



**УНИВЕРСИТЕТ ЗА НАЦИОНАЛНО И
СВЕТОВНО СТОПАНСТВО**

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

ЕЛЕНА ИВАНОВА АНГЕЛОВА

**СИГУРНОСТ НА ИНФОРМАЦИЯТА
ВЪВ
ВИСШЕТО ОБРАЗОВАНИЕ**

ДИСЕРТАЦИОНЕН ТРУД

за придобиване на образователна и научна степен
„доктор“

Професионално направление: 3.8. Икономика

Докторска програма: Икономика и управление (Отбрана и сигурност)

Научен ръководител:

доц. д-р Георги Павлов Павлов

София
2024

СЪДЪРЖАНИЕ

СЪКРАЩЕНИЯ	4
ТЕРМИНОЛОГИЧЕН РЕЧНИК	5
УВОД	7
ПЪРВА ГЛАВА. ИНФОРМАЦИЯ И ИНФОРМАЦИОННА СИГУРНОСТ – ТЕОРЕТИЧНИ АСПЕКТИ	12
1.1. Информация – същност, произход и специфика на защитата	12
1.1.1. Съдържание на понятието	12
1.1.2. Специфика на защитата на информацията и информационната сигурност	17
1.1.3. Предизвикателства пред защитата на информацията в условията на четвъртата индустриална революция	24
1.1.4. Съвременни тенденции в осигуряването на информационната сигурност и управление на риска. Киберсигурност и киберпрестъпления	31
2.1. Висшето образование като обект на информационна сигурност	37
2.1.2. Нормативни актове, политики, стандарти и процедури, регулиращи информационната сигурност във висшето образование	37
2.2.2. Изграждане на информационна система във висшето образование за осигуряване сигурност на информацията	44
ИЗВОДИ ОТ ПЪРВА ГЛАВА	49
ВТОРА ГЛАВА. АНАЛИЗ НА СЪСТОЯНИЕТО НА ИНФОРМАЦИОННАТА СИГУРНОСТ ВЪВ ВИСШЕТО ОБРАЗОВАНИЕ	52
2.1. Методологически инструментариум за защита на информацията във висшето образование	52
2.1.1. Видове сигурност на информацията	52
2.1.2. Мерки при риск от нарушаване на достъпа на информация	58
2.2. Подходи и методи на изследване – сравнителен анализ	61
2.3. Специфика на анкетното проучване. Основни блокове въпроси	66
ИЗВОДИ ОТ ВТОРА ГЛАВА	77
ТРЕТА ГЛАВА. РЕЗУЛТАТИ И ИЗГРАЖДАНЕ НА КОНЦЕПТУАЛЕН МОДЕЛ ЗА ПОДОБРЯВАНЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ ВЪВ ВИСШЕТО ОБРАЗОВАНИЕ	80
3.1. Анализ на резултатите от проведеното анкетно изследване	80

3.2. Концептуален модел за ограничаване на уязвимостите и заплахите на информационната сигурност в университетите	102
3.1.1. Технология за подобряване на системите за информационна сигурност	125
3.1.2. Необходими инвестиции за подобряване на информационната сигурност	130
3.1.3. Очаквани ползи от внедряване на модела за подобряване на информационната сигурност във висшето образование.....	133
ИЗВОДИ ОТ ТРЕТА ГЛАВА	139
ЗАКЛЮЧЕНИЕ.....	144
ПРИЛОЖЕНИЕ	147
НАУЧНИ ПРИНОСИ.....	151
НАУЧНИ ПУБЛИКАЦИИ ПО ТЕМАТА	152
БИБЛИОГРАФИЯ	153

С Ъ К Р А Щ Е Н И Я

ВО	висше образование
ВУЗ	висше учебно заведение
ДМИС	Директива за мрежова и информационна сигурност
ЕС	Европейски съюз
ЗЗЛД	Закон за защита на личните данни
ЗКИ	защита на класифицирана информация
ИА	информационни активи
ИИ	информационна инфраструктура
ИКТ	информационни и компютърни технологии
ИС	информационната сигурност
ИТ	информационни технологии
КЗП	Комисия за защита на личните данни
КИ	комуникационна инфраструктура
КИИ	критична информационна инфраструктура
КИН	конфиденциалност – интегритет – наличност
КИС	комуникационни и информационни системи
КС	компютърна система
МИС	мрежова и информационна сигурност
МС	Министерски съвет
НП	национален план
НРОВ	Национална рамка за оценка на възможностите
НС	национална сигурност
НСКС	национална стратегия за киберсигурност
ОВ	оценка на възможностите
СПД	системи за проследяване на документи
СУЗО	системи за управление на записването и обучението
СУСИ	система за управление сигурността на информацията
ЦТ	цифрови технологии
GDPR	Общ регламент за защита на данните на Европейския съюз
2FA	двуфакторно удостоверяване
MFA	многофакторно удостоверяване

ТЕРМИНОЛОГИЧЕН РЕЧНИК

Информационна сигурност	<i>„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.“ - Закон за киберсигурност</i>
Сигурност на информацията	<i>организационен ангажимент, който насърчава добрите практики за сигурност на информацията на работното място, така че сигурната среда не само да защитава организацията, но и нейните чувствителни данни и да се грижи за създаване на атмосфера на благоприятен климат и защитеност – авторска дефиниция</i>
Киберсигурност	<i>„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.“ - Закон за киберсигурност</i>
Информация	<i>„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 умозаклучения, 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.“ – авторска дефиниция</i>

Национална сигурност	„динамично състояние на обществото и държавата, при което са защитени териториалната цялост, суверенитетът и конституционно установеният ред на страната, когато са гарантирани демократичното функциониране на институциите и основните права и свободи на гражданите, в резултат на което нацията запазва и увеличава своето благосъстояние и се развива, както и когато страната успешно защитава националните си интереси и реализира националните си приоритети.“ – Закон за управление и функциониране на системата за защита на националната сигурност
Информационна система	„изразител/представител на процесите на събиране, анализ и предоставяне на информация, които се осигуряват и чрез информационни (дигитални, кибер) технологии и хора.“ – Тагарев, Н.
Индустрия 4.0	„съвкупност от свързани цифрови технологични решения, подпомагащи развитието на автоматизацията, интеграцията и обмена на данни в реално време в производствените процеси.“ – Концепция за цифрова трансформация на българската индустрия
Цифрова трансформация	„процес, характеризиращ се с повсеместно внедряване и комбиниране на цифрови технологии във всички сфери на обществения и стопански живот.“ – strategy.bg

УВОД

Съвременното общество е основано на информацията. Тя е движещата сила на века. В един силно развит дигитализиран социум, използването на информация, която може да бъде събирана, предавана, съхранявана в огромни обеми, спомага за разгръщането на *икономика на знанието*¹. Осъзнаването на ИС е неразделна част от защитата на дадена организация от киберзаплахи. Информацията е един от основните ресурси, необходими за осъществяване дейността на всяка организация, включително висшето училище, заедно с финансовите ресурси, трудовите ресурси, материално-техническата база и други. Всички знания и сведения, които се натрупват във висшето образование от хората и информационните системи, формират информация и данни. Информацията не е статична, а е в непрекъснат процес на развитие, а носителите ѝ се променят, заедно с развитието на технологиите. През последните години достъпа до информация се променя поради широкото използване от потребителите на различни устройства и на социални мрежи. Съвременните смартфони, както и социалните медии, променят начина на обмен на информация и създават мрежово общество, което улеснява взаимодействието между организациите и хората, но и обуславят множество рискове за извършване на киберпрестъпления.

България полага усилия за развитие на своята информационна сигурност* в ерата на дигиталното общество и като страна членка на ЕС спазва директивите и законовите рамки за водене на прозрачни политики, свързани с информационната сигурност на обществото. Именно, поддържането на ефективността на дигиталните инфраструктури, е основен и критичен фактор за сигурността на цялата национална система. Набелязването на рисковете и заплахите спомагат за мащабирането на потенциалната киберсреда с нейните възможности и безграничност. Дигиталната зависимост на гражданското общество е сериозна уязвимост в XXI век, тъй като изтичането на данни, отнасящи се до лична и/или обществена информация, крие своите потенциални рискове.

¹ Unger, R. The Knowledge Economy. Available on: <https://www.oecd.org/naec/THE-KNOWLEDGE-ECONOMY.pdf>.

* *сигурност на информацията* и *информационна сигурност* би могло да се използват като синонимни замествания, но в терминологичния речник се извежда спецификата на словосъчетанията и конкретния смисъл, вложен в тях. Научният труд приема схващането, че в контекста на дисертационната разработка се влага единен и непротиворечив взаимнозаменяем смисъл.

В стратегията за национална сигурност на Република България е заложена хуманистичната идея, че сигурността е производна на ценностите на демократичното общество, изповядваните вярвания и култура на нацията, правата и свободите. Въплътеният миролюбив характер и пазените традиции на взаимно сътрудничество и добросъседство спомагат за осигуряването на успешни и ефективни политики в този жизнено важен сектор.

Националните интереси са на първо място – тяхното съхраняване и опазване са дело на всички, които искат те да бъдат отстоявани. Стратегиите за национална сигурност, а в глобализирания свят – един от най-важните аспекти е този на информационната сигурност и защита на личните данни и обществени интереси, допринасят за разгръщането на целенасочени политики.

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.

Проблемите на сигурността на информацията във висшето образование, и в частност на опазването на информацията и данните, са свързани с използването на конкретна информационна среда. При вече създадена и използвана информационна среда въвеждането на системи, чрез които да се повиши сигурността, е значително по-трудоемък процес в сравнение с въвеждане на сигурност по време на разработването на среда. При проектирането на среда за сигурност задължително следва да бъдат спазвани определени принципи, заедно с предприемането на конкретни мерки и дейности за повишаване на сигурността, а именно такива, свързани с предоставяне на минимум привилегии на потребителите, проверяване на пълномощията при достъп до системата, разделяне на ресурсите в базите данни и други.

