УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И СВЕТОВНО СТОПАНСТВО

Факултет „Икономика на инфраструктурата“
Катедра „Национална и регионална сигурност”

А В Т О Р Е Ф Е Р А Т

на дисертационен труд за придобиване на образователна и научна степен „доктор“ на тема:

СИГУРНОСТ НА ИНФОРМАЦИЯТА ВЪВ ВИСШЕТО ОБРАЗОВАНИЕ

Професионално направление: 3.8. Икономика
Докторска програма: Икономика и управление (Отбрана и сигурност)

Докторант:
Елена Ангелова

Научен ръководител:
доц. д-р Георги Павлов

София
2024

Дисертационният труд е с обем 162 страници и се състои от увод, три глави, съкращения, терминологичен речник, заключение, приложение, научни приноси, научни публикации и библиография. Съдържа общо 145 цитирани източника, 57 от които са на български, а 88 са чуждоезични.

Дисертацията съдържа 50 фигури и 6 таблици. Включените в автореферата фигури и таблици съвпадат с тези в дисертационния труд.

Дисертационният труд е обсъден и насочен за защита от научно звено, включващо преподаватели от катедра „Национална и регионална сигурност" и хабилитирани преподаватели от катедра „Информатика" при УНСС, град София, състояло се на 10.12.2024 г.

Защитата на дисертационния труд ще се състои на открито заседание пред научно жури, назначено от ректора на УНСС, на 11.02.2025 г. от 10 часа в зала "Научни съвети" (2032А). Материалите на докторанта са на разположение на заинтересованите в катедра „Национална и регионална сигурност". Авторефератът е публикуван в сайта за развитие на академичния състав на университета.

Автор: Елена Ангелова

Заглавие: „Сигурност на информацията във висшето образование"

С Ъ Д Ъ Р Ж А Н И Е

ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Актуалност на проблема

Актуалността на проблема се определя от глобалните промени, породени от развитието на технологиите и киберпрестъпността. Информационната сигурност се постига чрез:

- ⇒ превантивни мерки – свързани с контролиране на риска и ограничаване на нежелани събития, като въвеждане на пароли и политики за сигурност, засекретяване на информация, файъруоли и т.нат.
- ⇒ откриващи мерки – отнасящи се до откриване на събития, които могат да доведат до нежелани явления, като проследяване, използване на сензори за движение, системи за наблюдение и т.нат.
- ⇒ възстановителни мерки – имащи за цел възстановяване на целостта, конфиденциалността и наличността на информацията (като резервни копия, въвеждане на планове за работа при аварии, определяне на допустим диапазон от грешки и т.нат.).

Предметната област на информационната сигурност се свързва освен със защита на информацията и с изискванията за сигурност на информационните системи, начините за оценка на риска, предприетите политики за защита на информацията. Основна характеристика на сигурността на информацията е нейната наличност, отразяваща, от една страна, единствено достъпа на оторизирани лица до нея, а от друга – необходимостта от определено време и ресурси за представяне на информацията на база, извършена заявка за достъп.

2. Изследователски проблем

Изследователският проблем на дисертационния труд е да се установят основните политики за информационна сигурност, които оказват ефективно и ефикасно въздействие върху съхраняването на информацията.

Апробирането на модел за сигурност на информацията във висшето образование спомага да се:

- ⇒ подобри информационната сигурност във висшето образование;

⇒ ограничат уязвимостите и заплахите в информационната сигурност във висшето образование;

⇒ ограничат рисковете от кибератаки;

⇒ регламентира достъпа до информация и данни.

3. Цел и задачи на дисертационния труд

Цел на дисертационния труд е да се създаде концептуален модел на информационната сигурност във висшето образование. Предложеният модел следва освен да анализира всички уязвимости на информационната система във висшето образование, да отговаря на нормативната уредба и да позволи създаване на ефективно наблюдение, извършване на превенция, повишаване на ефективността на използваните ресурси, ограничаване на киберпрестъпленията и актуализиране.

Задачи:

1. Да се представят теоретичните аспекти на информационната сигурност.
2. Да се разгледат правно-организационните и технологичните аспекти в информационната сигурност във висшето образование.
3. Да се анализира текущото състояние на информационната сигурност във висшето образование.
4. Да се изготви модел за ограничаване на уязвимостите и заплахите в информационната сигурност във висшето образование.
5. Да се определят ползите от внедряване на модела за подобряване на информационната сигурност във висшето образование.

4. Научна теза

Научната теза се основава на твърдението, че създаването на модел на информационна сигурност в сектора на висшето образование ще предостави нови възможности за съхраняване, защита и актуализиране на информацията и потока от данни.

5. Обект и предмет на дисертационния труд

Обект на изследване е системата за осигуряване на сигурност на информацията в университетите.

Предмет на изследване са възможностите за ограничаване уязвимостите и заплахите в информационната среда чрез предлагане на концептуален модел на информационната сигурност във висшето образование.

6. Методи за изследване

Използвани **методи** в дисертационния труд са анализ и синтез, индукция, дедукция, сравнителен анализ, логически и системен подход, както и анкетен метод.

СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

ПЪРВА ГЛАВА. ИНФОРМАЦИЯ И ИНФОРМАЦИОННА СИГУРНОСТ

В точка 1.1. „Информация – същност, произход и специфика на защитата“ се извеждат основни дефинитивни понятия относно същността и спецификата на информацията. Учените извеждат формулировката за информация като *„ценен и важен ресурс“*, от който напълно зависи *„цялостното икономическо и социално развитие на регионите.“*[1]. В своята широка смислова цялост, информацията е: данни, знания, ноу-хау, опит, които спомагат да се задоволят потребителските очаквания и нагласи, както и да се достигне до конкретни цели[2]. Това е основната причина информацията като ценен капитал да бъде защитена през всички фази на своя жизнен цикъл – от създаването ѝ до нейното унищожаване. Независимо от формата, която приема, тя винаги трябва да бъде добре защитена[3].

Думата произлиза от латинската *informare* – давам форма, т.е. информацията винаги е представена с някаква форма, структура, модел; *informatio* – давам представа, понятие за нещо[4]. Оксфордският речник я обяснява като *„факти, предоставени или научени за нещо или някого“*; *„съобщено знание относно конкретен факт, предмет или събитие“*[5], т.е. информацията се съобщава на получателя при наличието на някаква конкретност, събитийност. Може да се направи заключението, че информацията пряко се отнася към човешки действия с активен характер, които са насочени към съобщаване на нещо, придаване на форма на нещо посредством словото, за да може да се стигне до твърдението, че *„информационното общество вече функционира“*[6].

[1] Pavlov, G., Poudin, K. (2019). Challenges to information security at regional level. // Trends in Regional Development and Security Management. Sofia: UNWE Publishing Complex, pp. 16–22.
[2] Ibidem.
[3] Семерджиев, Ц. (2007). Управление на информационната сигурност. София: Софттрейд.
[4] Цветкова, М. Внимателна употреба на понятието „информация“. // Медии и обществени комуникации. Достъпно на: https://media-journal.info/?p=item&aid=155.
[5] Oxford English Dictionary. Available on: https://www.oed.com/search/dictionary/?scope=Entries&q=information.
[6] Krztoń, W. (2021). (In)security of the functioning of the information society in the Cyberspace. // Przegląd Europejski. 3, p. 86.

През 1948 г. Винер, основател на кибернетиката, заявява, че *„информацията е информация, а не материя или енергия. Нито един материализъм, който не признава това, не може да оцелее в наши дни”*[7]. Така той въвежда понятието информация в теорията на комуникацията във философията. Следователно, изследователи и философи работят за дефиниране на концепцията за информация в продължение на 60 години. Статистиката показва, че до 1980 г. е имало около 130 дефиниции[8]. Основателят на теорията на информацията, К. Шанън, счита, че е невъзможно да се поставя доверието на една-единствена концепция, тъй като информацията подлежи на всички области на науката и научната дейност[9].

За целите на дисертационния труд авторът използва собствена дефиниция, основана на проучването, а именно, че ***информацията*** **е съвкупност от знания и опит, основани на преки и/или косвени наблюдения за даден обект и/или явления, които водят до субективни и/или обективни умозаключения, основани на факти, доказателства, истинни хипотези. Предава се директно (вербално слово) или индиректно (е-кореспонденция и/или писмена кореспонденция) и води до откриване на нови неща, новини, събития. Най-естественият белег за съществена информация е нейната истинност. Информацията е най-ценният ресурс на новото време и той трябва да има защитеност от злоумишлени атаки и всевъзможни претенции за злоупотреби.**

Според изложеното следва да се направи извода, че информацията е динамична система, която включва отговори на въпроси, за да се постигне потребността от знание.

В Закона за защита на класифицираната информация[10] се постановява водещия принцип *„необходимост да се знае“*, който по презумпция извежда идеята за човека като социално животно[11], което има нужда да съобщава и да му бъде съобщавана някаква новост, новина.

[7] Цит по: Qiao, T. (2011). Definition and Essence of Information. // triple. 9(2), p. 342.
[8] Gang, L. (2007). An inquiry into the origin of the philosophy of information. Beijing: JinCheng Press, p. 71.
[9] Ibidem.
[10] Закон за защита на класифицираната информация. Достъпно на: https://lex.bg/bg/laws/ldoc/2135448577.
[11] Аръндън, Е. (2009). Човекът – „социално животно“. София: Дамян Яков.

Съществуват няколко източника на риск при предаване и получаване на информация[12]:

⇒ загуба на доверие;

⇒ нарушения на сигурността и компютърни престъпления;

⇒ промени в технологиите;

⇒ загуба на ключов персонал;

⇒ повреда на оборудването;

⇒ времева неефективност.

Друга дефиниция за информацията я отвежда като *„елементарен фактор във всички организирани дейности“*[13] и се уточнява, че без информация за текущата ситуация на вземане на решения е трудно да се предприемат стъпки, които да осигурят гаранция за постигане на поставената цел. С други думи, всяко целенасочено действие изисква информация, която да доведе до границата на активната организация. Оценката на всяка решаваща ситуация, т.е. предприемане на действия с конкретна цел, води до всичките проявления на информация.

Информационните и комуникационни технологии са съществени за организациите и хората, за да поддържат високи нива на производителност. Възприемането на тези технологии, идва с множество нови уязвимости и следователно нови заплахи за поверителността и целостта на личните и организационните данни. Експертите, обаче, са съгласни, че хората са най-слабото звено в защитата на системата за информационна сигурност на една организация[14].

Понятието *сигурност* се използва посредством два основни термина – *интерес* и *заплаха*. Първият оформя гледището за осъзната потребност, ценност, която чрез волята за действие, води до задоволяване на потребности. Втората е всичко онова,

[12] Bryson, J. (2016). Managing information services: an innovative approach. Farnham, Surrey, UK: Ashgate, pp. 268–269.
[13] Kwecka, R. (2016). Information in the Area of Security. New Paradigms. // Journal of Defence Resources Management. 7(2), p. 102.
[14] Furnell, S. et al. (2012) Power to the people? The evolving recognition of human aspects of security. // Comput Secur. 31(8), pp. 857–1014.

което пряко или косвено застрашава реализирането на интересите на личността в посока сигурността ù[15].

Според Джоузеф Най сигурността е изключително важен въпрос и може да бъде сравнена с кислорода – не се забелязва, докато не се изгуби[16]. Социалните системи се нуждаят от сериозна сигурност, защото външните заплахи може да доведат до катастрофални последици. Ученият счита, че всяка една социална система притежава специфична култура на сигурност, която именно детерминира отношението към себеподобните и към околната среда[17]. От друга страна, Цветков счита, че категорията *сигурност* е *„сложна и многоаспектна“*[18] и поради този факт се затрудняват опитите да се изведе систематизация на познанието.

Според Павлов термините *информационна сигурност, компютърна сигурност и осигуряване на информацията* имат своята взаимносвързаност, като от тази теоретично-обусловена хипотеза може да се направи заключението, че информацията в XXI век се разглежда в контекста на дигиталните предизвикателства на времето и създаването на мощни системи за противодействие на престъпленията, породени от кибератаки. Гарантирането на националната сигурност може да се случи единствено чрез *„изграждане на еволюционно-развиваща се комплексна информационна система за стратегическо управление“*[19]. Ученият уточнява, че независимо, че тези области на сигурност се използват като синонимни заместители поради общата им цел – защита на информацията, то е неправилно да бъдат тълкувани еднакво, тъй като има съществени различия между тях.

Павлов и Пудин определят информационната сигурност като способност да се осигури *„тайна, цялостност и наличност“*[20], а в историческия си контекст се употребява, за да *„изрази комбинация между „компютърна сигурност“ и „комуникационна сигурност“*[21].

---

[15] Стефанов, Г. (2008). Теория на международната сигурност. София: Сиела, с. 71.
[16] Цит. по Poudin, K. (2018). Developing and Maintaining business Security Culture. // Yearbook of UNWE. 1. Sofia: UNWE, pp. 255–269.
[17] Ibidem.
[18] Цветков, Цв. (2016). Съвременен инструментариум за оценяване на сигурността. // Икономически и социални алтернативи. 2, с. 24.
[19] Павлов, Г. (2010) Цит. съч.
[20] Павлов, Г., Пудин, К. (2011). Информационна сигурност в организацията. София: УИ „Стопанство“, с. 9.
[21] Пак там, с. 8.

По своята същност НС е динамично състояние на обществото, в което са защитени основните права и свободи на българските граждани, държавните граници, териториалната цялост и е гарантирано демократичното функциониране на държавните и гражданските институции с цел запазване и увеличаване на благосъстоянието[22].

Дефинициите на информационна сигурност обикновено се фокусират върху два аспекта. Първият е степента, до която служителите разбират поведението за безопасна информационна сигурност, което често се очертава в политиките, правилата и насоките на тяхната организация[23]. Kruger et al.[24] определят това като степен, до която всеки член на персонала разбира важността на информационна сигурност, нивата, подходящи за организацията и техните индивидуални отговорности за сигурност. Вторият аспект се фокусира върху степента, до която служителите са ангажирани и се държат в съответствие с най-добрите практики, които често се очертават в политиките, правилата и насоките за информационна сигурност[25].

Разработването и успешното внедряване на политика за сигурност, е сложен, многопластов и отговорен процес на национално ниво[26]. Следва да се уточни обстоятелството, че при провеждането на ефективна политика за ИС предварително условие е да се оцени рисковият компонент при вземането на управленски и организационни решения[27].

