures for working with the reference model have been developed and the roles and responsibilities related to IT management in higher education institutions have been established.

The proposed reference model describes the main information systems and services in higher education institutions, as well as the ways in which they connect and interact with each other. The model brings together several IT governance and cybersecurity standards and sets standards for both the entities in the model and their relationships to each other.

[67] ISACA, "COBIT | Control Objectives for Information Technologies," ISACA, 2022, https://www.isaca.org/resources/cobit.

Using the reference model will help managers in the development of online services to divide the problem space into smaller parts that can be understood, solved and improved. This will improve communication between those involved in the various processes and procedures by creating clear roles and responsibilities.

Reference model operating procedures include clearly defined service design processes to ensure that each proposed service and accepted change is evaluated in a consistent and repeatable manner from a cybersecurity perspective.

Chapter IV. Reference model verification and validation

In Chapter IV, the following set tasks are completed:

1. The model should be verified and validated through document analysis and interviews with experts. The reference model to be implemented by creating an online application.

In section 4.1, a platform selection is made for developing a test software application. The most popular open source content management systems are reviewed - WordPress, TYPO3, Joomla!, Drupal, Contao, Neos, WooCommerce, OpenCart, AbanteCart, PrestaShop. A comparison is made of their specific functionalities in the areas of installation and configuration, user management, service catalog, content creation, data filtering, source code modification capabilities, and system adaptation to individual design and cyber security requirements.

In order to find the best software solution, an assignment was made to the platform, divided into the areas: administration, content management, service catalog, notifications and comments, tracking and reporting, in accordance with the research analyzes made in Chapter Two, Section 2.3.

For the purposes of the dissertation, the OpenCart platform was chosen, which allows creating multiple administrator roles with different access rights, adding an unlimited number of services, creating links to a selected category or subcategory (e.g. information systems, cyber security areas, cybersecurity controls), service status (active, inactive, under development), similar and related services, and adding information pages.

In the admin panel there is an overview of all services, users, recent revisions, data saving and recovery tools, open source code and rich documentation. Specific functionality is adding attribute groups and attributes to a group. The attribute groups are used to introduce the standards used, and the attributes to each group to introduce the cybersecurity controls of the corresponding standard. The ability to filter and sort services by specific functions (eg service criticality) has also been created.

Application Description - User Interface

The main menu bar is located horizontally at the top of the site. The buttons are as follows: Home, Reference Model, Standards, Information Systems, Cyber Security and Online Services. Figure 7 shows a screenshot of the first page of the site.

Figure 7. Screenshot of the first page of the platform – www.csservices.online

The Reference Model part includes four submenus: Description, Workflow, Verification and Validation, Team. On the Model Description page, a video has been made and uploaded, showing how to work with the main functionalities of the platform.

The Verification and Validation section (https://csservices.online/verification-and-validation) contains information from the web platform audit performed through the site www.semrush.com/siteaudit. Made a "Web Platform Testing" gallery with screenshots from the audit. The page contains a link to the survey and the case study in Forms for verifying the reference model.

The Standards section covers the standards used (ISO/IEC 27001, COBIT 2019, ITIL, NIST CSF, CIS CSC), with a brief description, security controls and useful links to official sites for each.

The Information Systems section covers the four main types of systems: administrative, information, learning and science.

The Cybersecurity part covers the five areas: access control, data security, awareness and training, information protection and protective technologies.

The "Web services" part covers the main types of university services related to the types of information systems: administrative, information, support and training, scientific research.

The navigation of the internal pages in the website has consistent naming, styling and positioning. The site has a responsive design, displaying the content on different screen sizes (eg mobile devices and tablets).

Application Description - Administrative Interface

The administrative panel is divided into the following parts: overview, journal, catalog, gallery, design, clients, system, reports, file manager and visual editor.

Overview is the part that gives information about users and new requested services. The journal is the part responsible for the design, styles, views of individual page types, information to be included in the top and bottom of the site, module management, and all system settings. Catalog is the main part related to category and service management and includes: product tags, filters, attributes, options, downloads, comments and general information.

The gallery enables adding albums of screenshots from the different stages of a web service's development or testing, making reviewing design, functionality and service auditing very easy. Design is responsible for views, theme editor, banners, SEO URLs. All settings, users, database, hosting panel, support (archiving, error log) are defined from System. Various statistics can be viewed in Reports. In File Manager is the organization of all uploaded files into custom folders.

Advantages are various templates and modules management interfaces, automatic image resizing, service editing, reports and statistics make it easy to manage the service catalog.

Entering or editing a service has the following fields:

• General – name of the service and automatic generation of SEO address, description;
• Data - status, alphabetical order or manual numbering
• Links – service provider, link to categories, filters, downloads, related services
• Attributes – security and description controls that are called from a predefined list
• Options
• Period – time during which the service is active and available
• Image – photos from the design and service design processes

The platform has the possibility of adding an unlimited number of attributes (standards used in the reference model), as well as their order of priority.

Auditing and testing of the software application is done through the website www.semrush.com. It shows that there are no issues with duplicate content or broken internal links. A gallery showing all stages of the audit has been made: https://csservices.online/index.php?route=gallery/album.