Глобализацията и бързото развитие на технологиите водят до използването на интернет като средство за комуникация. Активното използване на онлайн пространството предизвиква увеличаване на престъпността в интернет, имаща за цел финансова облага, намаляване доверието в изграден имидж на организации и държавни институции и нанасяне на вреди на цялостното национално икономическо развитие. Основно предизвикателство в съвременния свят е опазването на сигурността на информацията и данните на потребителите и компаниите в онлайн среда. Все повече се увеличават случаите на киберпрестъпления, които могат да бъдат преднамерени или не, както и да варират в широки граници, а последствията от тях могат да бъдат както за отделни хора, така и за цялото общество. Непрекъснатото развитие на технологиите предоставя възможност за използването на всеки един хардуер и софтуер за злонамерени действия в онлайн пространството, като киберпрестъпленията се развиват и обхващат все повече области като изкуствен интелект, дронове, блокчейн, виртуална реалност, биотехнологии и т.н. Основните цели на киберпрестъпленията са: достъп до чувствителна информация, като лични данни, пароли, банкови сметки, търговска информация, счетоводни баланси и др., както и злоупотреба или изтриване на данни и чувствителна информация.

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.

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.

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.

Прави се важно уточнение, че под формулировката *висше образование* се има предвид висшите учебни заведения на територията на Република България.

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.

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

Ограниченията на изследването са свързани с анализиране на предложения модел за намаляване на уязвимостите и заплахите в информационната сигурност във висшето образование до неговото проектиране, без да се навлиза в детайли, свързани с технически характеристики и внедряването му. Поради спецификата на информацията, свързана с проблема за ИС, се използват данни от проучвания в чужди страни, което удостоверява наличието на сравнителния анализ като метод на изследване. Това се изисква от факта, че в България не е налична рамка за следене, съхраняване и контрол на данните за нарушения на ИС.

ПЪРВА ГЛАВА.

ИНФОРМАЦИЯ И ИНФОРМАЦИОННА СИГУРНОСТ – ТЕОРЕТИЧНИ АСПЕКТИ

1.1. Информация – същност, произход и специфика на защитата

1.1.1. Съдържание на понятието

Учените извеждат формулировката за информация като „ценен и важен ресурс“, от който напълно зависи „цялостното икономическо и социално развитие на регионите.“². 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 цели³. 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 защитена⁴.

Въпреки съгласието за това, че съвременният човек живее в общество на информационна ера и че „информацията е основният източник на стойност в глобалната икономика“⁵, самият термин *информация* остава абстрактен и недостатъчно дефиниран.

Думата произлиза от латинската *informare* – давам форма, т.е. информацията винаги е представена с някаква форма, структура, модел; *informatio* – давам представа, понятие за нещо⁶. Оксфордският речник я обяснява като „факти, предоставени или научени за нещо

² 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.

³ Ibidem.

⁴ Семерджиев, Ц. (2007). Управление на информационната сигурност. София: Софттрейд.

⁵ Henno, J. (2014). Information and Information Security. // Proceedings of the 3rd Workshop on Software Quality, Analysis, Monitoring, Improvement, and Applications (SQAMIA).

⁶ Цветкова, М. Внимателна употреба на понятието „информация“. // Медии и обществени комуникации. Достъпно на: <https://media-journal.info/?p=item&aid=155>.

или някого“; „съобщено знание относно конкретен факт, предмет или събитие“⁷, 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“⁸.

Проблемът за същността на информацията е основен теоретичен въпрос в науката за информацията, науката за системите и философията. Предишни изследвания върху онтологията на информацията я разглеждат само от гледна точка на нейното (просто) съществуване⁹, докато ново сегментиране в полето на съществуване в информационно отношение води до нов светоглед, нова екзистенциална картина на света¹⁰. Оттук следва да се изведе дефиницията, че „информацията е маркер на философската категория косвено съществуване, това е самопоказването на начина и състоянието на материалното съществуване (директно съществуване)“¹¹. Тоест, човекът заявява себе си, собствените си намерения съгласно индивидуалните нужди на себетърсене и себенамиране посредством информация.

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“¹². 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 дефиниции¹³. Основателят на теорията на информацията, К. Шанън, счита, че е невъзможно да се поставя доверието на

⁷ Oxford English Dictionary. Available on: <https://www.oed.com/search/dictionary/?scope=Entries&q=information>.

⁸ Krztoń, W. (2021). (In)security of the functioning of the information society in the Cyberspace. // Przegląd Europejski. 3, p. 86.

⁹ Wu, K. (2012). The Essence, Classification and Quality of the Different Grades of Information. // Information. 3(3), pp. 403–419.

¹⁰ Ibidem.

¹¹ Wu, K. (1981). The status and role of information in philosophy. // Potential Sci. J. 3, pp. 53–60.

¹² Цит по: Qiao, T. (2011). Definition and Essence of Information. // triple. 9(2), p. 342.

¹³ Gang, L. (2007). An inquiry into the origin of the philosophy of information. Beijing: JinCheng Press, p. 71.

една-единствена концепция, тъй като информацията подлежи на всички области на науката и научната дейност¹⁴.

Информацията може да бъде както материална, така и ментална, съществуваща или съзнателна, произведена или получена, вярна или невярна, истинска или фиктивна, правилна или грешна, запомнена или забравена, известна или неизвестна; може да съществува обективно, но не може да бъде възприета субективно или обратното; и може да бъде мощна или слаба, да има материална или нематериална стойност и т.н. Информацията, конвенционално разбрана, е сама по себе си противоречива¹⁵.

Парадоксално е, че няма задоволителен и общоприет отговор на ключовия въпрос какво е информация¹⁶. В общата теория за информацията се отразяват свойствата ѝ на природен, социален и технологичен феномен, както и закономерностите на информационното функциониране¹⁷. Уилсън подкрепя общото мнение на учените, че „информация“ е широко използвана дума, която, обаче, създава множество проблеми през годините относно нейното дефинитивно формулиране¹⁸.

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 умозакljučения, 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.**

В допълнение към гореспоменатото се извеждат методологични аргументи, обясняващи защо не е разумно, логично и дори последователно да се разглежда

¹⁴ Ibidem.

¹⁵ Qiao, T. (2011). Op. cit.

¹⁶ Burgin, M. (2003). The Essence of information: paradoxes, contradictions, and solutions. // tripleC. 1(1), pp. 53–70.

¹⁷ Ibidem.

¹⁸ Wilson, T. (1993). Trends and Issues in Information Science – a General Survey. // Media, Knowledge and Power. Groom Helm, London/Sydney, pp.407–422.

информацията като вид знание или знанието като вид информация¹⁹, но **научният труд запазва правото си да възприеме информацията като съществено знание.**

1. Само някои видове информация са свързани със знанието. Има и други видове, които са свързани с емоции, които често се противопоставят на знанието.

2. Според методологичния принцип, наречен „бръснач на Окам“, не е необходимо едно и също нещо да се нарича с две имена: знание и информация. Едно име е достатъчно, а знанието е по-добро в този случай. Освен това свойствата на информацията са съществено различни от свойствата на знанието.

3. В допълнение към това, не е логично да се разглежда информацията като някаква структура, тъй като структурните аспекти на света са обхванати от други научни концепции. Следователно, подобно на материята, е само съд за енергия, но не и самата енергия, статични структури (знание, данни, знаци, текстове и др.) са само носители на информация, докато информацията отразява динамични аспекти на реалността.

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

В Закона за защита на класифицираната информация²⁰ се постановява водещия принцип „*необходимост да се знае*“, който по презумпция извежда идеята за човека като социално животно²¹, което има нужда да съобщава и да му бъде съобщавана някаква новост, новина.

Съществуват няколко източника на риск при предаване и получаване на информация²²:

⇒ загуба на доверие;

⇒ нарушения на сигурността и компютърни престъпления;

¹⁹ Burgin, M. (2003). Op. cit., p. 13.

²⁰ Закон за защита на класифицираната информация. Достъпно на: <https://lex.bg/bg/laws/ldoc/2135448577>.

²¹ Арънсън, Е. (2009). Човекът – „социално животно“. София: Дамян Яков.

²² Bryson, J. (2016). Managing information services: an innovative approach. Farnham, Surrey, UK: Ashgate, pp. 268–269.

- ⇒ 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*“²³, като 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.

Важно уточнение е, че погледнато от ракурса на НС, информацията се разглежда като „*стратегически актив*“²⁴, което предполага, че тя трябва да бъде много добре пазена и съхранявана. *Информационните активи* във вид на материални и нематериални ресурси представляват²⁵:

- ⇒ база данни, съдържаща различна по вид информация като: договори, документи, ръководства, планове и други;
- ⇒ софтуерни активи;
- ⇒ физически активи;
- ⇒ изчислителни и комуникационни ресурси;
- ⇒ човешки ресурс;
- ⇒ нематериални ценности (имидж на организацията).

Съгласно Общия регламент за защита на личните данни (GDPR), правата и неприкосновеността на личните данни, стоят на първо място, като в повечето държави

²³ Kwecka, R. (2016). Information in the Area of Security. New Paradigms. // Journal of Defence Resources Management. 7(2), p. 102.

²⁴ Димов, П., Здравков, З., Добрева, Х. (2021). Информационна сигурност. София: ВА „Георги Раковски“, с. 18.

²⁵ Пак там, с. 19.

правото на защита на личните данни, е заложено в конституцията²⁶. Сигурността на информацията е основно човешко право и този европейски регламент коренно променя начина на организация, контрол и функции с цел защита и съхраняване.

1.1.2. Специфика на защитата на информацията и информационната сигурност

Информационното общество – неговото възникване и развитие, се основават на Информационните и комуникационните технологии (ИКТ) и на интернет като глобална информационна мрежа²⁷. Благодарение на този широк спектър от информационни възможности, се формира т.нар. глобално информационно пространство²⁸, което освен с положителни перспективи, е натоварено с изключително много и непредвидими рискове и заплахи за информационната сигурност.

ИКТ 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 организация²⁹. Глобалните проучвания на състоянието на информационната сигурност съобщават, че служителите са най-разпространеният източник на нарушения на информационната сигурност³⁰. Изследователи от Станфордския университет и водеща организация за киберсигурност установяват, че приблизително 88% от всички пробиви на данни са причинени от грешка на служител. Човешката грешка все още до голяма степен е движещата сила зад огромното

²⁶ Младенов, М. (2018). Административните санкции на основания от GDPR. // Вътрешен одитор. 2, с. 23.

²⁷ Павлов, Пл. (2022). Информационна сигурност. Стандарти от серията ISO 27000 – перспективи и проблеми. Велико Търново, с. 6.

²⁸ Георгиев, К., Георгиева, П. (2015). Предизвикателства пред иновационната парадигма за осигуряване на интелигентен, устойчив и приобщаващ растеж. // Устойчиво развитие, с. 11.

²⁹ Furnell, S. et al. (2012) Power to the people? The evolving recognition of human aspects of security. // Comput Secur. 31(8), pp. 857–1014.