Терминът „Индустрия 4.0“ е публично представен през 2011 г. на панаира в Хановер[28], като фундамент са следните дефиниции на първите три индустриални революции. Първата индустриална революция е белязана от преход от ръчни производствени методи към машини, задвижвани с пара или вода. Благодарение на

[22] Концепция за национална сигурност на Република България, приета с Решение на 38-о НС от 16. 04. 1998 г., обн., ДВ, бр. 46 от 22. 04. 1998 г. Достъпно на: https://www.strategy.bg/Strategic Documents/View.aspx?lang=bg-BG&Id=655.
[23] Bulgurcu, B. et al. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. // MIS Quart. 34(3), pp. 523-548.
[24] Kruger, H. et al. (2006) A prototype for assessing information security awareness. // Comput Secur. 25(4), pp. 289–296.
[25] Ibidem.
[26] Пудин, К. (2013). Политика за национална сигурност през призмата на мениджърската теория. Наука, образование, сигурност: Юбилейна международна конференция „Десет години образование по сигурност в НБУ“: състояние и перспективи пред обучението в условия на динамична и труднопредвидима среда. София: НБУ, pp. 96–104.
[27] Матеев, М. (2000). Анализ и оценка на риска при избор на инвестиционни решения. София: Стопанство, с. 8.
[28] Vogel-Heuser, B., Hess, D. (2016). Guest editorial: Industry 4.0–prerequisites and visions. // IEEE Trans Autom Sci Eng. 13.

електричеството, Втората индустриална революция, трансформира фабриките в модерни производствени линии, което води до висока производителност и значителен икономически растеж. Третата индустриална революция извежда компютри на полево ниво като програмируем логически контролер и комуникационни технологии в производствения процес, което довежда до автоматизирано производство[29]. В ерата на Индустрия 4.0 производствените системи, под формата на CPPS, могат да вземат интелигентни решения чрез комуникация в реално време и сътрудничество между *„производствени цикли“*[30], което позволява гъвкаво производство на висококачествени персонализирани продукти при масова ефективност[31].

Индустрия 4.0 представлява *„съвкупност от свързани цифрови технологични решения, подпомагащи развитието на автоматизацията, интеграцията и обмена на данни в реално време в производствените процеси.“*[32] и не само – в организационните такива. Тя включва в същността си нови цифрови технологии и голям набор от технологични решения, които създават качествено нов ландшафт на икономически активности.

Най-новите заплахи и предизвикателства пред ИС, каквито са заплахите в киберпространството, се превръщат във фундаментален проблем на днешната епоха. С изискванията, които са изложени в Наредбата за оперативна съвместимост и информационна сигурност[33], се излагат основните законодателни постановки, които определят начините за водене, съхраняване и достъп до регистъра на стандартите, както и методиката за извършване на оценка за съответствие с изискванията по оперативна сигурност. Спазването им се гарантира чрез сертификация на информационните системи и функционалността на единната среда за обмен на електронни документи. Контролът се осъществява от председателя на Държавната агенция за информационни технологии и съобщения.

[29] Xu, X., Lu, Y. et al. (2021). Industry 4.0 and Industry 5.0—Inception, conception and perception. // Journal of Manufacturing Systems. 61, pp. 530–535.
[30] Lu, Y., Xu, X., Wang, L. (2020). Smart manufacturing process and system automation – a critical review of the standards and envisioned scenarios. // J Manuf Syst. 56, pp. 312-325.
[31] Zhong, R., Xu, X., Klotz, E., Newman, S. (2017). Intelligent manufacturing in the context of Industry 4.0: a review. // Engineering. 3(5), pp. 616–630.
[32] Пак там.
[33] МС. Наредба за общите изисквания за оперативна съвместимост и информационна сигурност. Достъпно на: https://www.mtitc.government.bg/sites/default/files/naredba_za_obsite_iziskvaniq_za_mrejova_i_informacionna_ sigurnost_zagl_izm_dv_br_5_ot_2017_g_v_sila_.pdf.

Законът за киберсигурност на Република България[34] урежда организацията, управлението и контрола по киберсигурност, както и предприемането на мерки за постигане на *„високо общо ниво на мрежова и информационна сигурност“*[35]. В Чл. 2, ал. 1 се тълкува определението за киберсигурност, а именно като „*състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат да нарушат работата им.“*[36]. Допълва се, че киберсигурността включва в същността си мрежовата и информационната сигурност, от една страна, а от друга – противодействие на киберпрестъпността и киберотбрана. В Чл. 2, ал. 3 се прилага дефиниция на мрежова и информационна сигурност, а *именно „способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях.“*[37]. Като мерки за безопасност и предотвратяване на потенциални рискове и заплахи, се прилагат организационни, технологични и технически способи с цел минимизиране на рисковите фактори. Посочват се Националната стратегия за киберсигурност, както и Съвета по киберсигурността, който е консултативен и координиращ орган към МС, а като основен орган за справяне и противодействие се назовава министърът на отбраната, който има правомощията по този закон да провежда държавна политика за защита и активни действия срещу кибер- и хибридни атаки посредством изграждането и развиването на киберотбрана.

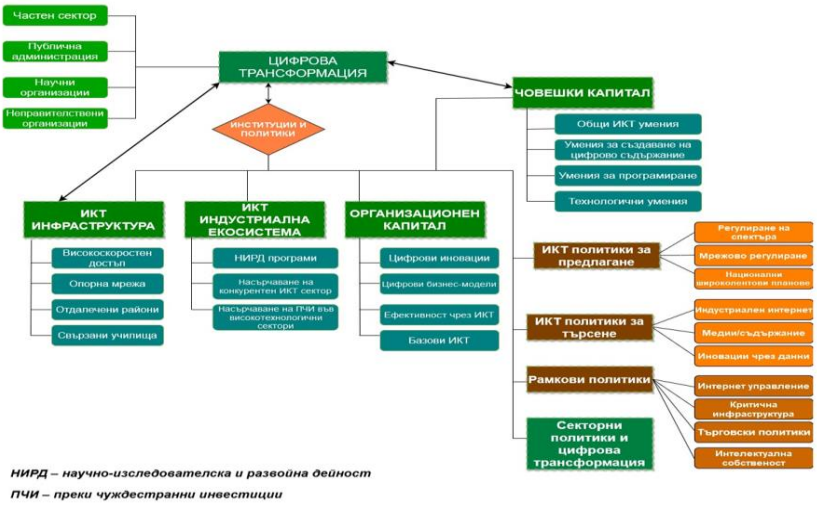
ISO/IEC 27001 е стандарт за ИС, като в него се дефинират изискванията, свързани с управлението на сигурността на данните и информацията, киберсигурността и защитата на поверителността. Приемането на система за управление на информационната сигурност, е стратегическо решение за една организация. Създаването и внедряването на система за управление на информационната сигурност на организацията, се влияе от нуждите и целите на организацията, изискванията за

[34] Закон за киберсигурност. Достъпно на: https://lex.bg/bg/laws/ldoc/2137188253.
[35] Пак там.
[36] Пак там.
[37] Пак, там.

сигурност, използваните организационни процеси, размера и структурата на организацията. Всички тези фактори се очаква да се променят с времето.

Системата за управление на информационната сигурност запазва поверителността, целостта и достъпността на информацията чрез прилагане на процес за управление на риска и дава увереност на заинтересованите страни, че рисковете се управляват адекватно. Важно е СУИС да е част от и да е интегрирана с процесите на организацията и цялостната структура на управление и че информационната сигурност се взема предвид при проектирането на процеси, информационни системи и контроли[38].

В точка 2.1. „Висшето образование като обект на информационна сигурност“ се изреждат различни закони и наредби, които регламентират устройството, функциите, управлението, достъпа до сигурността. Извежда се дефиниция на цифровата трансформация като *„процес, характеризиращ се с повсеместно внедряване и комбиниране на цифрови технологии във всички сфери на обществения и стопански живот.“*[39].



Фигура 1
Цифрова трансформация
Източник: Strategy.bg

[38] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Available on: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en.

[39] Цифрова трансформация на България за периода 2024-2030 г. Достъпно на: https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1661.

В ход е Програмата „Цифрова Европа“, която е насочена към предоставянето на цифрови технологии в отговор на предизвикателствата на съвременния свят[40]. Чрез нея се разкриват нови възможности, насърчава се разработването на надеждни технологии, подкрепя се изграждането на едно отворено демократично общество. Основава се на трите стълба за цифрова икономика и цифрова трансформация[41]:

⇒ **технологии в услуга на хората** – инвестиции в разгръщане на цифрови умения; защита от кибератаки; изкуствен интелект и разработването му в контекста на правата на човека; въвеждане на високоскоростен интернет; разширяване капацитета на суперкомпютрите;

⇒ **справедлива и конкурентоспособна цифрова икономика** – достъп до иновации и динамични общности; отговорност на онлайн платформите; гарантиране пригодността на правилата на онлайн услуги, лоялната конкуренция; повишаване достъпа до висококачествени данни;

⇒ **открито, демократично и устойчиво общество** – използване на технологиите с цел намаляване на въглеродните емисии в цифровия сектор; възможности на гражданите за контрол на данните им; създаване на пространство за здравни данни; борба срещу дезинформацията.

Изграждането на информационна система във висшето образование, се подчинява на политиката по мрежова и информационна сигурност. По този начин информационната сигурност се приобщава към принципите и ценностите, културата и традициите на Република България. От друга страна, изграждането на електронна визия в уебпространството на дадена организация (ВУЗ), изцяло трябва да е съобразена с архитектурата на учебното заведение[42]. Най-ефективна е т.нар. *комплексна система*, която се състои както от осигуряване на защита на устройствата, така и на защита от грешки на самите потребители[43].

[40] Програма „Цифрова Европа“. Достъпно на: https://digital-strategy.ec.europa.eu/bg/activities/digital-programme.
[41] ЕК. Изграждане на цифровото бъдеще на Европа. Достъпно на: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_bg.
[42] Димов, П. и др. (2021). Здравков, З., Добрева, Х. (2021). Информационна сигурност. София: ВА „Георги Раковски“, с. 150.
[43] Пак там.

Правят се изводи от първа глава, като се набляга върху това, че сигурността винаги е една от най-важните цели и потребности на индивида, обществото и държавата като цяло. Формирането и развитието на човешката цивилизация винаги е било свързано с премахването на различни заплахи, причинени от природата, обществото, враждебните страни, технологичните съоръжения и т.н. С други думи, сигурността е едно от най-важните условия за съществуването и развитието на обществото и държавата. Понятието „безопасност“ е използвано за първи път през 1190 г. като *„тихо състояние на човешкия дух, в което се чувства в безопасност от всякакви опасности“*[44].

[44] Sidorkin, A., Iroshnikov, D. (2019). Theoretical issues of "security" concept. // Journal of Politics and Law. 3(12), pp. 34–39.

ВТОРА ГЛАВА.

АНАЛИЗ НА СЪСТОЯНИЕТО НА ИНФОРМАЦИОННАТА СИГУРНОСТ ВЪВ ВИСШЕТО ОБРАЗОВАНИЕ

В точка 2.1. „Методологически инструментариум за защита на информацията във висшето образование“ се разглеждат видовете сигурност, като се отбелязва, че през 2018 г., когато GDPR влиза в сила[45], предизвиква различни реакции в общността на висшето образование. Организациите натрупват големи количества информация по-бързо от всякога. Чрез технологиите могат да използват тези обеми от данни, за да подобрят ефективността и да осигурят по-информирани възможности за вземане на решения. Тази нарастваща зависимост от ИТ въведе различни предимства, но също така означава допълнителни рискове.

Защитата на технологичната инфраструктура на лица и организации е важна. В тази връзка се използват технологии за информационна сигурност и киберсигурност. Информационната сигурност защитава информацията на организациите от неразрешено модифициране, прекъсване, проверка и разкриване[46]. Тази информация може да бъде под каквато и да е кибер- или друга форма. ИКТ и практиките за сигурност се занимават конкретно със защитата на цифровата инфраструктура на организациите, за да помогнат за смекчаване и предотвратяване на заплахите[47].

Въведени са инструменти и техники за сигурност на ИКТ за защита на цифровите активи и инфраструктури[48]. Изследванията за това и приемането в организациите обикновено са казуси, специфични за организацията.

Институциите за висше образование (ВУЗ) са силно дигитализирани през XXI век, разчитайки на технологиите, за да управляват своите огромни количества

[45] Общ регламент за защита на данните. Достъпно на: https://gdprinfo.eu/bg.
[46] Magomelo, M., Mamboko, P., Tsokota, T. (2014). The Status of Information Security Governance within State Universities in Zimbabwe. // Journal of Emerging Trends in Computing and Information Sciences. 5(8), pp. 710–727.
[47] Anderson, D., Abiodun, O., Christo□els, A. (2020). Information security at South African universities – implications for biomedical research. // Int. Data Priv. Law. 10(2), pp. 180–186.
[48] Eze, T., Aroh, C. (2020). Management of Information Security in Public Universities in Nigeria. // Int. J. Digit. Soc. 11(1), pp. 1575–1578.

информация[49]. Компютърната инфраструктура и мрежи са въведени в помощ на студентите, преподавателите и служителите в работата на институциите.

На Фигура 2 са категоризирани заплахите според уязвимия субект на организациите.

Фигура 2
Категоризация на ИКТ инструменти за сигурност и техники
Източник: авторска интерпретация

Организационната сигурност се справя със заплахите, произтичащи от уязвимости в управлението на човешки и цифрови активи от ВУЗ. Човешките рискове също са основен фактор, допринасящ за сигурността на организацията. Това е особено вярно за ВУЗ-овете, които в много страни са с хронично недофинансиране, особено в спомагателни/подкрепящи сектори като ИТ. Освен това, даден факултет обикновено има по-възрастни служители, за които познанията по ИТ не се усвояват лесно. Неправилното управление на достъпа на персонала може да изложи организацията на риск от вътрешни заплахи. Персоналът с малко обучение и осведоменост относно практиките за сигурност също се счита за риск за ИКТ инфраструктурата за сигурност на организацията. Сред рисковите фактори, човешкият фактор, се счита за най-слабото звено[50].

Технологичната сигурност се занимава със заплахи, които произтичат от уязвимости в приложението, софтуера и мрежовите системи, които организацията

[49] Makupi, D. (2019). A Design of Information Security Maturity Model for Universities Based on ISO 27001. // Int. J. Bus. Manag. 7(6).
[50] Amigud, A., Arnedo-Moreno, J., Daradoumis, T. et al. (2018). An Integrative Review of Security and Integrity Strategies in an Academic Environment: Current Understanding and Emerging Perspectives. // Comput. Secur. 76, pp. 50–70.