The verification of the reference model aims to check whether the specification, program code and documentation created in the course of development conform to the rules and standards of IT. By means of formal verification, a review of the correctness of the software provision was made, and key information systems and a database were selected.

Scenarios for developing online services related to different types of information systems

Sample services have been uploaded to the web platform, for which it has been determined which information systems they work with, the types of services they belong to, as well as the security controls referenced to them. *For example: VPN remote access, student accommodation services, changing a forgotten password in Web Student, registration in Web Student, online enrollment of newly admitted undergraduates, NID planning and reporting, provision of web hosting for research purposes. Some of the services are marked as "under development" and the reference model may be applied to them. For example: sport selection*

request, annual leave inquiry, information campaign, administration of research systems, archiving and storage.

Based on the created procedures for working with the reference model in Chapter 3, section 3.3, a template table is filled with information about the new service. In it, users of the service are entered, it is determined with which type of information systems the future service will work, to which group of services it can be assigned. Cybersecurity areas are reviewed and only those areas are included that are necessary for the particular group of services and security controls are applied from the reference documents that meet the intended level of risk for the designed service.

Survey, description and case study for working with the reference model

In order to validate the proposed model and to identify the possibilities for its improvement, a study was conducted based on the expert opinion of people from the IT sector. The study is structured in three sections, including a survey with participant information, information security issues in the design of online services, and a practical case study aimed at creating an example service and defining cybersecurity controls for it. Solving the case and expressing an expert opinion on the issues covered in the scientific research carry the most weight.

The survey and a description of working with the reference model were sent to more than 50 experts working in higher education, as well as in other fields related to cyber security and online services. 28 experts responded to the survey and completed the case study.

The positions held by the respondents are in different areas of IT. The survey included department managers and team leaders related to IT and cybersecurity management, network engineers responsible for configuring and managing firewalls, software application design and programming experts, graphic designers, web optimization experts, web testers software, network and system administrators, as well as professors, associate professors and postdoctoral researchers from universities working in the field of cyber security.

When asked "Does your organization implement a certified information security management approach?", 75% answered "Yes" and 21% answered "No". The answers to the question “Is there a policy for the use of cryptographic protection of critical information?” are also close in value. This is because a large number of respondents work in large corporations and the banking sector, where IT and cybersecurity management is standards-based.

From the survey, it is clear that employees working in large organizations must undergo cyber security training, which is tied to information security policies. When asked "Do employees receive cyber security awareness training?", 71% answered "Yes", 4% "Unable to judge" and 25% "No".

To the questions related to the development of proprietary software, information systems and services and policies requiring the implementation and evaluation of cybersecurity controls, the responses were close in value, with 75% answering "Yes", 7% "Unable to assess" and 18% "No".

Do you think the reference model is suitable for secure service design? 96% answered "Yes" and only 4% answered "I can't judge". 64% shared that they believe it covers all areas of cybersecurity, which is shown in Figure 8.

Figure 8. Screenshot 2 of the reference model survey

The question "Would you use controls from different standardized approaches when designing an online service?" is extremely important because it provides information on what type of services are in the organization and whether there is a working catalog of services. To this question, 61% answered "Yes" and 36% "I cannot judge".

Analyzing the answers and comments to the survey and the case study, we can conclude that the proposed reference model examines the problems related to cyber security in depth and guarantees the security of the classified information related to the activity of the relevant university. The respondents agreed that the proposed reference model is well structured, logically connected and offers a flexible approach. Some of them point out that the reference model enables the choice of security controls between standards and provides a solution to many challenges and problems facing HE. A small number of respondents expressed the opinion that the model is too detailed and using different approaches to cybersecurity would confuse employees.

The case that the respondents had to develop is related to working with the software application and requires the creation of a new online service by going through all the procedures of working with the reference model described in section 3.3.

The execution of the case study covers coordination of the design of a service, selection of information systems to work with, classification of the service, review of cyber security areas, selection of security standards and controls to be implemented. Recommendations for improving the reference model after the case study include adding more buttons and drop-down menus to the user interface of the software application to show the internal content. Another proposal is related to new functionalities and filters to facilitate working with the reference model – a filter for service criticality, service status, as well as adding the roles and responsibilities of people related to the design and management of an online service.

Conclusions

In Chapter Four, the reference model is verified and validated. The model validation was done using a software application based on a content management system. The verification done shows that the technical specification and the program code created in the course of the development correspond to the good practices in IT.

Validation of the reference model shows that the design of an online service meets its intended purpose and that the cyber security controls applied do not contradict the classification of that type of service.

The proposed model will be useful because HEIs offer many online services, some of which are related to the main university activities. Designing secure online services is about implementing secure baseline configurations, strict security controls, and a reliable network infrastructure.

CONCLUSION

In the course of the scientific research, the relevance and significance of the research problem related to the need for structured security management in the design of new electronic procedures and services in higher education was confirmed. The relevance of the researched problem is determined by the need for digital modernization and management of IT in higher education.

IT management in higher education institutions covers structures and processes, roles and responsibilities, IT policies, characteristics and specific features of existing management models, good IT management practices.