³⁰ PWC. Shaping our future. Global Annual Review 2015. Available on: <https://www.pwc.com/gx/en/about-pwc/global-annual-review-2015/campaign-site/pwc-global-annual-review-2015.pdf>.

мнозинство от проблемите на киберсигурността. Проучването подчертава, че служителите не желаят да признаят грешките си, ако организациите ги съдят строго³¹.

Наивното и случайно поведение на компютърните потребители се счита за най-честата причина за пробиви в информационната сигурност³². Изследователски доклад за киберразследвания на пробиви на IBM показва, че човешката грешка е фактор в 95% от инцидентите със сигурността³³.

Други проучвания осведомяват, че липсата на знания за ИС на управленско ниво е една от причините за неадекватни или несъществуващи стратегии за управление на ИС³⁴.

По своята същност информационната сигурност се възприема като „*защитеност на държавата на стратегическо, оперативно и тактическо ниво*“³⁵, което изразява нейната комплексност и фундаменталност в аспектите на националната сигурност. Тази защитеност се формира въз основа на няколко показателя³⁶:

- ⇒ разрушаване на информационни ресурси;
- ⇒ компрометиране на възможностите за създаване и използване на информация;
- ⇒ (не)преднамерени влияния върху цялата информационна система;
- ⇒ целенасочени действия в посока дезинформация;
- ⇒ несанкциониран достъп върху ИС на държавни органи.

Понятието *сигурност* се използва посредством два основни термина – *интерес* и *заплаха*. Първият оформя гледището за осъзната потребност, ценност, която чрез волята за

³¹ Hancock, J. (2022). Psychology of Human Error. Understand the Mistakes that compromise your Company's Cybersecurity. Tessian. Available on: https://f.hubspotusercontent20.net/hubfs/1670277/%5B%20Tessian-Research-Reports/%5BTessian%20Research%5D%20Psychology%20of%20Human%20Error%202022.pdf?hstc=&__hssc=&hsCtaTracking=8cc3440e-eb09-43bc-962f-51403868c8e0%7C37fefaef-476b-4bea-b78b-6a469a28172a

³² Parsons, K. et al. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). // Comput Secur. 42, pp. 165–176.

³³ IBM Security Services 2014 Cyber Security Intelligence Index. Available on: https://www.editoraroncarati.com.br/v2/phocadownload/ibm_security.PDF.

³⁴ Smith, S., Spafford, E. (2004). Grand challenges in information security: Process and output. // IEEE Security & Privacy, 2(1), pp. 69–71.

³⁵ Павлов, Г. (2010). Защита на информацията. София: УИ „Стопанство“, с. 9.

³⁶ Пак там.

действие, води до задоволяване на потребности. Втората е всичко онова, което пряко или косвено застрашава реализирането на интересите на личността в посока сигурността ù³⁷.

Според Джоузеф Най сигурността е изключително важен въпрос и може да бъде сравнена с кислорода – не се забелязва, докато не се изгуби³⁸. 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 среда³⁹. От друга страна, Цветков счита, че категорията *сигурност* е „сложна и многоаспектна“⁴⁰ 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“⁴¹. 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.

Ученият извежда определение за ИС, като я поставя в един общ план с националната сигурност на страната и я разглежда комплексно като „защитеност на държавата на стратегическо, оперативно и тактическо ниво“⁴² от ракурса на⁴³:

⇒ опити да се разрушат нейни информационни ресурси;

³⁷ Стефанов, Г. (2008). Теория на международната сигурност. София: Сиела, с. 71.

³⁸ Цит. по Poudin, K. (2018). Developing and Maintaining business Security Culture. // Yearbook of UNWE. 1. Sofia: UNWE, pp. 255–269.

³⁹ Ibidem.

⁴⁰ Цветков, Цв. (2016). Съвременен инструментариум за оценяване на сигурността. // Икономически и социални алтернативи. 2, с. 24.

⁴¹ Павлов, Г. (2010) Цит. съч.

⁴² Павлов, Г. (2010). Защита на информацията. София: УИ „Стопанство“, с. 9.

⁴³ Пак там.

- ⇒ опити да се отслабят възможностите ѝ да създава и използва информация;
- ⇒ преднамерени или непреднамерени въздействия върху нейната информационна система;
- ⇒ целенасочено дезинформиране на обществото или на вземащите решения лица и структури;
- ⇒ несанкциониран достъп и въздействие върху информационната система на държавни органи.

Павлов и Пудин определят ИС като способност да се осигури „тайна, цялостност и наличност“⁴⁴, а в историческия си контекст се употребява, за да „изрази комбинация между „компютърна сигурност“ и „комуникационна сигурност“⁴⁵.

По своята същност ИС 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 благосъстоянието⁴⁶.

ИС се свързва с понятийните аспекти на⁴⁷:

- ⇒ тайна – КС да разполага с автентикация и авторизация за достъп;
- ⇒ цялостност – КС да поддържа ненарушима целостта на информацията и информационния поток;
- ⇒ наличност – хардуерът и софтуерът на КС да са ефективни и ефикасни.

Всяка КС е изправена пред рискове и заплахи на сигурността, които се окончават в три основни понятия⁴⁸:

⁴⁴ Павлов, Г., Пудин, К. (2011). Информационна сигурност в организацията. София: УИ „Стопанство“, с. 9.

⁴⁵ Пак там, с. 8.

⁴⁶ 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/StrategicDocuments/View.aspx?lang=bg-BG&Id=655>.

⁴⁷ Павлов, Г. (2010) Цит. съч., с. 11.

⁴⁸ Пак там, с. 12–13.

- ⇒ уязвимост – обуславя се като незащитеност на дадено място, което е уязвимо на атаки. Важен принцип е, че нито една система не е изцяло сигурна, което извежда хипотезата, че съществува вероятност всяка система да пропусне злонамерени атаки. Политиките на сигурността и качествените продукти, които се използват трябва да са с много високо ниво на защитеност;
- ⇒ заплахи – те се разделят на природни, случайни и преднамерени и по своята същност представляват потенциални опасности;
- ⇒ противодействие – събитие, което изисква предприемането на конкретни и целенасочени действия за възпирането и/или премахването на злоумишлени прояви на вредители.

Според Националния институт за стандарти и технологии към САЩ, дефиницията за ИС гласи, че това е защита както на информацията в нейната цялост, така и на информационните системи с неоторизиран достъп в посока разкриване, нарушаване, модифициране или пълно унищожаване с основна цел да се осигури поверителност, цялостност и достъпност на системата⁴⁹. Стъпките, които се следват, са в посока на три основни корелата:

- 1) Цялост – стремеж към осигуряване на предпазни мерки от неправомерни и закононарушаващи действия чрез осигуряване на автентичност на информацията.
- 2) Конфиденциалност – ограничения за достъп и сигурна защита на данни, касаещи личната информация, нейната поверителност и неприкосновеност.
- 3) Достъпност – осигуряване на навременен, достоверен и надежден достъп до информационни ресурси.

ИС се установява в 5 ключови критерия, както следва⁵⁰:

- ⇒ разработване, внедряване и защитеност на ИС в интерес на заинтересованите страни;

⁴⁹ Kissel, R. (Ed.). (2019). NIST Interagency or Internal Report (NISTIR). Glossary of Key Information Security Terms. 7298(2). Washington: U.S. Department of Commerce.

⁵⁰ Димитров, Р. (2018). Насоки за оптимизиране счетоводното отчитане на паричните средства по сметки на бюджетни организации в банките. // Бизнес управление. 1, с. 60–77.

- ⇒ състояние на ИИ, което спомага самата информация да бъде използвана само и единствено по предназначение;
- ⇒ предотвратяване на намерения за нарушаване на конфиденциалността, целостта и достъпността на информацията;
- ⇒ повишаване на ефективността и ефикасността на система за управление на информацията;
- ⇒ ефективност на финансовите информационни бази данни и системите за финансова информация.



Фигура 1
Фактори на информационната сигурност
Източник: Parsons, K. et al. (2017)⁵¹

На Фигура 1 е представен моделът „Знание – Отношение – Поведение“. Въз основа на него се прави заключението, че когато знанията на служителите за безопасното поведение на информационната сигурност на работното място се увеличават, тяхното отношение се подобрява, което води до подобро поведение на информационната сигурност⁵².

⁵¹ Parsons, K., Calic, D., Pattinson, M. et al. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. // Computers & Security. 66, pp. 40–51.

⁵² Parsons, K. et al. (2014). Op. cit.

Осведомеността на служителите относно ИС е жизненоважна за смекчаване на рисковете, свързани с нарушения⁵³. Хората многократно се наричат „*първата линия на защита*“⁵⁴ срещу различни заплахи за информационната сигурност – особено важна за организациите, които искат да протектират чувствителна организационна и клиентска информация.

Дефинициите на ИС 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 организация⁵⁵. Kruger et al.⁵⁶ определят това като степен, до която всеки член на персонала разбира важността на ИС, 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 ИС⁵⁷.

Информацията, като ключов актив на една организация, е ценна, но в същото време и чувствителна, тъй като през нейния жизнен цикъл може да бъде прихваната, модифицирана, прекратена, измислена или унищожена⁵⁸. Следователно, както е посочено в международния стандарт ISO/IEC 27002, информационната сигурност е „*защитата на информацията от широк спектър от заплахи, за да се осигури непрекъснатост на бизнеса, минимизиране на бизнес риска и максимизиране на възвръщаемостта на инвестициите и бизнес възможностите*“⁵⁹. В същото време, с повишаване нивата на сигурност на тази информация, установената информационна сигурност постига

⁵³ Arachchilage, N. et al. (2014). Security awareness of computer users: a phishing threat avoidance perspective. // Comput Human Behav. 38, pp. 304–312.

⁵⁴ European Union Agency for Network and Information Security (ENISA). (2010). The new users' guide: how to raise information security awareness (EN). Available on: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide.

⁵⁵ 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.

⁵⁶ Kruger, H. et al. (2006) A prototype for assessing information security awareness. // Comput Secur. 25(4), pp. 289–296.

⁵⁷ Ibidem.

⁵⁸ Wang, J., Guo, M. (2009). Security Data Mining in an Ontology for Vulnerability Management. // Proceedings of the International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing, pp. 597–603.

⁵⁹ International Organization for Standardization. (2005). ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management.