използва. Заплахите в мрежата възникват от уязвимости, вкоренени във взаимосвързани устройства, особено тези, свързани с интернет. Неправилно конфигурираните мрежи и сървъри могат да осигурят на нападателя неоторизиран достъп до компютрите и базите данни на институцията[51]. Тези заплахи могат да идват под формата на наводнение, пожар, земетресения, кражби, грабежи и физически щети[52].

Физическа сигурност. Използването на следните мерки за предотвратяване на физическо увреждане на киберинфраструктурата на ВУЗ се постига чрез[53]:

⇒ контрол на температурата;

⇒ системи за ранно предупреждение за бедствия.

Физическата сигурност на класифицираната информация включва система от мерки, начини и средства за предотвратяване на неоторизиран достъп до материали, документи, техника и оборудване, класифицирани като държавна или служебна тайна. Системата е част от общите изисквания за сигурност по защита на класифицираната информация и включва общи и специфични мерки.

Стандарти и рамки. ВУЗ-овете използват стандартизирани рамки за киберсигурност с цел защита на своята киберинфраструктура.

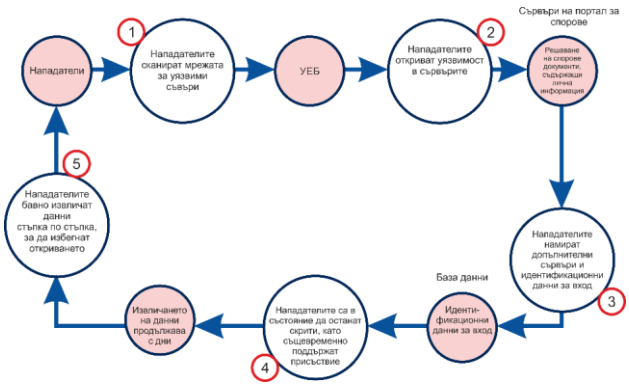
Мерките, които се предприемат и които са продиктувани от нарушаване на достъпа на информация, са:

1) **Мониторинг на организацията** – трябва да се извършва както чрез редовен надзор от ръководството, така и чрез използване на инструменти. Регистрационни файлове от операционни системи, приложения и мрежови устройства трябва редовно да се преглеждат за аномалии и могат да помогнат за идентифициране на злонамерени атаки срещу системи.

[51] Patten, K., Harris, M. (2013). The Need to Address Mobile Device Security in the Higher Education IT Curriculum. // Journal of Information Systems Education. 24(1), pp. 41–52.
[52] Huang, Z. (2021). An Analysis of Information Security and Protection Strategies in Colleges and Universities in the Environment of Smart Campuses. // J. Phys. Conf. Ser. 1852(4).
[53] Singh, V., Margam, M. (2018). Information Security Measures of Libraries of Central Universities of Delhi: A Study. // DESIDOC J. Libr. Inf. Technol. 38(2), p. 102.

2) **План за управление на набор от данни** – това позволява на организацията да реагира бързо и адекватно чрез систематичен подход на управление на нарушенията. По този начин служителите, които пряко отговарят за ресора, се насърчават да действат проактивно, като разработват и внедряват стабилно управление.

3) **Извършване на оценка за нарушение на данните** – при настъпване на нарушение организацията е задължена да предприеме разумни, адекватни и експедитивни действия и преценка за това дали кризисната ситуация подлежи на уведомяване, съгласно ЗЗЛД. Всяко неразумно забавяне при нарушаване на сигурността на информацията може да струва много за организацията.



Фигура 3
Модел на хакерска атака при пробив и кражба на лични данни
Източник: Адаптирано по: GAO, Equifax[54]

Предотвратяването на неоторизиран достъп, изисква цялостен подход, който съчетава няколко стратегии[55]:

1. Политика за силни пароли – един от най-основните, но ефективни начини за предотвратяване на неоторизиран достъп, е прилагането на политика за силна парола. Това включва изискване потребителите/служителите да създават сложни пароли, които са трудни за разпознаване, и налагане на редовни промени. Силната парола трябва да е дълга поне осем знака и да включва комбинация от главни и малки букви, цифри и

[54] GAO. Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. Available on: https://www.gao.gov/products/gao-18-559.
[55] Sammons, J., Cross, M. (2015). The Basics of Cyber Safety. Elsevier Inc. pp. 75–86; 117–137.

специални знаци. Също така, не трябва да съдържа лесна за отгатване информация, като: име на потребителя, дата на раждане или често срещани думи.

2. Двуфакторна автентификация и многофакторна автентификация – друга ефективна стратегия е използването на 2FA и MFA. Първото изисква потребителите да предоставят два различни вида идентификация за достъп до система. Това може да бъде например парола и код, изпратени до мобилния телефон на потребителя. Второто, от друга страна, включва използването на три или повече фактора за удостоверяване. Те могат да съчетават нещо, което потребителят знае (напр. парола), нещо, което потребителят има (напр. токен за сигурност) и нещо, което потребителят е (напр. пръстов отпечатък).

3. Мониторинг на потребителската активност – наблюдението е друга важна стратегия за предотвратяване на неоторизиран достъп. Това включва следене какво потребителите правят в системите и мрежите, както и следене за всякакви необичайни дейности. По този начин може да се открият потенциални пробиви в сигурността и да се предприемат необходимите действия, преди да бъдат нанесени сериозни щети.

4. Внедряване защита на крайната точка – стратегия, която се фокусира върху защитата на всяка крайна точка или потребителско устройство в мрежа, за да се предотврати неоторизиран достъп. Това може да включва лаптопи, настолни компютри, мобилни телефони, таблети и всякакви други устройства, които се свързват към мрежа. Мерките за сигурност на крайната точка могат да включват антивирусен софтуер от следващо поколение, защитни стени и системи за откриване на проникване. Те могат също да включват политики, които ограничават използването на сменяеми носители като USB устройства, които могат да се използват за въвеждане на зловреден софтуер или кражба на данни.

5. Редовни софтуерни актуализации и управление на корекции – друга важна стратегия за предотвратяване на неоторизиран достъп. Софтуерните актуализации често включват подобрения в сигурността, които коригират уязвимости, които могат да бъдат използвани от хакери.

Подходите и методите за сравнение могат да бъдат качествени и количествени.

Използваната методология се основава на презумпцията за изпълнимост на заложените цел и задачи на дисертационния труд. В своята същина той се поделя на анкетно проучване и разработване на концептуален модел за ограничаване на заплахите и уязвимостите на информационната сигурност.

При анкетното проучване се извежда спецификата, като се изграждат основни блокове въпроси. Извеждат се предимствата и недостатъците на анкетния метод, като в дисертационния труд се извършва анкетно проучване сред 56 български граждани, работещи в сектора на висшето образование (български университети) и участващи на доброволен принцип, за да се установи състоянието на информационната сигурност, както и да се оценят възможностите за внедряване на нова, по-добра система за управление на сигурността. Проучването на експертното мнение следва да се проведе чрез пряка анкета (онлайн чрез Google Forms), тъй като този метод предполага бързо набавяне на разнообразна информация. Споменават се обект, предмет, методи на проведеното проучване.

Изводите, които се правят във втора галва, са свързани с изграждане на методологическата рамка и нейния инструментариум на проведените проучвания. Съсредоточава се върху видовете сигурност на информацията, като се прави сравнителен анализ.

ТРЕТА ГЛАВА.

РЕЗУЛТАТИ И ИЗГРАЖДАНЕ НА КОНЦЕПТУАЛЕН МОДЕЛ ЗА ПОДОБРЯВАНЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ ВЪВ ВИСШЕТО ОБРАЗОВАНИЕ

В точка 3.1. „Анализ на резултатите от проведено анкетно изследване“ се внася важното уточнение, че анкетното проучване се провежда, за да се удостовери и верифицира необходимостта от представяне на Модел за информационна сигурност. Без да се направи допитване до специалисти – университетски преподаватели и служители в университетите, няма да има възможност да се представи достоверността и валидността на желанието за нов модел. Това е нужна необходимост, за да може дисертационният труд да представи съвременна гледна точка на работещите в сектора на висшето образование. Анкетното проучване се съобразява с мнението на анкетираните респонденти и черпи ресурси за проектирането на Модела.

Въпросите са групирани на три основни принципа – демографски характеристики, професионални характеристики и лично мнение, структурирани в три основни блока: свързани с персонална информация; свързани с качеството на системата за ИС и свързани с компетентностите на служителите, като тук се обръща внимание на конкретните въпроси, свързани с удовлетвореността на служителите от информационната сигурност в тяхната месторабота.

На въпрос № 6 *Спокоен/Спокойна ли сте за информационната си сигурност и за сигурността във Вашата организация?* 62.5% отговарят с „Да, може да се каже“, а 32.1% утвърдително с „Да, напълно съм спокоен/спокойна“. Останалите проценти са разпределени между отговорите „По-скоро не съм спокоен/спокойна“ (3.4%) и „Не, изобщо не съм спокоен/спокойна“ (2%). Може да се направи извода, че в по-голямата си численост респондентите са по-скоро спокойни за своята сигурност, отколкото не или изобщо. Това довежда до предпоставката, че системите за информационна сигурност са достатъчно ефективни, за да се справят с предизвикателствата на съвремието. При възможен отговор „Не мога да преценя“ няма респонденти, които да

са дали този вид отговор, което показва тяхното усещане за сигурност в организацията, която представляват.

Фигура 4
Въпрос: Спокоен/Спокойна ли сте за информационната си сигурност и за сигурността във Вашата организация?

На въпрос № 7 *Според Вас на какво предимно се дължат различните пробиви и проблеми с информационната сигурност?* 57.1% отговарят, че човешка грешка е в основата на пропускливостта на ИС, което твърдение теоретично се изведе като верифицирано в първа и втора глава на дисертацията. 30.4% считат, че проблемът е в слабости в системата, а 10.7% - на все по-добри хакери. Анкетирани, които да са отбелязали отговор „Не мога да преценя“, са 1,8%. Няма респонденти, които да са отбелязали отговор „на различни и разноречиви указания към административния персонал“. Въпросът има за цел да проследи професионалното и общочовешко мнение на работещите в организацията, като на преден план излиза човешката грешка, като причинител на пропускливост в системата и на зловредни атаки. В одитен доклад на ЕС относно киберсигурността се счита, че многобройните видове заплахи се класифицират според начина, по който се борави с данните – разгласяване, модифициране, унищожаване или отказ от достъп[56]. Извеждат се и видовете кибератаки, например: малуер, софтуер за изнудване, тип „отказ от обслужване“, уеббазирани атаки, като комплексните устойчиви атаки са класифицирани, като *„най-злонамереният вид*

[56] Одитен сборник. Киберсигурност в ЕС и неговите държави членки. Одитни доклади, публикувани през периода 2014 – 2020 г. ЕС. Достъпно на: https://www.eca.europa.eu/sites/CC/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_BG.pdf, с. 11.

заплахи"[57]. Човешката грешка се състои най-вече в неправилен избор на парола, случайно разкриване на информация и използване на неподходящ или вече остарял софтуер[58]. Именно случайните заплахи възникват, когато служителят няма достатъчни познания относно системите за сигурност, неправилна конфигурация, както и при изтичане на информация поради незащитеност при трансфер на данни[59].

Фигура 5
Въпрос: Според Вас на какво предимно се дължат различните пробиви и проблеми с ИС?

На въпрос № 8 *Колко често Ви се е случвало да има срив в информационната система, докато упражнявате своите работни дейности?* 66.1% отговарят с твърдението, че не се е случвало скоро в рамките на година. 19.6% изразяват мнение, че никога не им се е случвало да стават непосредствени свидетели и/или потърпевши от срив в системата, което да попречи на упражняване на техните професионални дейности. 10.7% са на мнение, че не много често стават свидетели в рамките на веднъж до няколко месеца. 3.6% споделят, че често попадат в такава ситуация в период от един-два пъти месечно. Анкетираните изцяло изключват отговора „много често (веднъж седмично)". От така изнесените резултати може да се направи извода, че има спорадични сривове на информационната система по време на упражняване на работни дейности на служителите, но като цяло не са чести тези прояви на слабости в системата, което е обнадеждаващ фактор за сигурността, качеството и ефективността на ИС в организациите на висшите учебни заведения. Процентът на респондентите,

[57] Пак там, с. 13.
[58] Стоицов, Г. (2020). Информационна и комуникационна сигурност. ПУ „Паисий Хилендарски", с. 15.
[59] Пак там.

които споделят, че често попадат на такъв тип ситуации, не трябва да бъде подценяван, тъй като е важна отговорност на съответната организация да предприеме стриктни, съобразителни и сериозни мерки спрямо качеството на изпълнение на системата за ИС.

Фигура 6
Въпрос: Колко често Ви се е случвало да има срив в информационната система, докато упражнявате своите работни дейности?

На въпрос № 9 *По кой канал най-често получавате информация, за да може да извършвате ежедневните си работни задължения?* 53.6% отговарят, че най-предпочитаното средство за тях е запитването по e-mail, а на другата крайност, т.е. с най-малко събрани отговори е предпочитанието за писмено запитване на хартиен носител (7.1%), което оформя оста дигитален – книжен вариант. В съвременното общество информацията, като ценен ресурс, е най-подходяща и бърза за доставяне посредством интернет разнообразни канали. Също така не трябва да се пренебрегва и факта, че природата и нейното опазване зависят от рутинните дейности на човека и начина, по който той влага усилия, за да я опази. 17.9% от респондентите посочват интернет страницата на висшето учебно заведение, а с равен брой проценти от 10.7% са отговорили работещите, които желаят да получават бърза и навременна информация посредством различни социални интернет канали и телефон.

Всеизвестно е, а и в анкетата се потвърждава, че имейла е една от най-популярните форми на комуникация, която хората използват, но е и една от най-злоупотребяваните такива. В края на миналата година Sinch Mailgun[60] анкетира повече

[60] Email. Key takeaways from Sinch Mailgun's Email and the customer experience 2024. Available on: https://www.mailgun.com/blog/email/email-cx-key-takeaways/.

от 2000 потребители в САЩ, Великобритания, Франция, Германия и Испания, за да разбере как предпочитат да кореспондират и взаимодействат, както и какво ги мотивира да се ангажират с имейл комуникации. Най-ясната констатация в този доклад е, че имейлът е най-предпочитаният начин. Това важи както за маркетингови кампании например, така и за транзакционна комуникация. 75,4% от потребителите са избрали имейл кутията като предпочитан канал за съобщения, докато 74% са го направили за транзакционни известия.

Друго проучване (The Digital Everyday Life in Finland 2022) показва, че гъвкавостта и историята на съобщенията са основните причини за популярността на имейла. Хората са готови да изчакат няколко работни дни за отговор, но не повече, преди да преминат към друг комуникационен канал[61].