The thesis defended in the dissertation, that at the moment there is no specialized model for cyber security in HE, and therefore it is necessary to explore the possibilities and create one, has been confirmed.

The main problem related to the management of online services and cyber security was identified, as well as the complex structure of universities, the high demands on them and the rapidly changing IT environment.

The purpose and objectives of the study have been met. As a result of the fulfillment of the tasks set in the dissertation, the need for the creation of a reference model for cyber security and standardization of the management processes of online services in higher education institutions is confirmed.

The proposed reference model for cyber security, aimed at secure design of online services, is specific to Bulgarian higher education and is based on IT service standards, taking into account the peculiarities of the organization of higher education institutions in the Republic of Bulgaria. Its implementation will lead to the improvement and modernization of processes, increasing the maturity of the organization, achieving the strategic goals and objectives of the institution, adding value and acquiring strategic advantages, as well as appropriate managerial practices and effective management of information technologies.

The model has been verified and validated through document analysis, interviews with experts and implemented through the creation of an online application.

In addition, a number of issues related to the legal aspects and modification of existing legislation in the current cyber security policy were identified that require further investigation.

The reference model will help to improve communication and exchange of information between different structural units, create conditions for the rapid introduction of new electronic procedures and services, digitalization of scientific research, as well as standardized criteria for analysis and increase the security of data exchange and information.

IV. SCIENTIFIC AND SCIENTIFIC-APPLIED CONTRIBUTIONS

Scientific contributions

1. A methodology for designing online services that meets cybersecurity standards and requirements has been modified. The proposed methods and means of their application offer increased scalability and traceability during the cybersecurity design of complex, networked information systems.

Scientific and applied contributions

2. The main information systems used in higher education organizations have been identified and are structured from the point of view of cyber security of the services offered. A classification of information systems from the point of view of cyber security risks is proposed.

3. A reference model has been developed for cyber security in the design of online services in higher education institutions in the Republic of Bulgaria. The model was developed based on the use of IT management and cyber security standards.

4. A process for the design of new online services has been developed, which includes all activities from the design to the selection of cyber security controls and enables the achievement of higher efficiency and expands the possibilities of control and auditing of online services.

Applied Contributions

5. The developed reference model has been verified and validated by creating an online application enabling the creation of a catalog of online services with referenced security controls for each service, according to internationally recognized standards in the field.

V. PUBLICATIONS AND RESEARCH PROJECTS

Publications

1. Pavlova "Enhancing the Organizational Culture related to Cyber Security during the University Digital Transformation", Second International Scientific Conference "Digital Transformation, Cyber Security and Resilience" (DIGILIENCE 2020), magazine Information&Security, vol.46, no.2 (2020) : 239-249, https://doi.org/10.11610/isij.5006, ISSN 0861-5160 (print), ISSN 1314-2119 (online).
2. Pavlova "Increasing cybersecurity in the process of digitization in higher education institutions in Bulgaria", 10th International Conference on application of information and communication technology and statistics in economy and education (ICAICTSEE 2020), November 27-28th, 2020, UNWE, Sofia , page 474-481, ISSN 2367-7635 (print), ISSN 2367-7643 (online).
3. Pavlova "Infrastructure and management of access to information resources at UNSS", Reports from the tenth anniversary international scientific conference for doctoral students and students "Infrastructure: business and communications", pp. 33-43, April 21, 2021, UNWE.
4. Pavlova "Challenges for cyber security in the use of personal devices in the UNSS", 2021, Scientific works of the UNWE, ISSN 2534-8957 (online).
5. Pavlova "Implementation of Federated Cyber Ranges in Higher Education in Bulgaria: Challenges, Requirements and Opportunities", Third International Scientific Conference "Digital Transformation, Cyber Security and Resilience" (DIGILIENCE 2021), magazine Information&Security, vol.50, no.2 (2021): 149-159, https://doi.org/10.11610/isij.5006, ISSN 0861-5160 (print), ISSN 1314-2119 (online)
6. Pavlova "Economic aspects of cyber security in higher education institutions". Participation in the conference "Economic challenges: crisis, recovery, sustainability", November 19, 2021, UNSS.
7. Pavlova "Reference model for cybersecurity in the design of online services in higher education institutions in Bulgaria", 11th International Conference on application of information and communication technology and statistics in economy and education (ICAICTSEE 2021), November 25-26th, 2021, UNWE, Sofia.
8. Pavlova "Awareness and training on cyber security in universities in Bulgaria. Compliance with ISO 27001", conference "Economic Challenges 2022", June 17, 2022, UNWE.

Participation in research projects

- 2021, NID NI: Requirements and conceptual model for the creation of a training laboratory in the "Magiser" OCSC on cyber security in the UNSS
- 2022, NIP Fulbright Poland: University Cyberclinic at University of National and World Economy

- 2023, NIP under the program "Horizon-Europe": Creation of a prototype system for authentication of users of secure information systems, based on a brain-computer interface
- 2023, NIP under the "Horizon-Europe" program: Construction of a database and development of specialized software for automated processing and analysis of Big data to ensure the functionality of the National Situation Center (NSC) and Crisis Management Center (CMC)