допълнително количество информация, което затруднява манипулирането и управлението на информацията. Поради големия обем информация, получена от различни източници, като например системни записи, регистрационни файлове на защитната стена или предупреждения за уязвимости, администраторите по сигурността са изправени пред труден проблем за ефективно генериране на знания за проблеми със сигурността на информацията, предупреждения и инциденти, пред които са изправени и трябва да направят правилни решения⁶⁰.

1.1.3. Предизвикателства пред защитата на информацията в условията на четвъртата индустриална революция

Разработването и успешното внедряване на политика за сигурност, е сложен, многопластов и отговорен процес на национално ниво⁶¹. 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 решения⁶².

Терминът „Индустрия 4.0“ се използва в смисъла на четвърта индустриална революция, като на практика се извеждат основните доминанти на явлението⁶³:

- ⇒ ИКТ;
- ⇒ киберсистеми;
- ⇒ съхранение, обработване и защита на огромни масиви от данни в т.нар. облачни системи;
- ⇒ изграждане на системи за моделиране, стимулиране и виртуално представяне на информацията;

⁶⁰ Martimiano, L., Moreira, E. (2005). An OWL-based Security Incident Ontology. // Proceedings of the Eighth International Protege Conference, pp. 1–4.

⁶¹ 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.

⁶² Матеев, М. (2000). Анализ и оценка на риска при избор на инвестиционни решения. София: Стопанство, с. 8.

⁶³ Радев, К. (2018). Четвъртата индустриална революция – предизвикателства пред предприемачеството и управлението на бизнеса. // Научни трудове. 4. УНСС, 47–60.

⇒ подобряване на инструментите за взаимодействие между човек – машина.

Добавена реалност, машинна автоматизация и други довеждат до твърдението, че индустриалната революция на XXI век е цифрова. Индустрия 4.0 се отнася до настоящата ера на свързаност, подобрени анализи, автоматизация и усъвършенствани производствени технологии, които трансформират глобалния бизнес от години⁶⁴. Тази вълна от промени в производствения сектор започва в средата на 2010 г. и притежава значителен потенциал за операциите и бъдещето на производството⁶⁵.

Терминът „Индустрия 4.0“ е публично представен през 2011 г. на панаира в Хановер⁶⁶, 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 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 производство⁶⁷. 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“⁶⁸, което позволява гъвкаво производство на висококачествени персонализирани продукти при масова ефективност⁶⁹.

Самият термин препраща към индустрия (инициатива, насочена към производството), нула (интернет технологии), четири (ново ниво по веригата на

⁶⁴ What are Industry 4.0, the Fourth Industrial Revolution, and 4IR? Available on: <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir>.

⁶⁵ Ibidem.

⁶⁶ Vogel-Heuser, B., Hess, D. (2016). Guest editorial: Industry 4.0—prerequisites and visions. // IEEE Trans Autom Sci Eng. 13.

⁶⁷ 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.

⁶⁸ 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.

⁶⁹ 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.

индустриална стойност), като елементите свързват идеята за достигане на ново потребителско ниво на индустриална стойност⁷⁰, изцяло свързано и зависимо с web каналите на комуникация и информация.

Принципите на Индустрия 4.0 са⁷¹:

- ⇒ взаимно свързване – посредством wifi и интернет всички устройства може да контролират процесите по обмен на информация;
- ⇒ прозрачност – предоставените информация и количество данни, спомагат за по-бързото и адекватно взимане на важни решения;
- ⇒ децентрализация – комбинирането на местна и глобална информация спомага за по-голямата ефективност и ефикасност на индустриалните процеси, както и за увеличаването на цялостната производителност;
- ⇒ техническа помощ – системите за подпомагане и вземане на информирани решения спомагат за решаването на проблемите в най-кратък срок.

Именно индустриалните отношения в глобализираното общество *„водят до търсене и постигане на възможният за определен период баланс между икономическите и социалните интереси“*⁷², което се постига благодарение на Индустрия 4.0.

Предизвикателствата пред този тип индустриална революция са⁷³:

- 1) Замяна на труда с капитала – довежда до нарушаване на трудовите отношения поради едностранното присвояване на печалбата.
- 2) Поява на дигитални платформи – те са своеобразни посредници между производителите и потребителите на стоки и услуги, което води до монопол и коренни промени в условията на покупко-продажба.

⁷⁰ Овчарова, Ж. (2019). Внедряване на индустрия 4.0 в малките и средни предприятия: минимизиране на рисковете и определяне на възможностите. // Индустрия 4.0. Предизвикателства и последици за икономическото и социалното развитие на България. София: ФФЕ.

⁷¹ Hermann, M., Pentek, T. Otto, B. (2015). Design Principles for Industrie 4.0 Scenarios: A Literature Review. // Working Paper. 01.

⁷² Евгениев, Е. (2019). Бъдещето на труда и индустриалните отношения. // Труд и социална справедливост. Фондация „Фридрих Еберт“, с. 12.

⁷³ Пак там, с. 13–15.

- 3) Внедряването на дигитални технологии – довежда до заличаването на множество професии, свидетели сме на явлението изкуствен интелект, който заплашва роботът да измести човека.
- 4) Национална специфика – процесът на реализация се усложнява предвид продължаващата демографска криза, нестабилните микро- и малки предприятия, ниските доходи и жизнен стандарт.



Фигура 2
Предизвикателствата на Индустрия 4.0
Източник: авторска интерпретация

Министерството на икономиката и индустрията създава Концепция за цифрова трансформация⁷⁴, в която се посочва, че Индустрия 4.0 създава „*предпоставки за модернизирание, автоматизиране и конкурентно позициониране на българската икономика*“. Растежът на новите технологии поражда именно тази необходимост за изграждане на човешки, институционален и организационен капацитет, който ще доведе до технологичен, икономически и социален прогрес. Навлизането на цифровите технологии в глобален мащаб създава динамика и конкурентоспособност – предпоставки за най-пълноценно разгръщане на възможностите на всяка една организация. По своята същност

⁷⁴ Концепция за цифрова трансформация на българската индустрия (Индустрия 4.0). Достъпно на: <https://www.mi.government.bg/files/useruploads/files/ip/Industry4.0.pdf>.

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.“⁷⁵ 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.

Основните характеристики са⁷⁶:

- ⇒ оптимизация при вземане на решения;
- ⇒ ресурсна продуктивност и ресурсна ефективност;
- ⇒ индивидуален подход към потребителите;
- ⇒ гъвкавост;
- ⇒ потенциал за създаване на стойност чрез предлагане на качествено нови услуги.



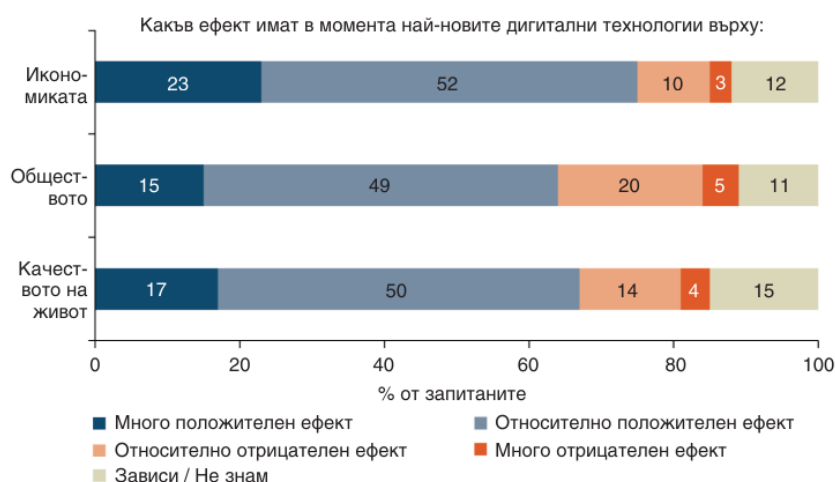
Фигура 3
Характеристики на Индустрия 4.0
Източник: авторова интерпретация

⁷⁵ Пак там.

⁷⁶ Пак там.

Под термина се разбира също „технологии, които съчетават хардуер, софтуер и биотехнологии“⁷⁷, като революцията на информационното общество е „белязана от иновативни пробиви в области като роботика, изкуствен интелект, нанотехнологии, квантови технологии, компютри“⁷⁸ и прочее иновации. Това променя коренно общественения живот, като не се изключва и пазара на труда.

Водещ доклад за световното развитие⁷⁹ провежда проучване, в което респондентите са на мнение, че технологиите подобряват европейската икономика, обществото и качеството на живот.



Фигура 4
Ефект на дигиталните технологии
 Източник: Екип на Доклада за световно развитие 2019⁸⁰

В отговор на променящата се среда обществата се възползват от потенциалните алтернативи, които предлагат технологиите. Те са свързани с ефектите, политиките и социалното включване на базата на променящите се условия и начин на живот, на публичните политики, които спомагат да се произведе инвестиране в човешкия капитал, засилване на социалната защита и мобилизиране на печалбите.

⁷⁷ РБ. Икономически и социален съвет. (2019). Предизвикателства пред труда в контекста на цифровизацията на икономиката. Достъпно на: <https://esc.bg/wp-content/uploads/2021/01/opinion-esc-3-060-2019-bg-1.pdf>.

⁷⁸ Пак там.

⁷⁹ Световна банка. (2019). Променящата се природа на работата. Доклад за световното развитие 2019. Washington, DC 2.

⁸⁰ Пак там, с. 9.



Фигура 5
Политики за дигитална сигурност
Източник: Екип на Доклада за световно развитие 2019⁸¹

Извежда се твърдението, че Икономика 4.0 е съсредоточена върху два основни аспекта – външен (макрофактор), съвместяващ новите технологии, и вътрешен, който отговаря за технологичния ресурс на организацията⁸².

Обикновено революцията в индустрията се движи от трансформация технологичен напредък, който довежда до фундаментални промени в начина, по който функционира индустрията. Тези промени имат икономически и обществени последици. Някои са предвидени и желани, други – непредвидени и нежелани. Подобно на други предшественици, Индустрия 4.0 се ръководи от технологиите, докато Индустрия 5.0 – от стойността. Първото се нуждае от второто, за да напомня за основните обществени нужди, стойност и отговорност като крайни цели, а последното изисква първото за технологичните тласъци и решения⁸³.

⁸¹ Пак там, с. 12.

⁸² Бошняку, А. (2023). Особенности на бизнес средата в контекста на Индустрия 4.0. // Диалог. 1, с. 17.

⁸³ Xu, X. et al. (2021). Op. cit.