В XXI век длъжността анализатор по информационна сигурност става все по-търсена. Длъжностната характеристика се окончава в това да защитава компютърните мрежи, системите и базите данни на организацията от кибератаки и пробиви на данни. По-конкретно включва[62]:

- ⇒ откриване, наблюдение и посредничество в различни аспекти на сигурността – включително физическа сигурност, софтуерна сигурност и мрежова сигурност;
- ⇒ извършване на тестове за контрол на съответствието;
- ⇒ разработване на препоръки и програми за обучение за минимизиране на рисковете за сигурността в компанията;
- ⇒ създаване на яснота относно развиващите се заплахи в пространството на киберсигурността чрез комуникация с външни източници;
- ⇒ сътрудничество с други екипи и ръководството в организацията за прилагане на най-добрите практики за сигурност

[61] Liikkanen, L., Monto, E., Nisula, N. Why is email still the preferred daily communication method for older generations? Available on: https://qvik.com/news/why-is-email-still-the-preferred-daily-communication-method-for-older-generations/.
[62] Force, J. (2020). Security and Privacy Controls for Information Systems and Organizations. U.S. Department of Commerce: National Institute of Standards and Technology.

Анализатори по информационна сигурност са необходими в организации, които съхраняват чувствителни данни и информация, в т.ч. сектора на образование.

Фигура 7
Въпрос: Според Вас знанията и компетентностите на обслужващия и административния персонал на достатъчно високо ниво ли са спрямо предприемане на адекватни действия за предотвратяване на рискови ситуации, свързани с информационната сигурност?

На въпрос № 11 *През последната една година посещавали ли сте курсове, семинари за квалификация относно възникване на рискови ситуации, свързани с информационната сигурност в работна среда?* 89.3% изразяват отрицателно мнение по зададения въпрос, а 10.7% споделят, че са посещавали подобни мероприятия. Това води до преосмислянето на стратегиите в университетите относно тяхната информационна сигурност. Без квалифициран и добре обучен персонал, който да реагира максимално адекватно на злоумишлени действия, нивото на сигурност рязко се понижава и отива в пейоративното осмисляне на това доколко се инвестира в полезност на действията и в квалификация на служителите. Ежегодно се появяват нови източници на заплахи и единствено добре запознатите професионалисти, специалистите по киберсигурност, IT специалистите могат да допринесат за обучението на работещите в сферата на висшето образование служители. Различни курсове и семинари, срещи и беседи спомагат за повишаване нивото на информираност, което довежда до благополучие на цялата организация.

Служителите се нуждаят от причина да се грижат за сигурността. Обучението трябва да съобщи на организацията бизнес стойността на най-добрите практики за сигурност: какво позволява самото обучение, осигурява приходи или защитава активи и

репутация. Хората ще бъдат по-склонни да вземат внимателно решения за сигурността, когато имат чувство за лична отговорност и гледат на сигурността, като на важна за ежедневния им живот. Следователно, обучението за осведоменост относно сигурността трябва да показва връзката между сигурността и задълженията на всички роли в организацията, от персонала на първа линия до висшите ръководители[63].

Фигура 8
През последната една година посещавали ли сте курсове, семинари за квалификация относно възникване на рискови ситуации, свързани с информационната сигурност в работна среда?

На въпрос № 12 *При възникване на инцидент, свързан с информационната сигурност, Вие първо ще:* 92.9% от запитаните отговарят единодушно, че ще уведомят свой колега, който пряко отговаря за информационното обслужване. 3,5% са на мнение, че ще предприемат действия в посока уведомяване на дирекцията за киберпрестъпност към ГДБОП или ще запазят спокойствие и ще се опитат да се справят сами. Без процентно съотношение е оставен отговорът *„ще уведомите Държавната агенция за национална сигурност“*.

[63] Ibidem.

Фигура 9
Въпрос: При възникване на инцидент, свързан с информационната сигурност, Вие първо ще:

На въпрос № 13 *Според Вас системата за информационна сигурност във висшето учебно заведение, в което работите, ефективна ли е?* 67.9% отговарят, че по-скоро е ефективна, отколкото не е, а 26.8% изразяват убедително положително мнение. Може да се направи извода, че служителите са на единодушно мнение, че системата за информационна сигурност е ефективна.

Фигура 9
Въпрос: Според Вас системата за информационна сигурност във висшето учебно заведение, в което работите, ефективна ли е?

На въпрос № 14 *Според Вас личните Ви данни защитени ли са добре в институцията, в която работите?* 58.9% отговарят с „Да, може да се каже“, а 26.8% - „Да, напълно“. Тези резултати оформят усещането за сигурност в организацията, което спомага работещите в нея да се чувстват защитени и да изпълняват качествено своите

професионални отговорности. Пропорционално по 6% получават отговорите „По-скоро не“ и „Не мога да преценя“, а 2.3% от запитаните са на мнение, че изобщо нямат усещането, че личните им данни са защитени.

Фигура 10
Според Вас личните Ви данни защитени ли са добре в институцията, в която работите?

На въпрос № 15 *По Ваше лично мнение, чувствате ли се защитен/защитена от атаки, извършвани в интернет пространството и нарушаващи личните данни и права на потребителите?* 66.1% отговарят с „Да, може да се каже“, а 21.4% - „Да, напълно“, което спомага да се разбере нивото на сигурност в организацията. Служителите се чувстват защитени от зловредни атаки, които имат за цел да нарушат личните данни и правата на потребителите. 7,5% от запитаните са на диаметрално противоположни позиции, като категорично застават зад мнението, че изобщо не се чувстват защитени. 4% не могат да преценят, а 1% отбелязват за отговор „По-скоро не“.

Фигура 11
По Ваше лично мнение, чувствате ли се защитен/защитена от атаки, извършвани в интернет пространството и нарушаващи личните данни и права на потребителите?

На въпрос № 16 *Моля да споделите Вашето мнение относно информационната сигурност във висшето учебно заведение, в което работите*. се предоставя възможност на респондентите да изразят своето свободно мнение относно информационната сигурност в организацията, която представляват. Част от отговорите се групират в спрямо приблизително еднакви отговори, които включват: задоволително ниво (5,4%), добро ниво (8,9%), високо ниво (21,4%), ефективна (5,4%), предприети са нужните мерки (16,1%). От така изведените преобладаващи резултати следва изводът, че работещите във висше учебно заведение считат системата за информационна сигурност за надеждна и качествена.

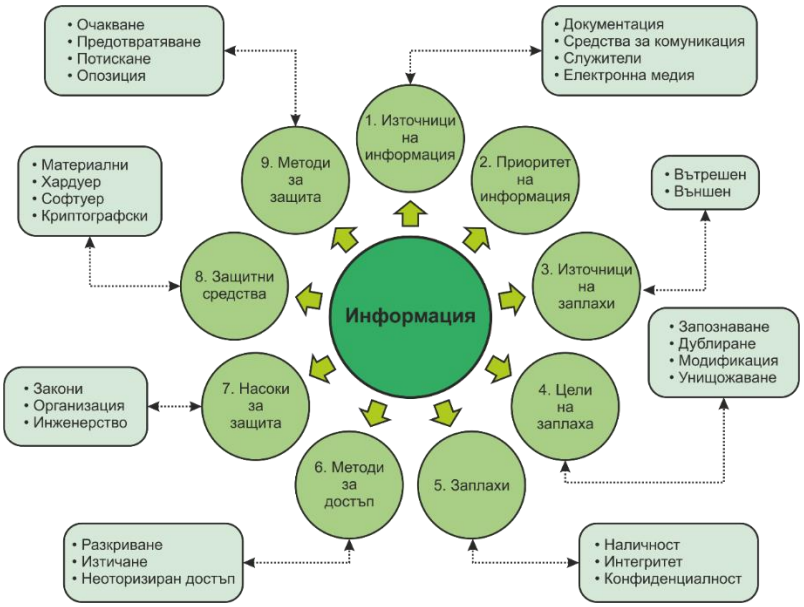
Фигура 12
Моля да споделите Вашето мнение относно информационната сигурност във висшето учебно заведение, в което работите.

В свободен текст се прилагат останалите отговори, които са много интересни по своята същност: *„С много резерви и възможности за подобрения!“; „Има постигнато ниво на сигурност, но са чести проблемите с по-ниска степен на критична опасност“; „Предвид липсата на сериозни ситуации, свързани със сигурността, считам, че нивото е сравнително добро“; „Нивото отговаря на съвременните условия, но се изисква по-голяма квалификация на експертите за защита на информацията“; „Има нужда от надграждане с по-модерни защитни системи“; „В университета, в който работя, съществува непрекъснат стремеж към повишаване на информационната сигурност, въпреки че и към момента тя е на много добро ниво. Подкрепям мерките, които са свързани с повишаване информираността на служителите. През 2023 и 2024 г. в рамките на един ден всички заети можеха да се информират относно политиката на университета по отношение на киберсигурността.“; „Оценявам я като много надеждна“; „Нямам притеснения относно информационната сигурност. Считам, че са взети нужните мерки, за да бъде тя гарантирана.“.*

В така формулираните отговори може да се обобщи следното, че подобренията на информационните системи, повишаването на сигурността, допълнителните курсове за квалификация на служителите в тази насока, мерките, които всеки университет предприема за киберсигурността си, са от решаващо значение за ефективността на

информационните системи[64]. Оттук се извежда и теоретичното схващане, че киберсигурността е отражение на поддържането на активни и превантивни мерки в киберпространството, чието ниво се дължи на конфиденциалността, интегритета, достъпността и належащите ресурси[65].

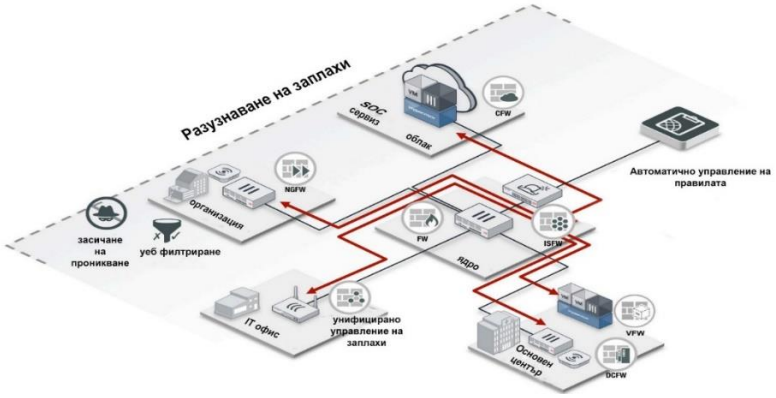
В следващата част на изследването се създава концептуален модел за ограничаване на уязвимостите и заплахите на информационната сигурност в университетите. Прилагат се критерии, показатели и компоненти. Поетапно се онагледява всеки компонент от изведените критерии.



Фигура 13
Имплементиране на концепция за информационна сигурност към Модела
Източник: авторова интерпретация

Извежда се структурата за сигурност, която може да помогне на ВУЗ да се справи с предизвикателства в сътрудничество със собствения си административен и ИТ персонал.

[64] Полимирова, Д., Шаламанов, В., Стоянов, Н, Тагарев, Т. и др. (2019). Киберсигурност и възможности за приложение на иновативни технологии в работата на държавната администрация в България. Институт за публична администрация.
[65] Edgar, T., Manz, D. (2017). Research Methods for Cyber Security. Elsevier Inc.



Фигура 14
Структура на сигурност на Модела
Източник: авторова интерпретация

Състои се от:

1. Защитна стена от следващо поколение (NGFW) – част от третото поколение технология за защитна стена, комбинираща конвенционална защитна стена с други функции за филтриране на мрежови устройства, като например защитна стена на приложения, използваща дълбока инспекция на пакети (DPI), система за предотвратяване на проникване (IPS). Могат да се използват и други техники като TLS-криптирана проверка на трафика, филтриране на уебсайтове, QoS/управление на честотната лента, антивирусна проверка, интегриране на управление на идентичността на трети страни (напр. LDAP, RADIUS, Active Directory) и SSL декриптиране.
2. Персонализираният фърмуер, или пространството за приложения (CFW) се превръщат в стратегически императив за мнозина, тъй като организациите се стремят да решат критичния недостиг на работна ръка, пропуските в уменията и проблемите със задържането в операциите на първа линия. Доказано е, че технологията, позволяваща CFW, помага на организациите да се справят с предизвикателствата на работната сила на първа линия, като същевременно оптимизира оперативната производителност в аспектите на безопасност, качество и производителност.
3. Фърмуер (FW) – проектиран да бъде интерфейсът между хардуера и софтуера на компютъра. Той абстрахира много от ниско ниво, специфични за хардуера подробности за това как работи компютърът, което улеснява разработването на софтуер и стартирането на същия софтуер на множество системи. Внедряването

му осигурява редица предимства като: доверие от партньорите, служителите, заинтересованите страни (преподаватели, студенти, персонал); конкурентно предимство; интегрирана сигурност.

4. Вътрешната защитна стена за сегментиране (ISFW) е предназначена да защитава мрежовите сегменти от злонамерен код, който си проправя път към вътрешната мрежа. Архитектурата ISFW осигурява максимална производителност и максимална сигурност, като същевременно предлага гъвкавостта да бъде поставен навсякъде в организацията.
5. Virtual Firewall (VFW) е проектиран да отговори на уникалните нужди за сигурност на съвременните виртуализирани инфраструктури. Виртуалната защитна стена контролира достъпа до подмрежи и поддържа разрешаващи правила и отказващи правила за обслужване на клиенти. Клиентът сам може да добавя правила, когато има нужда, като VFW определя дали пакетите с данни могат да преминават към или извън подмрежите.
6. Защитна стена на центъра за данни (DCFW) – описва работата, извършвана от пълния спектър от киберработната сила, като има за цел да предпази центровете за данни от напреднали заплахи, като гарантира защитата на чувствителна информация и критични приложения.

Основните критерии, към които трябва да се придържа Моделът, са да се съобразява с източника, произхода, характера, времето и намерението на извършителя на заплахата.

Таблица 1
Видове заплахи за информационната сигурност

Критерии				
Източник	**Произход**	**Характер**	**Време**	**Намерение**
Вътрешен Външен	Естествен Социален (включва човешко поведение)	Икономически Политически Финансови Демографски	Временни Периодични Перманентни	Случайно Умишлено

Източник: Pavlov & Poudin[66]

[66] Pavlov, G., Poudin, K. (2019). Challenges to information security at regional level. // Trends in Regional Development and Security Management, pp. 16–22.