1.1.4. Съвременни тенденции в осигуряването на информационната сигурност и управление на риска. Киберсигурност и киберпрестъпления

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 сигурност⁸⁴, 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 на обмен на електронни документи. Контролът се осъществява от председателя на Държавната агенция за информационни технологии и съобщения.

От изключителна значимост е практическата приложимост на Националната рамка за оценка на възможностите към Агенцията на Европейския съюз за киберсигурност⁸⁵. Основната цел на Рамката е да „осигури на държавите членки самооценка на равнището им на зрялост“⁸⁶, което е индикатор за подобряване възможностите за изграждане на стратегическа и оперативна киберсигурност. ДМИС изисква от държавите членки на ЕС да приемат националната стратегия, в която са заложили стратегическите принципи, цели, приоритети, политики и регулаторни мерки. Изхожда се от предпоставката, че киберсигурността е сложно предизвикателство, което обхваща множество различни аспекти на управление, политика, оперативни, технически и правни аспекти⁸⁷.

⁸⁴ 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.

⁸⁵ Национална рамка за оценка на възможностите. Достъпно на: <https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-bg.pdf>.

⁸⁶ Пак там.

⁸⁷ Guide to Developing a National Cybersecurity Strategy. Available on: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

Равнището на зрялост в компонента киберсигурност създава ОВ – водещ инструмент, който спомага да се предостави⁸⁸:

- ⇒ информация за разработване на дългосрочна ефективна стратегия;
- ⇒ идентификация на липсващи елементи от НСКС;
- ⇒ потенциални възможности за киберсигурност;
- ⇒ отчетност на политически действия;
- ⇒ надеждност за обществеността и за международната партньорска мрежа;
- ⇒ подобряване на националния имидж и прозрачност на водените политики;
- ⇒ идентифициране на най-добри практики;
- ⇒ оценка на националните възможности в сектор „Киберсигурност“.

НРОВ (Национална рамка за оценка на възможностите) има общо 17 стратегически цели за киберсигурност, които са структурирани в 4 клъстера, показани на Таблица 1:

		Таблица 1 Национална рамка за оценка на възможностите
КЛЪСТЕР № 1	Управление и стандарти за киберсигурност	1. Разработване на НП за действие при извънредни ситуации. 2. Базови мерки за сигурност. 3. Цифрова идентичност и цифрови обществени услуги.
КЛЪСТЕР № 2	Изграждане на капацитет и осведоменост	1. Дейности по киберсигурност. 2. Реагиране при заплахи. 3. Повишаване на осведомеността. 4. Засилване на обучението. 5. Насърчаване на научно-изследователската дейност. 6. Стимули, инвестиции и мерки за сигурност. 7. Подобрения по веригата за доставки.

⁸⁸ Национална рамка за оценка на възможностите. Цит. съч.

КЛЪСТЕР № 3	Правни и регулаторни въпроси	1. Защита на КИИ. 2. Предотвратяване на киберпрестъпления. 3. Механизми за докладване на инциденти. 4. Защита на личните данни и неприкосновеността.
КЛЪСТЕР № 4	Сътрудничество	1. Публично-частно партньорство. 2. Институционализиране и сътрудничество между публичните агенции. 3. Участие в международно сътрудничество.

Източник: <https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-bg.pdf>

В Националната стратегия за киберсигурност „Киберустойчива България 2020“ на МС⁸⁹ се посочва отговорността на ръководството на страната за осигуряване на стабилна среда за развитие на киберсигурността за едно устойчиво и безопасно пространство. В стратегическата рамка се набелязват 9 фундаментални области за предотвратяване и преодоляване на „*еволюиращите киберзаплахи и кризи*“⁹⁰:

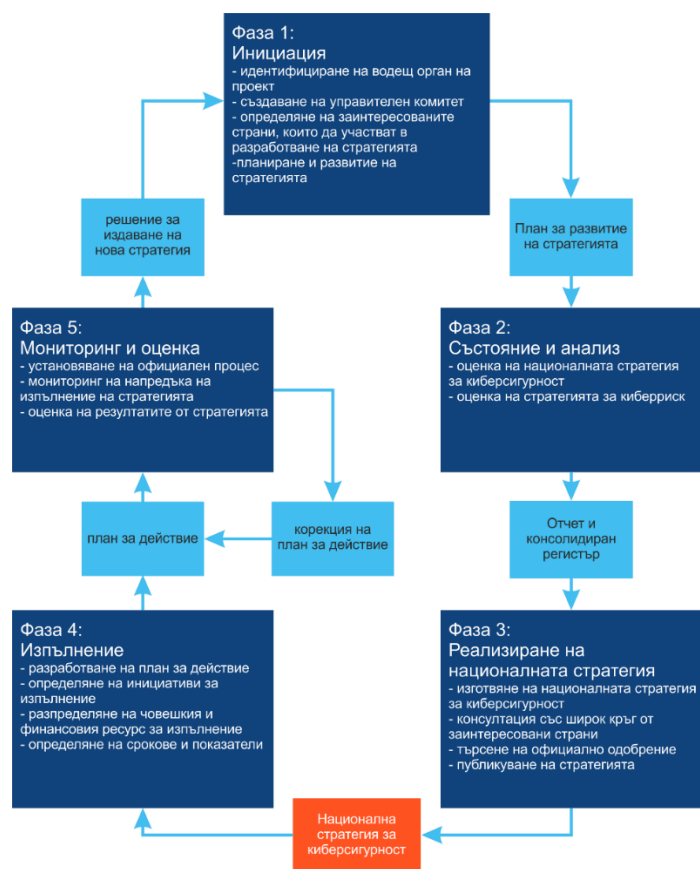
- 1) Установяване и развитие на националната система за киберсигурност и устойчивост.
- 2) Мрежовата и информационна сигурност – фундамент на киберустойчивостта.
- 3) Защита и устойчивост на дигитално зависимите критични инфраструктури.
- 4) Подобряване на взаимодействието и споделянето на информация между държава, бизнес и общество.
- 5) Развитие и подобряване на регулаторната рамка.
- 6) Засилване на противодействието на киберпрестъпността.

⁸⁹ Националната стратегия за киберсигурност „Киберустойчива България 2020“. Достъпно на: <https://www.strategy.bg/StrategicDocuments/View.aspx?Id=1120>.

⁹⁰ Пак там.

- 7) Киберотбрана и защита на националната сигурност.
- 8) Повишаване на осведомеността, знанията и компетентностите и развитие на стимулираща среда за изследвания и иновации в областта на киберсигурността.
- 9) Международно взаимодействие - кибердипломация и оперативно взаимодействие*.

Извежда се образа на България в съвременното киберпространство, като се показват дигиталната зависимост, заплахите, сигурността, предизвикателствата, рисковете и възможностите. Определят се и факторите за ефективно постигане на целесъобразността във фазите на прилагане и развитие на националната стратегия.

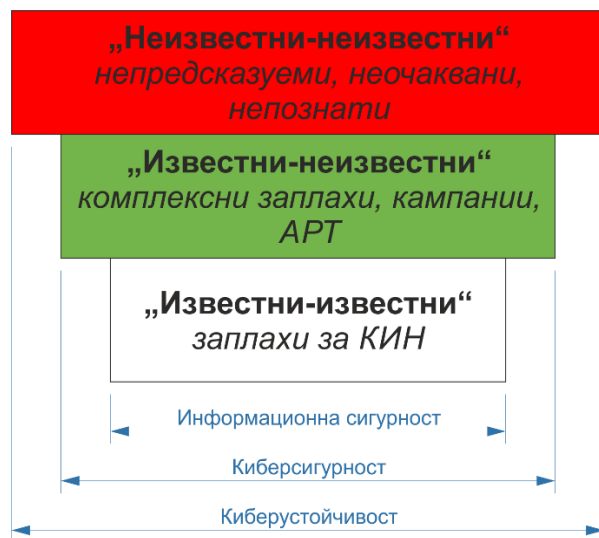


Фигура 6
Национална стратегия за киберсигурност
 Източник: Национална стратегия за киберсигурност

* Всички мерки са дословно цитирани от документа за Национална стратегия за киберсигурност.

За постигането на стратегически обозримите цели на едно киберустойчиво общество се набелязват областите на действие и целите, които са:

- ⇒ ефективност и комплексност при наличие на неизвестни заплахи и разрушителни въздействия в киберсредата;
- ⇒ запазване, съхраняване и функциониране на жизнено важни ресурси;
- ⇒ възстановяване на нормалните граници на действие.
- ⇒ информационна сигурност в триадата конфиденциалност – интегритет – наличност (КИН);
- ⇒ ниво на познаване на заплахи и рискове в класификацията *известните* – *неизвестните*.
 - *известни* – *известни* – защита на ИА и КИ от различни по вид и интензитет заплахи (КИН);
 - *известни-неизвестни* – комплексни и комбинирани заплахи, свързани с ИС (не-КИН).



Фигура 7

Области на действие и цели на Националната стратегия по киберсигурност

Източник: <https://www.strategy.bg/StrategicDocuments/View.aspx?Id=1120>

Законът за киберсигурност на Република България⁹¹ урежда организацията, управлението и контрола по киберсигурност, както и предприемането на мерки за постигане на *„високо общо ниво на мрежова и информационна сигурност“*⁹². 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.“*⁹³. 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.“*⁹⁴. Като мерки за безопасност и предотвратяване на потенциални рискове и заплахи, се прилагат организационни, технологични и технически способности 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 сигурност, използваните организационни

⁹¹ Закон за киберсигурност. Достъпно на: <https://lex.bg/bg/laws/ldoc/2137188253>.

⁹² Пак там.

⁹³ Пак там.

⁹⁴ Пак, там.

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 контроли⁹⁵.

2.1. Висшето образование като обект на информационна сигурност

2.1.2. Нормативни актове, политики, стандарти и процедури, регулиращи информационната сигурност във висшето образование

Националната програма за развитие „България 2030“⁹⁶ е един от най-важните рамкови стратегически документи, чрез които се определя визията, политиките и организацията за развитие във всички държавни институции. В приоритет „Цифрова свързаност“ целта на програмата е *„изграждане на мрежи с много голям капацитет, което ще осигури платформа за предоставяне на разнообразни цифрови услуги с добавена стойност, като едновременно с това гарантира, че никоя част от страната или група в обществото няма да остане без адекватна цифрова свързаност.“*⁹⁷. Основните области на въздействие, които се изброяват, са:

⇒ високоскоростна свързаност;

⇒ мобилни мрежи 5G.

⁹⁵ 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>.

⁹⁶ Националната програма за развитие „България 2030“. Достъпно на: <https://www.minfin.bg/bg/1394>.

⁹⁷ Пак там, с. 61.

Цифровата инфраструктура цели да се постигне изграждането на ефективна облачна система, както и валидни инструменти за обмен на данни, архитектура и механизми, също така и екосистеми за изкуствен интелект. Областите на въздействие тук са:

- ⇒ центрове за данни;
- ⇒ облачна инфраструктура.

При индикатора за цифрово включване основната цел е да се преодолеят териториалните дисбаланси с разпространението на ширококолов достъп, като по този начин ще се доведе до благотворно влияние на икономически и социални ползи. Областите на въздействие са:

- ⇒ свързаност за центрове на социалния живот;
- ⇒ безплатен достъп до интернет.

Законът за управление и функциониране на системата за защита на националната сигурност урежда управлението и функционирането на системата за защита. По смисъла на Чл. 2 под термина *национална сигурност* Законът счита: „*динамично състояние на обществото и държавата, при което са защитени териториалната цялост, суверенитетът и конституционно установеният ред на страната, когато са гарантирани демократичното функциониране на институциите и основните права и свободи на гражданите, в резултат на което нацията запазва и увеличава своето благосъстояние и се развива, както и когато страната успешно защитава националните си интереси и реализира националните си приоритети.*“⁹⁸. В този закон се прилага:

- ⇒ анализ на спецификите и зависимостите в средата за сигурност;
- ⇒ предотвратяване на рискове;
- ⇒ управление и преодоляване на кризи;
- ⇒ защита на критичната инфраструктура.

⁹⁸ Закон за управление и функциониране на системата за защита на националната сигурност. Достъпно на: <https://lex.bg/bg/laws/ldoc/2136588572>.

При управлението на системата за защита на НС на първо място се поставят националните интереси и приоритети на висшите училища в страната⁹⁹.

Законът за висшето образование постановява устройството, функциите, управлението, финансирането¹⁰⁰.

В Наредбата за минималните изисквания за мрежова и информационна сигурност се извеждат основните принципни постановки за постигането на целесъобразност спрямо МИС. По този начин се гарантира съхраняването на *„достъпността, интегритета (цялост и наличност) и конфиденциалността на информацията по време на целия ѝ жизнен цикъл (създаване, обработване, съхранение, пренасяне и унищожение) във и чрез информационните и комуникационните системи на Субекта.“*¹⁰¹.

Управлението на МИС според Наредбата по Чл. 3, ал. 1 се възлага на административният орган, който носи пряка отговорност, създава условия за прилагане на комплексна система от мерки за управление, осигурява необходимите ресурси за прилагане и упражнява контрол посредством:

⇒ одитиране;

⇒ минимум веднъж годишно периодичен преглед на МИС.

Наредбата за сигурността на комуникационните и информационните системи определя задължителните условия за сигурност на КИС за създаване, обработване, съхраняване и обмен на информация¹⁰². Органът по акредитиране на сигурността разполага със следните правомощия¹⁰³:

⇒ препоръки и указания за сигурността;

⇒ препоръки за стандарти и средства за ЗКИ;

⁹⁹ Пак там.

¹⁰⁰ Закон за висшето образование. Достъпно на: <https://lex.bg/laws/ldoc/2133647361>.

¹⁰¹ Наредбата за минималните изисквания за мрежова и информационна сигурност. Достъпно на: https://www.mtc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf.

¹⁰² Наредба за сигурността на комуникационните и информационните системи. Достъпно на: https://www.dksi.bg/media/1619/naredba_za_sigurnostta_na_komunikacionnite_i_informacionnite_sistem_i.pdf.

¹⁰³ Пак там.

- ⇒ утвърждава документите по сигурността;
- ⇒ извършва комплексна оценка;
- ⇒ издава сертификати;
- ⇒ определя условията за акредитация;
- ⇒ контролира и координира дейностите;
- ⇒ провежда обучения;
- ⇒ води регистър на сертифицираните КИС;
- ⇒ отнема и прекратява действието на сертификати;
- ⇒ одобрява механизми за защита;
- ⇒ определя стандарти;
- ⇒ определя условия и етапи за акредитация.

В Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност се определят общите изисквания на същите, методиката за оценяване, изискванията за водене, съхранение и достъп до списъка на акредитираните лица¹⁰⁴. Политиката за ИС в Наредбата постановява в Чл. 24, че всички ИС на административни органи следва да отговарят на изискванията срещу неправомерен или случаен достъп, промяна или унищожаване, като тези действия може да нарушат автентичността, целостта, конфиденциалността на съхраняваните данни. Ръководителите на администрациите са отговорни за МИС посредством утвърдените от тях вътрешни правила. Управлението на достъпа и защитата срещу неправомерен достъп следва да се придържа към класификацията:

Таблица 2
Нива на достъп според класификация

Ниво 0 или D	ниво на свободен достъп
Ниво 1 или C	ниво на произволно управление на достъпа

¹⁰⁴ Наредба за общите изисквания за оперативна съвместимост и информационна сигурност. Достъпно на: <https://www.netlaw.bg/p/n/o/noiosis.rtf-677-91.pdf>.

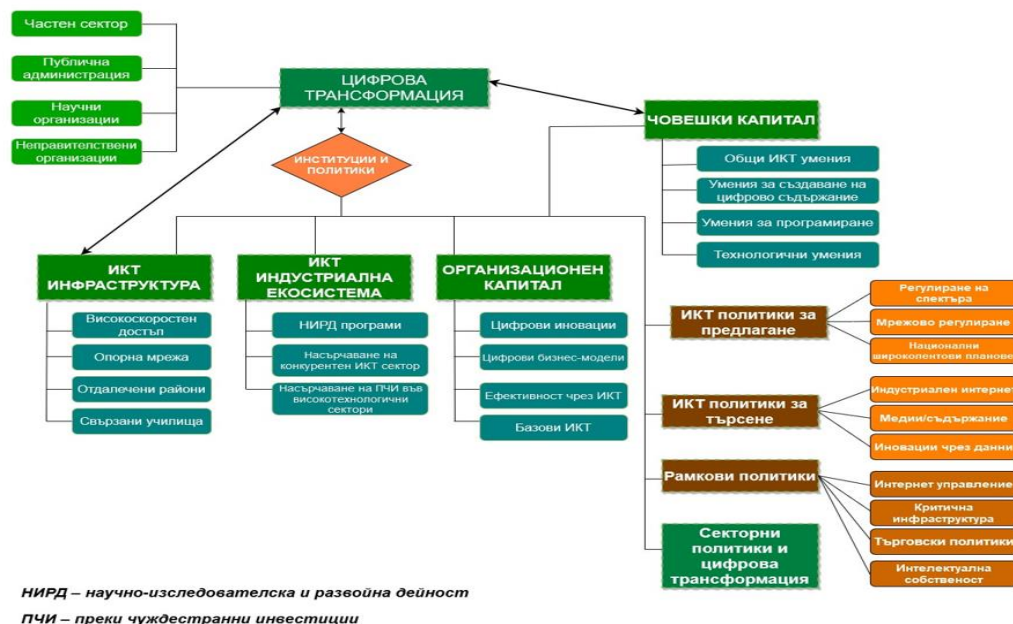
Ниво 2 или В	ниво на принудително управление на достъпа
Ниво 3 или А	ниво на проверена сигурност.

Източник: Наредба за общите изисквания за оперативна съвместимост и информационна сигурност

Ръководителите са задължени да извършват мониторинг според вътрешните правила на МИС.

В Проекта за Цифрова трансформация на България¹⁰⁵ се налага схващането, че ЦТ налага сериозната необходимост от преосмисляне на досегашните подходи по отношение използване на потенциала и повишаване конкурентоспособността.

ЦТ е дефинирана като „процес, характеризиращ се с повсеместно внедряване и комбиниране на цифрови технологии във всички сфери на общественения и стопански живот.“¹⁰⁶.



Фигура 8
Цифрова трансформация
Източник: Strategy.bg

¹⁰⁵ Цифрова трансформация на България за периода 2024-2030 г. Достъпно на: <https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1661>.

¹⁰⁶ Пак там.

На Фигура 8 е показан целият процес по ЦТ, който обхваща ИКТ инфраструктурата, ИКТ индустриална екосистема, организационен капитал, човешки капитал. Ускоряването на процесите по ЦТ, неминуемо ще доведе до развитие на икономиката.

Въвежда се механизъм за наблюдение и сътрудничество по европейската политическа програма „Цифрово десетилетие“, съгласно който се създава среда за иновации и инвестиции, стимулиране на сътрудничеството и насърчаване на съгласувателни политики и прозрачност.

Принципите, които изповядва стратегията, са¹⁰⁷:

- 1) Ориентиран потребителски подход на равнопоставен достъп.
- 2) Етичност и социална отговорност при споделяне и управление на данните.
- 3) Внедряване на модерни технологии.
- 4) Прилагане на система от норми и стандарти за киберсигурност.
- 5) Сътрудничество.

Предизвикателствата пред цифровото управление на данни не са малко, но държавните институции носят цялата отговорност за създаването на капацитет за Единен европейски цифров пазар, който благоприятства¹⁰⁸:

- ⇒ инвестиции в по-голяма и в по-добра свързаност;
- ⇒ засилване на индустриалното и технологично присъствие на ЕС, т.е. неговия технологичен суверенитет;
- ⇒ инвестиции за възстановяване в цифрови капацитети, съоръжения, технологии – 5G/6G, изкуствен интелект, квантови технологии и т.н.;
- ⇒ истинска икономика на данни и създаване на пространства за данни.

В ход е Програмата „Цифрова Европа“, която е насочена към предоставянето на цифрови технологии в отговор на предизвикателствата на съвременния свят¹⁰⁹. Чрез нея се

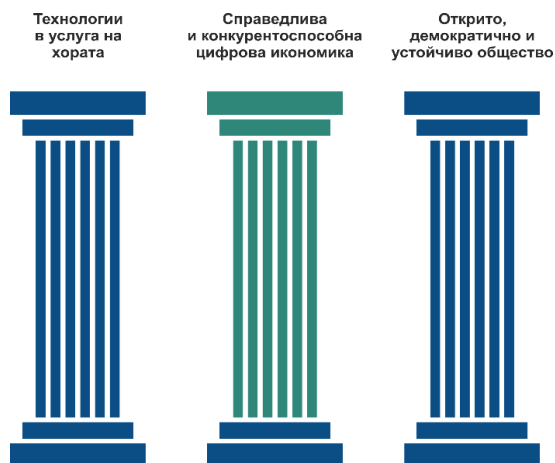
¹⁰⁷ Пак там.