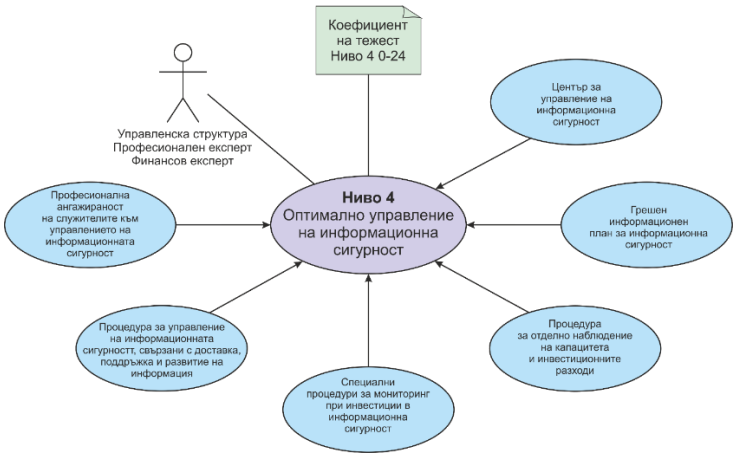
В зависимост от контекста на приложението на информационна сигурност има различни нива на устойчивост, развитие и функциониране на самото управление на информационната сигурност, но обичайно е, че нивата на устойчивост и функциониране са представени с числена стойност, която отразява текущото състояние на организация на наблюдаваната система. Общата характеристика е, че те се основават на шест нива на развитие и функциониране на процесите и зависи от това коя управленска рамка се прилага[67].

Фигура 15
Нива на развитие на технологията COBIT
Източник: Sikman et al. (2023)

Технологията на развитие и функциониране на ИС представлява рамка, която за всяко от съществуващите нива на развитие се изброяват подробно дейностите, които се извършват в него.

При създаване модел за управление на информационната сигурност във висшето образование, цялата система на елементите е първоначално зададена на всички нива. Когато се определи кои елементи да се използват, тогава се вземат предвид всички аспекти на нивото, които са необходими за идентификация и които съдържат всички необходими мерки за определяне на сигурността на информационната система.

[67] Sikman, L. et al. (2023). A model of sustainable information security management system in higher education institutions. // Journal of Physics: Conference Series. 2540, p. 3.



Фигура 16
Диаграма на оптимално управление на процесите на информационна сигурност
Източник: авторова интерпретация

Технологията на модела се извежда в оптималния вариант на диаграмата. На тази фигура е представена съкратена версия на технологията на модела в зависимост от неговата оптималност и целесъобразност.

Изброяват се необходимите инвестиции, които са нужни за подобряване на ИС в сектора на висшето образование: инвестиране в хора; инвестиране в процеси; инвестиране в софтуер.

Очакваните ползи от внедряването на модела за подобряване на информационната сигурност във висшето образование са от изключително естество за опазване сигурността на институцията. От една страна, е предназначен да укрепи организацията срещу киберзаплахи чрез установяване на контроли, които минимизират риска от атака. Моделът е воден от схващането, че *„бъдещите паневропейски кибернетични учения трябва да се възползват от общата рамка, която се основава на националните планове за действие в непредвидени ситуации и осъществява връзка между тях.“*[68].

Правят се основни изводи спрямо проведеното анкетно проучване, както и се посочва, че изграденият модел се основава на следните критерии: Риск мениджмънт, Имплементиране на ИС, Киберпространство, Архитектура на ИС.

[68] Тагарев, Н. (2009). Превенция на кибертероризма в Република България. // Димитров, Д. (ред.). Икономически аспекти на тероризма. Етап III. Анализ на българската практика и моделиране на връзката тероризъм – икономика. София: Издателски комплекс УНСС, с. 154.

ЗАКЛЮЧЕНИЕ

Информационната сигурност в организация като висше учебно заведение е основен стълб за осъществяване на правомерна и стабилна защита на информационните ресурси, с които разполага. Актуалността на темата е осъзнатата необходимост да се опази, съхрани и защити информацията от различни видове атаки, които целят нейната увреда.

В дисертационния труд се положи теоретичната основа на същността, произхода и спецификата на информацията, като в контекста на обекта и предмета на изследователски интерес се изведе авторска дефиниция за това какво означава информация: съвкупност от знания и опит, основани на преки и/или косвени наблюдения за даден обект и/или явления, които водят до субективни и/или обективни умозаключения, основани на факти, доказателства, истинни хипотези. Предава се директно (вербално слово) или индиректно (е-кореспонденция и/или писмена кореспонденция) и води до откриване на нови неща, новини, събития. Най-естественият белег за съществена информация е нейната истинност. Информацията е най-ценният ресурс на новото време и той трябва да има защитеност от злоумишлени атаки и всевъзможни претенции за злоупотреби. Информацията се разглежда като съществено знание.

В дисертационния труд се акцентира върху Индустрия 4.0, чиято специфика се основава на взаимно свързване посредством wifi и всички устройства, които спомагат за процесите по обмен на информация; прозрачност; децентрализация и техническо съдействие.

Посочват се съвременните тенденции в осигуряването на информационна сигурност, съвместими с Наредбата за оперативна съвместимост и информационна сигурност и с Националната рамка за оценка на възможностите към Агенцията на Европейския съюз за киберсигурност. В действие се поставя и Националната стратегия за киберсигурност „Киберустойчива България 2020“ на МС, в която се посочват 9 фундаментални области за предотвратяване на кризи и киберзаплахи.

Посочват се и се анализират нормативни актове, политики, стандарти и процедури, регулиращи информационната сигурност във висшето образование като: Национална програма за развитие „България 2030“, Закон за управление и функциониране на системата за защита на националната сигурност, Закон за висшето образование, Закон за защита на личните данни, Наредба за минималните изисквания за мрежова и информационна сигурност, Наредба за сигурността на комуникационните и информационните системи, Наредба за общите изисквания за оперативна съвместимост и информационна сигурност, Проект за Цифрова трансформация на България, Програма „Цифрова Европа“ и прочее. Дават се определения за организационна, технологична и физическа сигурност, както и се акцентира върху стандартизирани рамки за киберсигурност с цел защита на киберинфраструктурата, с които висшите учебни заведения покриват мерките и процедурите за защита на информацията.

Извеждат се мерките, които трябва да се предприемат при нарушено управление на достъпа на информация или при съмнения в изтичане на данни, а именно мониторинг на организацията, план за управление на набор от данни, извършване на оценка за нарушение на данните.

В емпиричната част на дисертацията се провежда анкетно проучване с цел да се установи състоянието на информационната сигурност във висшите учебни заведения чрез мнението, нагласите, възприятията на работещите в сферата. Изводите, които се правят, са, че голям процент от работещите в такъв тип организации се чувстват сигурни за своите лични данни и за данните на потребителите. На мнение са, че човешка грешка е в основата на пропускливостта на ИС. Друг важен фокус на проучването е недостатъчната квалификация на служителите относно адекватно реагиране в ситуации на риск и киберзастрашеност. 89.3% споделят, че през последната една година не са посещавали курсове, семинари за квалификация относно възникване на рискови ситуации, свързани с информационната сигурност в работна среда.

Създава се примерен концептуален модел за подобряване на информационната сигурност във висшето образование, който се основава на систематичния подход за идентифициране и вземане на решение кои контрамерки са необходими да се предприемат, за да се защити информацията, както и ресурсите и спомагателните източници въз основа на оценката на заплахите и уязвимостите. Подлежи на шест

основни критерии: риск мениджмънт, имплементиране на ИС, киберпространство, архитектура на ИС, процес на реагиране/разкриване на заплахи, киберсигурност.

НАУЧНИ ПРИНОСИ

Дисертационният труд извежда следните научни и научно-приложими приносни моменти, които имат както теоретичен, така и практико-приложен характер:

Научен принос:

1) Изведена е следната авторска разширена дефиниция на понятието „информация“: съвкупност от знания и опит, основани на преки и/или косвени наблюдения за даден обект и/или явления, които водят до субективни и/или обективни умозаключения, основани на факти, доказателства, истинни хипотези. Предава се директно (вербално слово) или индиректно (е-кореспонденция и/или писмена кореспонденция) и води до откриване на нови неща, новини, събития. Най-естественият белег за съществена информация е нейната истинност. Информацията е най-ценният ресурс на новото време и той трябва да има защитеност от злоумишлени атаки и всевъзможни претенции за злоупотреби.

Научно-приложни приноси:

1) Предложен е оригинален концептуален модел за подобряване на информационната сигурност във висшето образование.

2) Анализите се провеждат по авторски подход с подбрани методи, за да се идентифицират проблемите и да се предложи решение.

3) Моделът може да намери реално приложение в конкретна среда, т.е. във висшите учебни заведения в страната, тъй като има конкретни потребители на резултатите от проведеното изследване.

СПИСЪК НА НАУЧНИТЕ ПУБЛИКАЦИИ ВЪВ ВРЪЗКА С ДИСЕРТАЦИОННИЯ ТРУД

1. **Ангелова, Е. (2024).** Предизвикателства пред сигурността в условията на дигитална трансформация. // Икономически и социални алтернативи, И-во на УНСС, София стр. 123-135
2. **Ангелова, Е. (2024).** Информационна сигурност във висшите учебни заведения. // Знание, наука, иновации, технологии, Велико Търново
3. **Ангелова, Е. (2024).** Концептуален модел за подобряване на информационната сигурност във висшите учебни заведения. // Доклади от конференция „Знание, наука, иновации, технологии“, Велико Търново
4. **Ангелова, Е. (2024).** Съвременни тенденции в осигуряването на информационната сигурност и управление на риска. // Знание, наука, иновации, технологии
5. **Величков, Ив., Ангелова, Е. (2019)**. Информационна осигуреност на висшето образование. // Научни трудове на Педагогически факултет, София
6. **Angelova, E.** Cyber security in higher education institutions – challenges and measures for storing information. // Bulgarian Journal of International Economics and Politics. Под печат

БЛАГОДАРНОСТИ

Бих искал да изкажа личните си благодарности и респект към своя научен ръководител доц. д-р Георги Павлов за професионалното и отговорно отношение към мен, както и за градивната критика в процеса на съставянето на научния труд.

Благодарности и признателност на Катедра „Национална и регионална сигурност” към УНСС, за доверието да съм техен докторант.

Благодарности и на всички колеги, които ме подкрепиха в извървяването на този нелек и отговорен път за мен.

ДЕКЛАРАЦИЯ ЗА ОРИГИНАЛНОСТ И ДОСТОВЕРНОСТ НА ДИСЕРТАЦИОНЕН ТРУД

Долуподписаният Елена Ангелова,

Докторант в УНСС, град София,

Дисертация на тема „Сигурност на информацията във висшето образование“ за придобиване на ОНС „доктор“

ДЕКЛАРИРАМ:

1. Представената дисертация е мое авторско дело и е основана върху мои собствени проучвания / изследвания.

2. Представената дисертация – в нейната цялост и отделните ѝ части, не е използвана в същата или в друга институция за висше образование за присъждане на образователна или научна степен.

3. Използваните източници са цитирани/позовани коректно и никоя част от дисертацията не е в нарушение на авторските права на институция или личност.

4. Предоставям правото на УНСС да архивира тази дисертация с цел доказване на моето авторство.

5. Информирана съм, че в случай на констатиране на плагиатство в настоящата работа Комисията по защитата е в правото си да я отхвърли.

Дата:

Подпис: Elena Ivanova Angelova

Digitally signed by Elena Ivanova Angelova
Date: 2024.12.19 11:35:27 +02'00'

UNIVERSITY OF NATIONAL AND WORLD ECONOMY

Faculty: „Infrastructure Economics“
Department: „National and Regional Security”

ABSTRACT

OF A DISSERTATION FOR AWARDING THE EDUCATIONAL AND SCIENTIFIC DEGREE

“DOCTOR”

INFORMATION SECURITY IN HIGHER EDUCATION

Professional field: 3.8. Economics

Doctoral program: Economics and Management (Defense and Security)

Ph.D. Student:
Elena Angelova

Supervisor:
Assoc. Prof. Georgi Pavlov, Ph.D.

Sofia
2024

The dissertation consists of 162 pages and includes an introduction, three chapters, abbreviations, a glossary, a conclusion, an appendix, scientific contributions, scientific publications, and bibliography. It contains a total of 145 cited sources, of which 57 are in Bulgarian and 88 are in foreign languages.

The dissertation includes 50 figures and 6 tables. The figures and tables included in the abstract correspond to those in the dissertation.

The dissertation has been reviewed and recommended for defense by a scientific committee, including faculty members from the Department of "National and Regional Security" and habilitated professors from the Department of "Informatics" at the University of National and World Economy (UNWE), Sofia, on December 10, 2024.

The defense of the dissertation will take place at an open session before a scientific jury appointed by the rector of UNWE on February 11, 2025, at 10:00 AM, in the "Scientific Councils" Hall (2032A). The doctoral materials are available to interested parties at the Department of "National and Regional Security". The abstract is published on the university's website for the development of the academic staff.

Author: Elena Angelova
Title: "Information Security in Higher Education"

C O N T E N T

GENERAL CHARACTERISTICS OF THE DISSERTATION

1. Relevance of the Problem

The relevance of the problem is determined by the global changes caused by the development of technologies and cybercrime. Information security is achieved through:

- ⇒ **Preventive measures**: related to risk control and mitigation of undesirable events, such as implementing passwords, security policies, information encryption, firewalls, etc.
- ⇒ **Detective measures**: involving the identification of events that may lead to undesirable phenomena, such as tracking, using motion sensors, surveillance systems, etc.
- ⇒ **Restorative measures**: aimed at restoring the integrity, confidentiality, and availability of information (e.g., backups, disaster recovery plans, determining acceptable error ranges, etc.).

The field of information security is linked not only to the protection of information but also to the requirements for the security of information systems, methods of risk assessment, and the implementation of information protection policies. A key characteristic of information security is its availability, reflecting, on one hand, access exclusively by authorized individuals, and on the other, the time and resources required to provide information upon a valid access request.

2. Research Problem

The research problem of the dissertation is to identify the main information security policies that have an effective and efficient impact on information preservation.

Testing a security model for information in higher education contributes to:

- ⇒ Enhancing information security in higher education;
- ⇒ Reducing vulnerabilities and threats to information security in higher education;

⇒ Mitigating the risks of cyberattacks;

⇒ Regulating access to information and data.

3. Purpose and Objectives of the Dissertation

The purpose of the dissertation is to develop a conceptual model for information security in higher education. The proposed model should not only analyze all vulnerabilities of the information system in higher education but also comply with legal regulations and enable effective monitoring, prevention, resource optimization, cybercrime reduction, and timely updates.

Objectives:

1. Present the theoretical aspects of information security.

2. Examine the legal, organizational, and technological aspects of information security in higher education.

3. Analyze the current state of information security in higher education.

4. Develop a model to reduce vulnerabilities and threats to information security in higher education.

5. Identify the benefits of implementing the model to improve information security in higher education.

4. Scientific Thesis

The scientific thesis is based on the assertion that the development of an information security model for the higher education sector will provide new opportunities for storing, protecting, and updating information and data flows.

5. Object and Subject of the Dissertation

Object of research: The system ensuring information security in universities.

Subject of research: Opportunities to reduce vulnerabilities and threats in the information environment by proposing a conceptual model for information security in higher education.

6. Research Methods

The dissertation employs **methods** such as analysis and synthesis, induction, deduction, comparative analysis, logical and systemic approaches, as well as surveys.

CONTENT OF THE DISSERTATION

CHAPTER ONE. INFORMATION AND INFORMATION SECURITY

In section 1.1, “Information - essence, origin, and specifics of protection”, fundamental definitions regarding the nature and specifics of information are outlined. Scholars define information as a *“valuable and important resource”* on which the *“overall economic and social development of regions”* fully depends. In its broadest sense, information encompasses data, knowledge, know-how, and experience, which help meet user expectations and attitudes and achieve specific goals. This is the primary reason why information, as a valuable asset, must be protected throughout all phases of its life cycle—from its creation to its destruction. Regardless of the form it takes, information must always be well protected.

The word originates from the Latin *informare* - to give form, indicating that information is always presented in a form, structure, or model; *informatio* – “to give an idea or concept about something”. The Oxford Dictionary defines it as *“facts provided or learned about something or someone”*; *“knowledge communicated concerning a specific fact, object, or event”*. This means that information is conveyed to the recipient with a certain specificity or eventfulness. It can be concluded that information directly relates to human actions of an active nature aimed at communicating or shaping something through words, leading to the assertion that “the information society is already functioning”.

In 1948, Wiener, the founder of cybernetics, stated that *“information is information, not matter or energy. No materialism that does not recognize this can survive these days”*. Thus, he introduced the concept of information into communication theory in philosophy. Consequently, researchers and philosophers have worked on defining the concept of information for over 60 years. Statistics indicate that by 1980, there were about 130 definitions. The founder of information theory, C. Shannon, considered it impossible to rely on a single concept, as information pertains to all areas of science and scholarly activity.

For the purposes of this dissertation, the author employs a personal definition based on research: ***information*** **is a collection of knowledge and experience based on direct and/or**

indirect observations of an object and/or phenomena, leading to subjective and/or objective conclusions grounded in facts, evidence, and truthful hypotheses. It is transmitted directly (verbal communication) or indirectly (e-correspondence and/or written communication) and leads to the discovery of new things, news, or events. The most natural attribute of essential information is its truthfulness. Information is the most valuable resource of the modern era and must be protected from malicious attacks and all kinds of potential misuse.

Based on this discussion, it can be concluded that information is a dynamic system that answers questions to fulfill the need for knowledge.

The Classified Information Protection Act establishes the guiding principle of *"the need to know"*, which inherently reflects the idea of humans as social beings requiring the exchange of news and information.

Several sources of risk exist in the transmission and reception of information:

- ⇒ Loss of trust;
- ⇒ Breaches of security and cybercrimes;
- ⇒ Technological changes;
- ⇒ Loss of key personnel;
- ⇒ Equipment failure;
- ⇒ Inefficiency in time management.

Another definition of information refers to it as an *"elementary factor in all organized activities"*, emphasizing that without information about the current situation, it is challenging to take steps to ensure the achievement of set goals. In other words, any purposeful action requires information to drive active organization. The evaluation of any critical situation, i.e., taking actions with a specific goal, involves all manifestations of information.

Information and communication technologies are essential for organizations and individuals to maintain high productivity levels. Adopting these technologies introduces many new vulnerabilities and, consequently, new threats to the confidentiality and integrity of personal and organizational data. Experts agree, however, that people are the weakest link in the information security system of an organization.

The term *security* is used in two primary contexts - *interest* and *threat.* The former represents an awareness of needs and values that, through a willingness to act, leads to the satisfaction of needs. The latter encompasses anything that directly or indirectly threatens the realization of personal interests related to security.

Joseph Nye argues that security is critically important and can be compared to oxygen - it goes unnoticed until it is gone. Social systems require robust security because external threats can lead to catastrophic consequences. Nye suggests that each social system possesses a specific security culture, which determines its relationships with others and the surrounding environment. Conversely, Tsvetkov argues that the security category is *complex and multifaceted*, complicating attempts to systematize knowledge.

Pavlov notes that the terms *information security, computer security, and information assurance* are interconnected. This theoretical hypothesis leads to the conclusion that information in the 21st century is viewed in the context of the digital challenges of the time and the creation of powerful systems to counter crimes caused by cyberattacks. Guaranteeing national security can only occur through "*building an evolving complex information system for strategic management"*. The scholar clarifies that while these areas of security are often used interchangeably due to their shared goal of protecting information, it is incorrect to interpret them identically, as there are significant differences between them.

Pavlov and Pudin define information security as the ability to ensure *"confidentiality, integrity, and availability"*, which, historically, combines *"computer security"* and *"communication security"*.

By nature, national security is a dynamic state of society in which the fundamental rights and freedoms of Bulgarian citizens, state borders, and territorial integrity are protected, and the democratic functioning of state and civic institutions is guaranteed to preserve and enhance well-being.

Definitions of information security generally focus on two aspects. The first is the extent to which employees understand safe information security practices, often outlined in their organization's policies, rules, and guidelines. Kruger et al. define this as the degree to which each staff member understands the importance of information security, the levels appropriate for the organization, and their individual security responsibilities. The second

aspect focuses on the extent to which employees are engaged and act according to best practices, often outlined in policies, rules, and guidelines for information security.

Developing and successfully implementing a security policy is a complex, multi-layered, and responsible process at the national level. It is important to note that an effective information security policy requires an assessment of risk factors when making managerial and organizational decisions.

The term “Industry 4.0” was publicly introduced in 2011 at the Hannover Fair. It builds on the definitions of the first three industrial revolutions. The first industrial revolution marked the transition from manual production methods to machines powered by steam or water. Thanks to electricity, the Second Industrial Revolution transformed factories into modern production lines, leading to high productivity and significant economic growth. The Third Industrial Revolution introduced computers at the operational level, such as programmable logic controllers and communication technologies in manufacturing processes, enabling automated production. In the era of Industry 4.0, production systems in the form of Cyber-Physical Production Systems (CPPS) can make intelligent decisions through real-time communication and collaboration between "production cycles," enabling flexible manufacturing of high-quality, customized products with mass efficiency.

Industry 4.0 represents *“a collection of interconnected digital technological solutions that support the development of automation, integration, and real-time data exchange in manufacturing processes”* - and beyond, in organizational processes as well. It encompasses new digital technologies and a wide range of technological solutions, creating a qualitatively new landscape of economic activities.

The latest threats and challenges to information security, such as those in cyberspace, are becoming a fundamental issue of our era. The requirements outlined in the Regulation on Interoperability and Information Security set forth the primary legislative provisions that define the methods for maintaining, storing, and accessing the registry of standards, as well as the methodology for evaluating compliance with operational security requirements. Compliance is ensured through the certification of information systems and the functionality of the unified environment for the exchange of electronic documents. Oversight is carried out by the Chairperson of the State Agency for Information Technology and Communications.

The Cybersecurity Act of the Republic of Bulgaria regulates the organization, management, and control of cybersecurity, as well as the implementation of measures to achieve a *"high overall level of network and information security"*. Article 2, Paragraph 1 interprets the definition of cybersecurity as *"a state of society and the state in which, through the application of a set of measures and actions, cyberspace is protected from threats related to its independent networks and information infrastructure, or threats that may disrupt their operation"*. It is further clarified that cybersecurity encompasses both network and information security, on the one hand, and counteraction to cybercrime and cyber defense, on the other. Article 2, Paragraph 3 provides a definition of network and information security, specifically as *"the ability of networks and information systems to withstand a certain level of impacts that negatively affect the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data, or the related services offered by or accessible through these networks and information systems"*. To ensure safety and prevent potential risks and threats, organizational, technological, and technical measures are applied to minimize risk factors. The National Cybersecurity Strategy and the Cybersecurity Council are highlighted, the latter serving as a consultative and coordinating body under the Council of Ministers. The Minister of Defense is designated as the primary authority for addressing and countering threats under this law. The minister is empowered to conduct state policy for protection against and active response to cyber and hybrid attacks through the development and enhancement of cyber defense capabilities.

ISO/IEC 27001 is a standard for information security (IS), defining the requirements for managing data and information security, cybersecurity, and privacy protection. Adopting an information security management system (ISMS) is a strategic decision for any organization. The creation and implementation of an ISMS are influenced by the organization's needs and objectives, security requirements, operational processes, and size and structure. All these factors are expected to evolve over time.

The Information Security Management System (ISMS) preserves the confidentiality, integrity, and availability of information by applying a risk management process and provides assurance to stakeholders that risks are being adequately managed. It is important that the ISMS is part of and integrated with the organization's processes and overall management structure, ensuring that information security is considered in the design of processes, information systems, and controls.

In section 2.1, *"Higher Education as an Object of Information Security"*, various laws and regulations are listed that govern the structure, functions, management, and access to security. A definition of digital transformation is presented as "a process characterized by the pervasive implementation and combination of digital technologies in all areas of social and economic life".

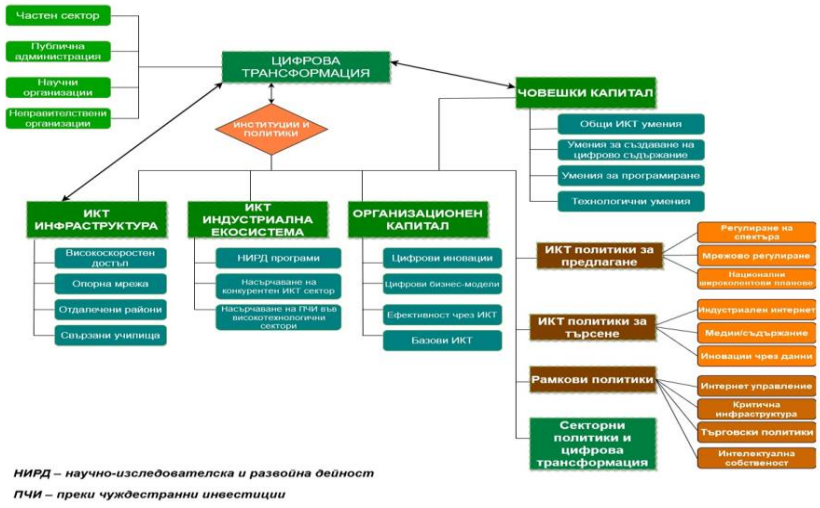


Figure 1
Digital transformation
Source: Strategy.bg

The "Digital Europe" Program is underway, aimed at providing digital technologies in response to the challenges of the modern world. Through it, new opportunities are revealed, the development of reliable technologies is encouraged, and the building of an open democratic society is supported. It is based on three pillars for digital economy and digital transformation:

⇒ **Technologies for the benefit of people -** investments in the development of digital skills; protection from cyberattacks; artificial intelligence and its development in the context of human rights; the introduction of high-speed internet; expanding the capacity of supercomputers;

⇒ **Fair and competitive digital economy -** access to innovations and dynamic communities; responsibility of online platforms; ensuring the suitability of online service rules, fair competition; enhancing access to high-quality data;

⇒ **Open, democratic, and sustainable society -** using technologies to reduce carbon emissions in the digital sector; citizens' ability to control their data; creating a space for health data; combating disinformation.

The construction of an information system in higher education is subject to the policy of network and information security. In this way, information security is integrated into the principles and values, culture, and traditions of the Republic of Bulgaria. On the other hand, the creation of an electronic presence in the web space of an organization (university) must be fully aligned with the architecture of the institution. The most effective approach is the so-called *complex system*, which consists of both securing the protection of devices and safeguarding against user errors.

Conclusions are drawn from the first chapter, emphasizing that security has always been one of the most important goals and needs of the individual, society, and the state as a whole. The formation and development of human civilization has always been linked to eliminating various threats caused by nature, society, hostile parties, technological devices, etc. In other words, security is one of the most important conditions for the existence and development of society and the state. The term *"safety"* was first used in 1190 as *"a state of calmness in the human spirit, in which it feels safe from any dangers"*.

CHAPTER TWO.
ANALYSIS OF THE STATE OF INFORMATION SECURITY

In section 2.1. *"Methodological Tools for Information Protection in Higher Education"*, various types of security are discussed, noting that in 2018, when the GDPR came into effect, it provoked different reactions within the higher education community. Organizations are accumulating large amounts of information more quickly than ever before. Through technology, they can utilize these data volumes to enhance efficiency and provide more informed decision-making opportunities. This increasing reliance on IT has introduced various advantages but also means additional risks.

The protection of technological infrastructure for individuals and organizations is important. In this regard, information security and cybersecurity technologies are used. Information security protects organizational information from unauthorized modification, interruption, verification, and disclosure. This information can exist in any form, including cyber or other types. ICT and security practices specifically deal with protecting the digital infrastructure of organizations to help mitigate and prevent threats.

Tools and techniques for ICT security have been introduced to protect digital assets and infrastructures. Research on this and its adoption in organizations are generally case studies specific to the organization.

Higher education institutions (HEIs) are highly digitized in the 21st century, relying on technology to manage their vast amounts of information. Computer infrastructure and networks have been implemented to assist students, faculty, and staff in the operations of the institutions.

Figure 2 categorizes the threats according to the vulnerable subject of the organizations.

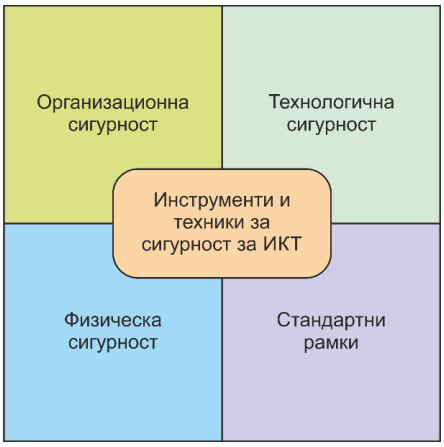


Figure 2
Categorization of ICT Security Tools and Techniques
Source: Author's interpretation

Organizational security deals with threats arising from vulnerabilities in the management of human and digital assets within higher education institutions (HEIs). Human risks are also a major factor contributing to the security of the organization. This is especially true for HEIs, which in many countries suffer from chronic underfunding, particularly in auxiliary/supporting sectors such as IT. Furthermore, a given faculty usually has older staff members, for whom acquiring IT knowledge is not easy. Improper access management of personnel can expose the organization to internal threats. Staff with little training and awareness regarding security practices are also considered a risk to the ICT security infrastructure of the organization. Among the risk factors, the human factor is considered the weakest link.