¹⁰⁸ Пак там.

¹⁰⁹ Програма „Цифрова Европа“. Достъпно на: <https://digital-strategy.ec.europa.eu/bg/activities/digital-programme>.

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 трансформация¹¹⁰:

- ⇒ **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.



Фигура 9
Три стълба на цифрова икономика и цифрова трансформация според ЕС
Източник: <https://commission.europa.eu>

¹¹⁰ 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.

2.2.2. Изграждане на информационна система във висшето образование за осигуряване сигурност на информацията

Изграждането на информационна система във ВО, се подчинява на политиката по МИС. По този начин ИС 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 заведение¹¹¹. 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 потребители¹¹².

По своята същност ИС е *„изразител/представител на процесите на събиране, анализ и предоставяне на информация, които се осигуряват и чрез информационни (дигитални, кибер) технологии и хора.“*¹¹³.

Средствата за защита на информацията се класифицират по следния начин¹¹⁴:

- ⇒ защита от несанкциониран достъп – т.нар. защитни стени (FireWall);
- ⇒ защита на e-mail;
- ⇒ защита от вируси и злонамерени софтуерни атаки;
- ⇒ осигуряване на регламентиран достъп;
- ⇒ разделяне на достъпа;
- ⇒ активна директория;
- ⇒ системи за откриване и проникване;
- ⇒ нестандартни методи за защита;
- ⇒ управление на сигурността.

На предложения модел на

¹¹¹ Димов, П. и др. (2021). Цит. съч., с. 150.

¹¹² Пак там.

¹¹³ Тагарев, Н. (2021). Съвременни подходи при управлението на киберсигурността. Ч. 1. София: Авангард Прима, с. 20.

¹¹⁴ Димов, П. и др. (2021). Цит. съч., с. 150–151.

за осигуряването на ИС се показва, че има две основни звена: политика и контрол на системата. Към първото се отнасят различните разновидности на управлението: персонал, процеси, технологии, организация. Към втория раздел се отнасят управленията на: критичните приложения, компютърните инсталации, комуникационната инфраструктура. Може да се направи извода, че ИС е хардуера и софтуера на националната сигурност на държавата в отрасъла висше образование.



Фигура 10
Изграждане на информационна система
Адаптирано по Туджаров, Х. (2009)¹¹⁵

Политиката на ИС за предоставяне на безопасност, адекватност и прозрачност на управляваните процеси се подчинява на:

- 1) Осведоменост – необходимостта от сигурност води до повишаване нивата на самата сигурност.
- 2) Отговорност – всички заинтересовани страни по управлението на ИС са пряко отговорни към създалите се процеси.

¹¹⁵ Туджаров, Х. (2009). Въведение в информационната сигурност. Достъпно на: <https://www.tuj.asenevtsi.com/>: <https://www.tuj.asenevtsi.com/Sec2009/Sec01.htm>.

- 3) Реакция – своевременното и отговорно действие на участниците и заинтересованите страни спомага за адекватното реагиране на инциденти по сигурността.
- 4) Проектиране, внедряване и управление на сигурността – разработването на ключови механизми спомага за ефективното и ефикасно представителство на МИС.
- 5) Преоценка – преразглеждането и преоценяването на различни процедури, мерки, практики, следва да се прилагат веднъж годишно, за да се избегнат рисковете от различни по интензитет атаки.

С изграждането и налагането на модел на ИС във висшето образование, се цели да се постигне:

- ⇒ пълна и адекватна защита на информацията от неразрешен достъп;
- ⇒ съхраняване на поверителността на информацията;
- ⇒ невъзможност да се разкрие информация на неоправомощени лица;
- ⇒ непокътнатост на информацията;
- ⇒ предоставяне на информация на оправомощени лица при нужда;
- ⇒ стриктно спазване на законовите и нормативните уредби на Република България;
- ⇒ разработване и внедряване на план за непрекъсваемост на сигурността на информацията;
- ⇒ защитни механизми против теч на информация;
- ⇒ двуфакторни удостоверения за вход и изход в информационния ресурс;
- ⇒ обучение по ИС на всички преки участници в информационния обмен;
- ⇒ ежегоден мониторинг за превенция на безопасността на информацията;
- ⇒ документиране и разследване на случаи и/или съмнения за нарушение на сигурността на информацията.

Основните направления са:

- ⇒ информацията да бъде защитена, тъй като се явява собственост на субекта на предявени права;
- ⇒ предпазване на информация, съдържаща лични данни;
- ⇒ съхраняване на информационните активи;
- ⇒ осигуряване на доверие към всички заинтересовани страни.

Основните стратегически и оперативни цели на МИС са:

- ⇒ усъвършенстване на информационната и технологична среда във ВУЗ;
- ⇒ осигуряване на надеждност и достъпност на качеството на информация;
- ⇒ осигуряване на интегритет на данните, съобразно нормативните изисквания;
- ⇒ създаване на план за непрекъсваемост на ИС;
- ⇒ управление на рисковете за сигурност;
- ⇒ управление на сключените договорености с трети страни;
- ⇒ осъществяване контрол на дейността;
- ⇒ оценка на риска;
- ⇒ управление на човешките ресурси;
- ⇒ управление на физическата сигурност;
- ⇒ контрол на достъпа;
- ⇒ осигуряване на непрекъснатост на процесите.

ИС се реализира посредством специализирана система, която се нарича СУСИ. Тя следва да разполага с набор от мерки като¹¹⁶:

- 1) Политика за ИС.
- 2) План за оценка на рисковете.

¹¹⁶ ISO/IEC 27001: 2013. (2016). Информационни технологии. Методи за сигурност. Системи за управление сигурността на информацията. Изисквания. Техническа справка. 2.

- 3) Списък на информационните активи.
- 4) Стандартни оперативни процедури.
- 5) Контрамерки за минимизиране на риска.

Инвестирането в сигурни и надеждни системи за защита на информацията, е начин организацията да се предпази от злонамерени атаки и да предотвратява рискове с безопасността.

Основните понятия, свързани с ИС, са¹¹⁷:

- ⇒ **противодействия** – съвкупност от техники за защита на КС;
- ⇒ **компютърна сигурност** – защита на информацията, която бива съхранявана в системи;
- ⇒ **комуникационна сигурност** – защита на информацията по време на нейното транспортиране в различни канали;
- ⇒ **физическа сигурност** – защита на оборудването от повреди, предизвикани от бедствия или зла умисъл.

Винаги трябва да се спазват принципите на политиките за сигурност, които съставляват *„множество от правила и практики, които определят как една организация управлява, защитава и разпределя чувствителна информация.“*¹¹⁸.

¹¹⁷ Павлов, Г. (2010). Цит. съч., с. 14.

¹¹⁸ Пак там, с. 31.

ИЗВОДИ ОТ ПЪРВА ГЛАВА

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“*¹¹⁹.

В литературно-теоретичния обзор на първа глава, свързан със спецификата на информационната сигурност, и по-специално - сигурността във висшите учебни заведения, се постигат няколко, ключови за изследователската част на дисертацията, моменти.

Първият е свързан с идеята за изясняване същността на информацията като понятиен конструкт. Отбелязва се, че информацията е от съществена значимост за провеждането на ефективна и качествена политика за сигурност на информацията в сектора на висшето образование. България полага усилия за развитие на своята информационна сигурност в ерата на дигиталното общество. Информацията като понятие е изведено с авторско определение за целите на дисертацията. Тя е основен източник на стойност в глобалната икономика, 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 умозаклучения, основани на факти, доказателства, истинни хипотези. Информацията е динамична система, която включва отговори на въпроси, за да се постигне потребността от знание.

Вторият се отнася до изясняване същността на понятието за информационна сигурност като защитеност на държавата на стратегическо, оперативно и тактическо ниво. В епохата на Индустрия 4.0 коренно се променят начините за приемане и предаване на информация, като цифровите технологии стават означители на развитието на автоматизацията, интеграцията и обмена на данни в реално време в производствените и организационните процеси. Извеждат се основните характеристики на този тип индустрия,

¹¹⁹ Sidorkin, A., Iroshnikov, D. (2019). Theoretical issues of “security” concept. // Journal of Politics and Law. 3(12), pp. 34–39.

като най-важното е, че се прави революция в трансфера, интензитета, ефективността и качеството на данни.

Третият е свързан с осигуряването на информационна сигурност - киберсигурността се превръща в знаков елемент за защита на масиви от данни. Отношенията, в които се намират информационната сигурност и киберсигурността са на дедуктивен принцип – от общото към частното. Тоест, киберсигурността е елемент от цялостната организация по информационната сигурност в дигиталното пространство. Разглеждат се различни стратегически документи, закони, наредби, програми, които установяват осигуряването на среда за устойчиво развитие на информационните инфраструктури.

Четвъртият се съсредоточава върху висшето образование като обект на информационна сигурност. В рамките на законосъобразността се разглеждат водещи нормативни актове, политики, стандарти, които имат за цел да упражнят регулаторни функции в контекста на цифровизацията на данни и информационен поток. Изграждането на справедлива и конкурентоспособна цифрова икономика, е един от стълбовете на европейската програма за предизвикателствата в съвременния свят. Обръща се поглед към защитата на информацията, като се визират няколко вида сигурност - организационна, технологична, физическа, стандарти и рамки. Предлагат се мерки за предотвратяване неоторизиран достъп до информация, което включва мониторинг на организацията, изготвяне на план за управление на данни, оценка за нарушение на данните. Като стратегии за предотвратяване на различни по тип пробиви се прилагат политики за силни пароли, двуфакторна автентификация и многофакторна автентификация, мониторинг на потребителската активност, внедряване защита на крайната точка, редовни софтуерни актуализации и управление на корекции.

Сигурността на образователната система (има се предвид в частност обекта на изследване – ВУЗ) и информационна сигурност са от жизненоважно значение за националната сигурност¹²⁰. С други думи, човешкият фактор е основният за сигурността. Образователната система играе изключителна роля за развитието на човешките ресурси, личността, формирането на миросгледа, интелекта, национално-нравствените ценности и патриотичен дух.

¹²⁰ Klein, J., Rice, C. (2014). US education reform and national security. Council on Foreign Relations.