Technological security addresses threats that arise from vulnerabilities in the applications, software, and network systems used by the organization. Network threats stem from vulnerabilities embedded in interconnected devices, particularly those linked to the internet. Improperly configured networks and servers can provide attackers with unauthorized access to the institution's computers and databases. These threats can come in the form of floods, fires, earthquakes, thefts, robberies, and physical damage.

Physical Security. The use of the following measures to prevent physical damage to the cyber infrastructure of HEIs is achieved through:

⇒ Temperature control;

⇒ Early warning systems for disasters.

Physical security of classified information includes a system of measures, methods, and tools to prevent unauthorized access to materials, documents, equipment, and machinery classified as state or official secrets. The system is part of the general security requirements for the protection of classified information and includes both general and specific measures.

Standards and Frameworks. HEIs use standardized frameworks for cybersecurity to protect their cyber infrastructure.

The measures taken, prompted by breaches in information access, include:

1) **Organization Monitoring -** should be carried out through regular oversight by management as well as using tools. Log files from operating systems, applications, and network devices should be regularly reviewed for anomalies and can help identify malicious attacks against systems.
2) **Data Breach Management Plan -** This enables the organization to respond quickly and adequately through a systematic approach to managing breaches. In this way, employees who are directly responsible for the domain are encouraged to act proactively by developing and implementing stable management processes.
3) **Conducting a Data Breach Assessment -** In the event of a breach, the organization is required to take reasonable, adequate, and expedient actions and assess whether the crisis situation warrants notification according to the Personal Data Protection Act (PDPA). Any unreasonable delay in reporting an information security breach can be very costly for the organization.

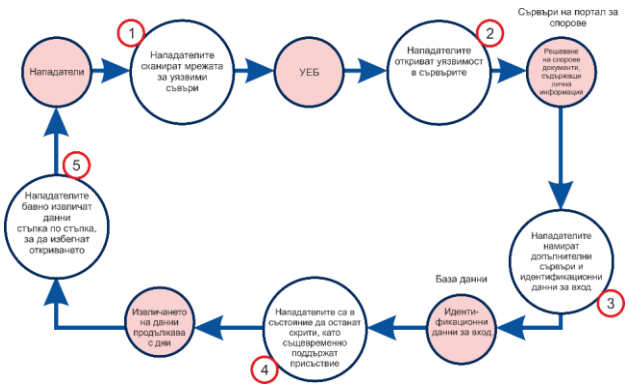


Figure 3
Model of a hacker attack for data breach and personal data theft

Source: Adapted from GAO, Equifax

Preventing unauthorized access requires a comprehensive approach that combines several strategies:

1. **Strong Password Policy -** one of the most basic yet effective ways to prevent unauthorized access is to implement a strong password policy. This includes requiring users/employees to create complex passwords that are difficult to guess, and enforcing regular changes. A strong password should be at least eight characters long and include a combination of uppercase and lowercase letters, numbers, and special characters. It should also not contain easily guessable information such as the user's name, birth date, or common words.

2. **Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) -** Another effective strategy is the use of 2FA and MFA. The first requires users to provide two different types of identification to access a system. This could be, for example, a password and a code sent to the user's mobile phone. The second, on the other hand, involves the use of three or more authentication factors. These can combine something the user knows (e.g., a password), something the user has (e.g., a security token), and something the user is (e.g., a fingerprint).

3. **Monitoring User Activity -** Monitoring is another important strategy for preventing unauthorized access. This involves tracking what users are doing within systems and networks, as well as looking for any unusual activities. In this way, potential security breaches can be detected and necessary actions can be taken before significant damage occurs.

4. **Endpoint Protection Implementation -** A strategy focused on protecting each endpoint or user device in a network to prevent unauthorized access. This can include laptops, desktop computers, mobile phones, tablets, and any other devices that connect to a network. Endpoint security measures can include next-gen antivirus software, firewalls, and intrusion detection systems. They can also include policies that limit the use of removable media, such as USB devices, which can be used to introduce malware or steal data.

5. **Regular Software Updates and Patch Management -** Another important strategy for preventing unauthorized access. Software updates often include security improvements that fix vulnerabilities that could be exploited by hackers.

The approaches and methods for comparison can be both qualitative and quantitative.

The methodology used is based on the assumption of the feasibility of achieving the goals and tasks outlined in the dissertation. In its essence, it is divided into a survey study and the development of a conceptual model for limiting threats and vulnerabilities in information security.

In the survey study, the specifics are identified by constructing key blocks of questions. The advantages and disadvantages of the survey method are outlined, with the survey conducted among 56 Bulgarian citizens working in the higher education sector (Bulgarian universities) and voluntarily participating, in order to assess the state of information security and evaluate the possibilities for implementing a new, improved security management system. The expert opinion survey is intended to be conducted through a direct survey (online via Google Forms), as this method allows for quick collection of diverse information. The object, subject, and methods of the survey are mentioned.

The conclusions drawn in the second chapter are related to the construction of the methodological framework and its tools based on the conducted studies. The focus is on the types of information security, with a comparative analysis being made.

CHAPTER THREE.
RESULTS AND CONSIDERATION OF A CONCEPTUAL MODEL FOR IMPROVING INFORMATION SECURITY IN HIGHER EDUCATION

In section 3.1, "Analysis of the Results from the Survey Study", an important clarification is made that the survey is conducted to verify the need for presenting a Security Model. Without consulting specialists – university lecturers and staff in universities – there would be no way to validate the reliability and validity of the desire for a new model. This is a necessary step to provide a contemporary perspective from those working in the higher education sector. The survey takes into account the opinions of the surveyed respondents and draws resources for the design of the Model.

The questions are grouped into three main principles – demographic characteristics, professional characteristics, and personal opinions, structured into three main blocks: related to personal information; related to the quality of the IS system; and related to the competence of employees. Special attention is given to the specific questions related to the satisfaction of employees with information security in their workplace.

In question № 6: *"Are you calm about your information security and the security in your organization?"* 62.5% answered *"Yes, I could say"*, and 32.1% affirmatively with *"Yes, I am completely calm"*. The remaining percentages were distributed between the answers *"Rather not calm"* (3.4%) and *"No, I am not calm at all"* (2%). The conclusion can be drawn that the majority of respondents are somewhat calm about their own security, rather than not at all or completely not calm. This suggests that information security systems are sufficiently effective to meet the challenges of today. In case of a possible answer *"I cannot assess"*, there were no respondents who chose this option, which indicates their feeling of security in the organization they represent.

Figure 4
Question: Are you confident about your information security and the security within your organization?

In question № 7: *"What do you think are the main causes of the various breaches and problems with information security?"* 57.1% answered that human error is at the core of the vulnerability of the IS, which statement was theoretically verified in the first and second chapters of the dissertation. 30.4% believe that the issue lies in weaknesses in the system, and 10.7% attribute it to increasingly skilled hackers. The respondents who marked *"I cannot assess"* are 1.8%. There were no respondents who selected *"due to different and contradictory instructions to administrative staff".* The purpose of the question is to track the professional and human opinion of those working in the organization, with human error coming to the forefront as the cause of system vulnerabilities and malicious attacks.

An audit report from the EU regarding cybersecurity classifies numerous types of threats based on how data is handled – disclosure, modification, destruction, or denial of access. It also identifies types of cyberattacks, such as malware, ransomware, denial-of-service (DoS) attacks, and web-based attacks. Complex persistent attacks are classified as *"the most malicious types of threats".* Human error mainly consists of the incorrect choice of passwords, accidental information disclosure, and using outdated or inappropriate software. Accidental threats arise when an employee lacks adequate knowledge about security systems, misconfigures systems, or when information leaks due to insecure data transfers.

Figure 5
Question: In your opinion, what are the primary causes of various breaches and issues with information security (IS)?

In question № 8: *"How often have you experienced a crash in the information system while performing your work activities?"* 66.1% responded that it has not happened recently within the year. 19.6% stated that they have never been immediate witnesses to or victims of a system crash that interfered with their professional activities. 10.7% believe that it happens not very often, roughly once every few months. 3.6% shared that they often encounter such situations once or twice a month. The respondents completely excluded the answer *"very often (once a week)"*.

From these results, it can be concluded that there are sporadic system crashes during work activities, but overall, these incidents are not frequent. This is an encouraging factor for the security, quality, and effectiveness of the information systems in higher education organizations. However, the percentage of respondents who report experiencing such situations often should not be underestimated, as it is an important responsibility of the respective organization to take strict, thoughtful, and serious measures regarding the quality of the information system's performance.

Figure 6
Question: How often have you experienced a failure in the information system while performing your work activities?

In question № 9: *"Which channel do you most frequently use to receive information in order to perform your daily work duties?"* 53.6% responded that the most preferred method for them is email inquiries. On the other end of the spectrum, with the least responses, is the preference for written inquiries on paper (7.1%), creating a digital vs. paper contrast. In contemporary society, information, as a valuable resource, is most effectively and quickly delivered through the internet via various channels. Also, it should not be overlooked that nature and its preservation depend on the routine activities of humans and the efforts they put into safeguarding it. 17.9% of respondents indicated the university's website, while an equal number of 10.7% expressed a preference for receiving quick and timely information through various social internet channels and by phone.

It is well-known, and the survey confirms, that email is one of the most popular forms of communication that people use, but it is also one of the most abused. At the end of last year, Sinch Mailgun surveyed more than 2,000 users in the US, the UK, France, Germany, and Spain to understand how they prefer to correspond and interact, as well as what motivates them to engage in email communications. The most evident finding in this report is that email is the preferred method. This is true not only for marketing campaigns, for example, but also for transactional communication. 75.4% of users selected the email inbox as their preferred channel for messages, while 74% did so for transactional notifications.

Another study (The Digital Everyday Life in Finland 2022) shows that the flexibility and history of messages are the main reasons for the popularity of email. People are willing to

wait a few working days for a response but no longer, before switching to another communication channel.

In the 21st century, the position of information security analyst is becoming increasingly in demand. The job description primarily focuses on protecting the organization's computer networks, systems, and databases from cyberattacks and data breaches. Specifically, it includes:

⇒ Detecting, monitoring, and mediating various aspects of security – including physical security, software security, and network security;

⇒ Performing compliance control tests;

⇒ Developing recommendations and training programs to minimize security risks within the company;

⇒ Creating clarity regarding evolving threats in the cybersecurity space through communication with external sources;

⇒ Collaborating with other teams and management within the organization to implement best security practices.

Security analysts are essential in organizations that store sensitive data and information, including the education sector.

Figure 7
Question: In your opinion, are the knowledge and competencies of the service and administrative staff at a sufficiently high level to take adequate actions to prevent risk situations related to information security?

In response to question № 11, *"In the last year, have you attended courses or seminars for qualification regarding the emergence of risk situations related to information security in the workplace?",* 89.3% expressed a negative opinion, while 10.7% shared that they had attended such events. This leads to a reconsideration of strategies in universities regarding their information security. Without qualified and well-trained staff capable of reacting promptly to malicious activities, the security level sharply declines, which calls into question the value of investments in the effectiveness of actions and staff qualifications. New sources of threats emerge every year, and only well-informed professionals, such as cybersecurity specialists and IT experts, can contribute to the training of employees in higher education. Various courses, seminars, meetings, and discussions help raise awareness, which ultimately benefits the entire organization.

Employees need a reason to care about security. Training should convey the business value of best security practices to the organization: how it enables training, generates revenue, or protects assets and reputation. People will be more likely to make careful security decisions when they have a sense of personal responsibility and view security as essential to their daily lives. Therefore, security awareness training should demonstrate the connection between security and the responsibilities of all roles in the organization, from front-line staff to top executives.

Figure 8
Question: In the past year, have you attended any courses or seminars for qualification regarding the occurrence of risk situations related to information security in the workplace?

In response to question № 12, *"In the event of an incident related to information security, you will first:"*. 92.9% of the respondents unanimously stated that they would notify a colleague directly responsible for information services. 3.5% believe that they would take action by notifying the Cybercrime Directorate of the General Directorate for Combating Organized Crime (GDBOP) or stay calm and attempt to handle the situation themselves. The answer *"notify the State Agency for National Security"* was left without a percentage ratio.

Figure 9
Question: In the event of an information security incident, what would you do first?

In response to question № 13, *"In your opinion, is the information security system in the higher education institution you work at effective?"*, 67.9% of respondents answered that it is more effective than not, while 26.8% expressed a strongly positive opinion. It can be concluded that the employees are unanimously of the opinion that the information security system is effective.

Figure 10
Question: In your opinion, is the information security system at higher education institution where you work effective?

In response to question № 14, *"In your opinion, are your personal data well protected in the institution where you work?",* 58.9% of respondents answered "Yes, it can be said," while 26.8% answered "Yes, completely." These results shape the sense of security within the organization, helping employees feel protected and perform their professional responsibilities with confidence. Proportionally, 6% selected the answers *"Rather not"* and *"I cannot assess",* while 2.3% of respondents believe that their personal data is not protected at all.

Figure 11
Question: In your opinion, is your personal data well protected in the institution where you work?

In response to question № 15, *"In your personal opinion, do you feel protected from attacks occurring in the online space that violate personal data and users' rights?",* 66.1% of respondents answered *"Yes, it can be said",* while 21.4% answered *"Yes, completely",* which helps to understand the level of security within the organization. Employees feel protected from malicious attacks aimed at violating personal data and users' rights. 7.5% of respondents are on the opposite side, strongly stating that they do not feel protected at all. 4% are unable to assess, and 1% selected the answer *"Rather not".*

Figure 12
Question: In your personal opinion, do you feel protected against attacks carried out in cyberspace that violate personal data and user's rights?

In response to question № 16, *"Please share your opinion on information security at the higher education institution where you work",* respondents are given the opportunity to express their free opinion on the information security in the organization they represent. Some of the answers are grouped into approximately equal categories, which include: satisfactory level (5.4%), good level (8.9%), high level (21.4%), effective (5.4%), necessary measures have been taken (16.1%). Based on these prevailing results, it can be concluded that employees in higher education institutions consider the information security system to be reliable and of high quality.

Figure 13
Please share your opinion regarding the information security at the higher education institution where you work?

The remaining responses, which were provided in free text, offer additional interesting insights: *"With many reservations and room for improvement!"; "A certain level of security has been achieved, but there are frequent issues with lower-risk problems"; "Given the lack of serious security incidents, I consider the level to be relatively good"; "The level meets current conditions, but greater qualification of experts for information protection is needed"; "There is a need for upgrades with more modern security systems"; "At the university where I work, there is an ongoing effort to improve information security, even though it is currently at a very good level. I support measures aimed at raising employee awareness. In 2023 and 2024, within one day, everyone employed could be informed about the university's policy on cybersecurity"; "I consider it very reliable"; "I have no concerns about information security. I believe the necessary measures have been taken to ensure it".*

From these responses, it can be summarized that improvements in information systems, enhancing security, additional qualification courses for employees in this area, and measures taken by each university to ensure cybersecurity are crucial to the effectiveness of information systems. From this, the theoretical understanding emerges that cybersecurity reflects the maintenance of active and preventive measures in cyberspace, the level of which is determined by confidentiality, integrity, availability, and necessary resources.

In the next part of the study, a conceptual model is developed to mitigate the vulnerabilities and threats to information security in universities. Criteria, indicators, and components are applied. Each component of the derived criteria is illustrated step by step.

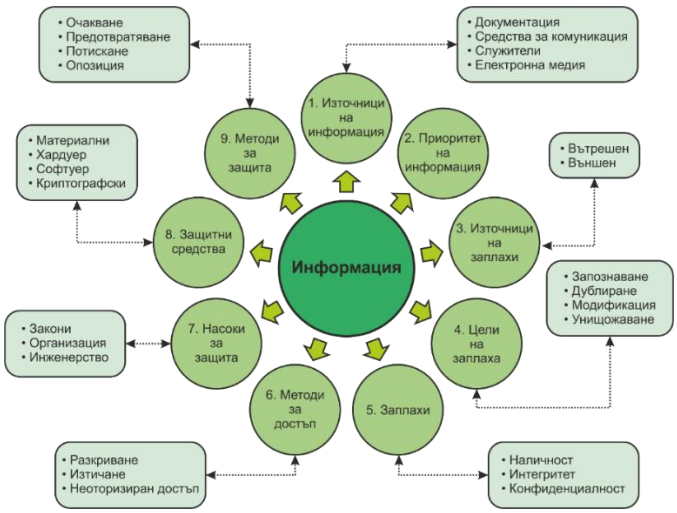


Figure 14
Implementation of an Information Security Concept into the Model
Source: Author's interpretation

The security structure is developed, which can assist the university in addressing challenges in collaboration with its own administrative and IT staff.

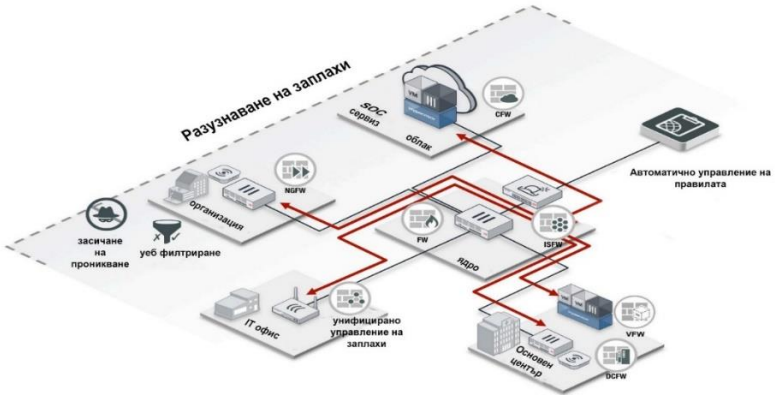


Figure 15
Security Structure of the Model
Source: Author's interpretation

It consists of:

1. Next-Generation Firewall (NGFW) - part of the third-generation firewall technology, combining conventional firewall functions with additional network device filtering features, such as application firewalls using deep packet inspection (DPI), intrusion prevention systems (IPS). Other techniques like TLS-encrypted traffic inspection, website filtering, Quality of Service (QoS)/bandwidth management, antivirus scanning, third-party identity management integration (e.g., LDAP, RADIUS, Active Directory), and SSL decryption can also be used.

2. Custom Firmware or Application Space (CFW) has become a strategic imperative for many organizations as they strive to address critical workforce shortages, skill gaps, and retention issues in frontline operations. It has been proven that CFW-enabling technology helps organizations tackle workforce challenges while optimizing operational performance in aspects such as safety, quality, and productivity.

3. Firmware (FW) - Designed to be the interface between the computer's hardware and software. It abstracts many low-level, hardware-specific details of how the computer operates, making it easier to develop software and run the same software across multiple systems. Its implementation provides several advantages, such as: trust from

partners, employees, and stakeholders (teachers, students, staff); competitive advantage; integrated security.

4. Internal Segmentation Firewall (ISFW) is designed to protect network segments from malicious code attempting to infiltrate the internal network. The ISFW architecture ensures maximum performance and security while offering the flexibility to be placed anywhere within the organization.

5. Virtual Firewall (VFW) is designed to meet the unique security needs of modern virtualized infrastructures. The virtual firewall controls access to subnets and supports allow and deny rules for customer service. The client can add rules as needed, and the VFW determines whether data packets can pass to or from the subnets.

6. Data Center Firewall (DCFW) - Describes the work carried out by the full spectrum of the cyber workforce, aiming to protect data centers from advanced threats, ensuring the protection of sensitive information and critical applications.

The main criteria that the Model must adhere to include considering the source, origin, nature, timing, and intent of the threat actor.

Table 2
Types of Information Security Threats

Criteria				
Source	**Origin**	**Nature**	**Time**	**Intent**
Internal External	Natural Social (Includes human behavior)	Economic Political Financial Demographic	Temporary Periodic Permanent	Accidental Deliberate

Source: Pavlov & Poudin

Depending on the context of the application of information security, there are various levels of resilience, development, and operation of the information security management itself. However, it is common for the levels of resilience and operation to be represented by a numerical value that reflects the current state of the organization of the observed system. The general characteristic is that they are based on six levels of development and operation of processes, and it depends on which management framework is applied.

Figure 45
Levels of development
Source: Sikman et al. (2023)

The technology for the development and functioning of information security (IS) represents a framework in which the activities performed at each of the existing levels of development are detailed.

When creating a model for managing information security in higher education, the entire system of elements is initially set at all levels. Once it is determined which elements should be used, all aspects of the level that are necessary for identification are considered, and they contain all the necessary measures for determining the security of the information system.

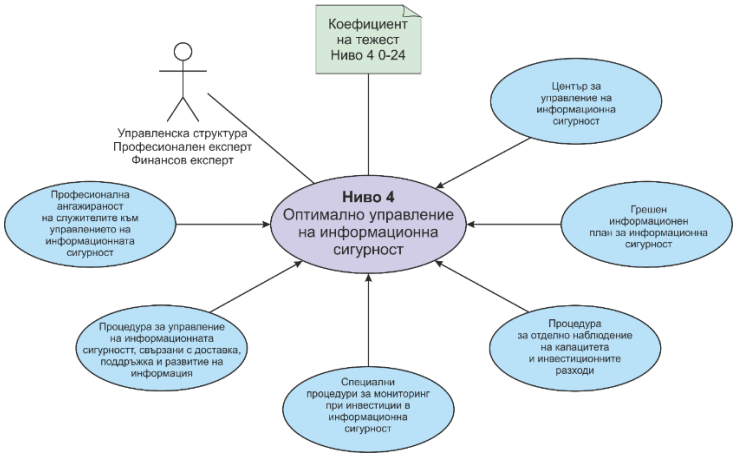


Figure 46
Diagram of optimal management of information security processes
Source: Author's interpretation

The technology of the model is derived in its optimal version on the diagram. This figure presents a simplified version of the model's technology depending on its optimality and feasibility.

The necessary investments required for improving information security (IS) in the higher education sector are listed: investment in people, investment in processes, and investment in software.

The expected benefits of implementing the model to improve information security in higher education are of paramount importance for protecting the institution's security. On the one hand, it is designed to strengthen the organization against cyber threats by establishing controls that minimize the risk of attack. The model is driven by the understanding that *"future pan-European cyber exercises should take advantage of the common framework based on national action plans for unforeseen situations and link them together".*

Key conclusions are drawn based on the conducted survey, and it is pointed out that the developed model is based on the following criteria: Risk Management, IS Implementation, Cyberspace, and IS Architecture.

CONCLUSION

Information security in an organization such as a higher education institution is a fundamental pillar for ensuring legitimate and stable protection of the information resources it holds. The relevance of the topic arises from the recognized need to preserve, safeguard, and protect information from various types of attacks that aim to harm it.

The dissertation lays the theoretical foundation for the essence, origin, and specifics of information, and within the context of the object and subject of research interest, an original definition of information is derived: a collection of knowledge and experience based on direct and/or indirect observations of a given object and/or phenomena, which lead to subjective and/or objective conclusions based on facts, evidence, and true hypotheses. It is transmitted directly (verbal communication) or indirectly (e-correspondence and/or written correspondence) and leads to the discovery of new things, news, or events. The most natural characteristic of essential information is its truthfulness. Information is the most valuable resource of modern times, and it must be protected from malicious attacks and any potential abuses. Information is regarded as essential knowledge.

The dissertation emphasizes Industry 4.0, whose specificity is based on mutual connectivity via Wi-Fi and all devices that facilitate the exchange of information processes; transparency; decentralization; and technical assistance.

Contemporary trends in ensuring information security, compatible with the Ordinance on Operational Compatibility and Information Security, as well as with the National Framework for Capability Assessment to the European Union Agency for Cybersecurity, are identified. The National Cybersecurity Strategy “Cyber-Resilient Bulgaria 2020” of the Council of Ministers is also put into action, which outlines 9 fundamental areas for preventing crises and cyber threats.

Normative acts, policies, standards, and procedures regulating information security in higher education are identified and analyzed, such as: the National Program for Development “Bulgaria 2030”, the Law on the Management and Functioning of the National Security Protection System, the Higher Education Act, the Personal Data Protection Act, the Ordinance

on Minimum Requirements for Network and Information Security, the Ordinance on the Security of Communication and Information Systems, the Ordinance on General Requirements for Operational Compatibility and Information Security, the Digital Transformation of Bulgaria Project, the “Digital Europe” Program, and others. Definitions of organizational, technological, and physical security are provided, with a focus on standardized cybersecurity frameworks aimed at protecting cyber infrastructure, through which higher education institutions ensure the necessary measures and procedures for information protection.

Measures to be taken in case of compromised information access management or suspected data breaches are outlined, such as monitoring of the organization, data set management planning, and conducting data breach assessments.

The empirical part of the dissertation presents a survey aimed at determining the state of information security in higher education institutions based on the opinions, attitudes, and perceptions of employees in the field. The conclusions drawn are that a large percentage of employees in such organizations feel secure about their personal data and user data. They believe that human error is at the core of information system vulnerabilities. Another important focus of the study is the insufficient qualification of employees regarding their adequate response in situations of risk and cyber threats. 89.3% of respondents share that, over the past year, they have not attended courses or seminars on qualification concerning risk situations related to information security in the work environment.

A sample conceptual model for improving information security in higher education is developed, based on a systematic approach to identifying and deciding which countermeasures need to be taken to protect information, resources, and auxiliary sources based on an assessment of threats and vulnerabilities. The model is based on six main criteria: risk management, IS implementation, cyberspace, IS architecture, threat response/disclosure process, and cybersecurity.

SCIENTIFIC CONTRIBUTIONS

The dissertation presents the following scientific and scientifically-applicable contributions, which have both theoretical and practical-application aspects.

Scientific Contributions:

1) A new, author-developed extended definition of the concept of "information" is proposed:
   "A collection of knowledge and experience, based on direct and/or indirect observations of a given object and/or phenomena, leading to subjective and/or objective conclusions based on facts, evidence, and truthful hypotheses. It is conveyed directly (spoken word) or indirectly (e-correspondence and/or written correspondence) and leads to the discovery of new things, news, events. The most fundamental characteristic of significant information is its truthfulness. Information is the most valuable resource of the modern era, requiring protection from malicious attacks and various misuse claims".

Applied Scientific Contributions:

1) An original conceptual model for improving information security in higher education is proposed.
2) Analyses are conducted using an author-developed approach with selected methods to identify problems and propose solutions.
3) The model is applicable in a specific environment, i.e., in higher education institutions in the country, as it has specific users of the results obtained from the research.

SCIENTIFIC PUBLICATIONS RELATED TO THE DISSERTATION

1. Angelova, E. (2024). Challenges to security in the context of digital transformation. // Economic and Social Alternatives, UNWE Publishing House, Sofia, pp. 123-135

2. Angelova, E. (2024). Information security in higher education institutions. // Knowledge, Science, Innovations, Technologies, Veliko Tarnovo

3. Angelova, E. (2024). Conceptual model for improving information security in higher education institutions. // Proceedings of the Conference "Knowledge, Science, Innovations, Technologies", Veliko Tarnovo

4. Angelova, E. (2024). Contemporary trends in ensuring information security and risk management. // Knowledge, Science, Innovations, Technologies

5. Velichkov, I., Angelova, E. (2019). Information assurance in higher education. // Scientific Works of the Pedagogical Faculty, Sofia

6. Angelova, E. Cyber security in higher education institutions – challenges and measures for storing information. // Bulgarian Journal of International Economics and Politics. Under print.

ACKNOWLEDGEMENTS

I would like to express my personal gratitude and respect to my scientific supervisor, Assoc. Prof. Georgi Pavlov, for his professional and responsible attitude towards me, as well as for his constructive criticism during the process of composing this scientific work. Thanks and appreciation to the Department of “National and Regional Security” at the University of National and World Economy (UNWE) for trusting me to be their doctoral student.

My thanks also go to all the colleagues who supported me on this difficult and responsible path.

DECLARATION OF ORIGINALITY AND ACCURACY OF THE DISSERTATION

I, Elena Angelova,
Ph.D. student at the University of National and World Economy (UNWE), Sofia,
Dissertation titled “Information Security in Higher Education” for the acquisition of the educational and scientific degree “Doctor”
DECLARE:

1. The presented dissertation is my original work and is based on my own research/studies.

2. The presented dissertation – in its entirety and in its individual parts – has not been used in the same or any other higher education institution for the awarding of an educational or scientific degree.

3. The sources used are cited/referenced correctly, and no part of the dissertation violates the copyright of any institution or individual.

4. I grant the right to UNWE to archive this dissertation for the purpose of proving my authorship.

5. I am informed that in case plagiarism is detected in this work, the Defense Committee has the right to reject it.

Date: _____ Signature: Elena Ivanova Angelova Digitally signed by Elena Ivanova Angelova Date: 2024.12.19 11:21:15 +02'00'