Една от стратегическите основи на системата за национална сигурност е свързана с образованието. То е еднакво важно за трите нива на национална сигурност: лична, социална и държавна¹²¹. Следователно сигурността на информацията, свързана с образователната система, е натоварена с много отговорности, свързани със защитаването и съхраняването ѝ¹²².

¹²¹ Oríkpe, E. (2013). Education and national security: Challenges and the way forward. // Journal of Educational and Social Research. 10(3), pp. 53–59.

¹²² Dai, N., András, K., Zoltán, R. (2016). E-learning security risks and counter measures. // Engineering Research and Solutions in ICT. 1(1), pp. 17–25.

ВТОРА ГЛАВА.

АНАЛИЗ НА СЪСТОЯНИЕТО НА ИНФОРМАЦИОННАТА СИГУРНОСТ ВЪВ ВИСШЕТО ОБРАЗОВАНИЕ

2.1. Методологически инструментариум за защита на информацията във висшето образование

2.1.1. Видове сигурност на информацията

През 2018 г., когато GDPR влиза в сила¹²³, 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 разкриване¹²⁴. 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 заплахите¹²⁵.

¹²³ Общ регламент за защита на данните. Достъпно на: <https://gdprinfo.eu/bg>.

¹²⁴ 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.

¹²⁵ Anderson, D., Abiodun, O., Christofides, A. (2020). Information security at South African universities – implications for biomedical research. // Int. Data Priv. Law. 10(2), pp. 180–186.

Въведени са инструменти и техники за сигурност на ИКТ за защита на цифровите активи и инфраструктури¹²⁶. 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 информация¹²⁷. Компютърната инфраструктура и мрежи са въведени в помощ на студентите, преподавателите и служителите в работата на институциите. Поради пандемията от COVID-19, висшите учебни заведения, все повече започват да разчитат на технологиите¹²⁸. Система за проследяване на документи (СДП), електронните библиотеки и СУЗО са популярни сред ВУЗ-овете, за да продължат своите образователни програми, въпреки пандемията¹²⁹. Всички тези технологии предоставят значителни ползи и удобство и най-вече – непрекъснатост на учебния процес.

Тъй като ВУЗ-овете увеличават използването на цифрови ресурси, това ги излага на по-висок риск от заплахи. Например ВУЗ, който предоставя дигитален хостинг за научни статии, е изправен пред заплахи от увреждане на интелектуалната собственост, ако хакер реши да открадне документите¹³⁰. В тази връзка ВУЗ-овете трябва да имат добро възприемане на практиките за сигурност, за да защитят собствената си институция от потенциални заплахи.

Видовете данни, съхранявани в записите на университетите, независимо дали са хартиени или електронни, може да се съчетаят в два конкретни типа¹³¹:

⇒ административни и инфраструктурни;

¹²⁶ Eze, T., Aroh, C. (2020). Management of Information Security in Public Universities in Nigeria. // *Int. J. Digit. Soc.* 11(1), pp. 1575–1578.

¹²⁷ Makupi, D. (2019). A Design of Information Security Maturity Model for Universities Based on ISO 27001. // *Int. J. Bus. Manag.* 7(6).

¹²⁸ Chandarman, R., Van Niekerk, B. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. // *Afr. J. Inf. Commun. AJIC.* 20.

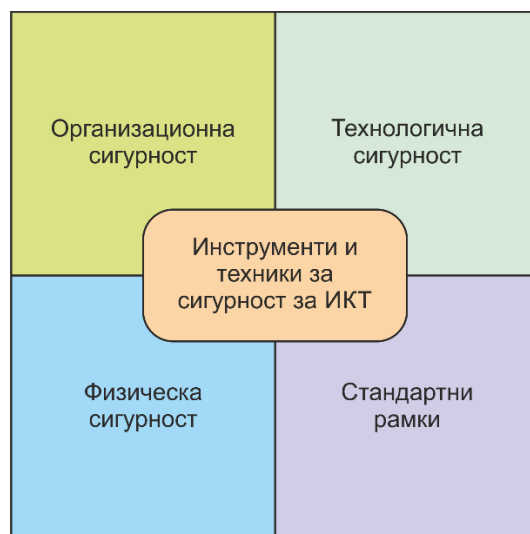
¹²⁹ Cohney, S., Teixeira, R., Kohlbrenner, A. et al. (2020). Virtual Classrooms and Real Harms: Remote Learning at U.S. Universities. Cornell University.

¹³⁰ Bandara, I., Balakrishna, C., Ioras, F. (2021). The Need for Cyber Threat Intelligence for Distance Learning Providers and Online Learning Systems. // 15th International Technology, Education and Development Conference. pp. 9312–9321.

¹³¹ Al-Rawas, A., Millmore, S. (2002). Information Security Risks on a University Campus. // *Sultan Qaboos University Journal for Science.* 7(1), p. 31–43.

⇒ академични и научни изследвания.

На Фигура 11 са категоризирани заплахите според уязвимия субект на организациите.



Фигура 11
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 звено¹³².

¹³² 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.

Технологичната сигурност се занимава със заплахи, които произтичат от уязвимости в приложението, софтуера и мрежовите системи, които организацията 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 институцията¹³³. Тези заплахи могат да идват под формата на наводнение, пожар, земетресения, кражби, грабежи и физически щети¹³⁴.

Физическа сигурност. Използването на следните мерки за предотвратяване на физическо увреждане на киберинфраструктурата на ВУЗ се постига чрез¹³⁵:

- ⇒ 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.

В

Таблица 3 са изведени технологичните канали на комуникация.

Таблица 3	
Технологии и комуникации на сигурността	
Технология	Проблеми със сигурността на данните
Централизирани хост базирани системи	Тясно контролирани данни, обработвани от професионален персонал. Собствен

¹³³ 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.

¹³⁴ 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).

¹³⁵ 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.

	комуникационен канал с ограничен общ потребителски достъп.
Персонални компютърни настолни системи	Ограничен, но локализиран достъп до данни в отделите от страна на местния персонал.
Мрежово базиран сървър	Контролирано сървърно базирано съхранение с данни, пренасяни по комуникационен канал.
Интернет разпределен компютърен модел	Споделено разпространение на данни, предавани по локален комуникационен канал (LAN).
Интернет/Екстранет разпределен компютърен модел	Споделено разпространение на данни, предавани през широкообхватен комуникационен канал (WAN).

Източник: Адаптирано по: Al-Rawas, A. et al. (2002), p. 34

Методите, използвани за организационна сигурност, обикновено включват прилагане на политики, които служителите на организацията, трябва да спазват¹³⁶:

- ⇒ политики за сигурност;
- ⇒ политики за пароли и достъп;
- ⇒ хардуерни политики;
- ⇒ политики за съхранение, споделяне и предаване на данни.

Политиките, които се занимават със сигурността на дадена организация, са се превърнали във важни корпоративни документи, които подпомагат защитата на инфраструктурата за сигурност на организацията¹³⁷. Такива политики насочват персонала на организацията към това какво трябва и какво не трябва да се прави при взаимодействие с цифрови активи и инфраструктура.

Технологичната сигурност, Кашперски дефинира, като защита на крайната точка: настолни компютри, лаптопи, мобилни устройства и други терминали. Това се прави, за да

¹³⁶ Patten, K., Harris, M. (2013). Op.cit.

¹³⁷ Ghazvini, A., Shukur, Z., Hood, Z. (2018). Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education. // Int. J. Adv. Comput. Sci. Appl. 9(8).

се попречи на киберпрестъпниците да ги използват като точки за влизане в системата или мрежата. Сигурността на крайната точка се състои от различни технологии, които работят заедно: защитни стени, антизловреден софтуер, криптиране на данни, защита от вътрешни заплахи и защита при сърфиране в мрежата¹³⁸. Технологичната сигурност включва и мрежовата инфраструктура на институциите¹³⁹. Защитата на мрежата е от жизненоважно значение за стратегията за киберсигурност на всяка организация.

При разглеждане проблемите на информационната сигурност се поставят конкретни цели, а именно да се гарантира¹⁴⁰:

- ⇒ наличност – ИС структурите са там през 100% от времето;
- ⇒ точност – данните са вярно, пълно и коректно възпроизведени;
- ⇒ защитеност – данните не се губят, повреждат или нарушават;
- ⇒ поверителност – информацията се разкрива само на тези, които трябва да имат достъп.

Сигурността на информацията и информационните инфраструктури може да се разглежда като съставена от няколко различни части¹⁴¹:

- 1) Компоненти на физическата инфраструктура, които са свързани с това къде и как е инсталирано оборудването.
- 2) Хора, които имат достъп и използват информацията.
- 3) Системи, които се използват за съхраняване и запазване на достъпната информация.
- 4) Комуникационни технологии, използвани за получаване на достъп до и транспортиране на тази информация.

¹³⁸ Joshi, C., Singh, U. (2017). Information Security Risks Management Framework – A Step Towards Mitigating Security Risks in University Network. // J. Inf. Secur. Appl. 35, pp. 128–137.

¹³⁹ Xu, Y. (2013). Research on Computer Network Security Architecture of Universities in China. // Adv. Mater. Res. 765–767, pp. 1486–1489.

¹⁴⁰ Al-Rawas, A. et al. (2002). Op. cit., p. 34.

¹⁴¹ Ibidem.

2.1.2. Мерки при риск от нарушаване на достъпа на информация

Университетите са в процес на технологично развитие. През изминалите години стана ясно, че достъпа до технологията е ценен за разработването на съвременни образователни среди, но от друга страна, увеличаването на уязвимостта на комуникационните мрежи и броя на заплахите, са сериозно предизвикателство¹⁴².

В Закона за защита на личните данни, действащият надзорен орган е КЗП¹⁴³. Законът обхваща отношенията, свързани с правата на физическите лица, уредени с Регламент 2016/679 на Европейския парламент и на Съвета¹⁴⁴.

Нарушаването на сигурността на данните във връзка с личните данни, се отнася до всеки неоторизиран достъп, събиране, използване, разкриване, копиране, промяна или разпореждане с лични данни. Също така, включва загуба на всякакъв носител за съхранение или устройство, на което се съхраняват лични данни при обстоятелства, при които има вероятност да възникне неоторизиран достъп. Пробивът на данни може да бъде резултат от злонамерени дейности, човешка грешка или слабости на компютърната система¹⁴⁵.

Мерките, които трябва да се предприемат при нарушено управление на достъпа до информация или при съмнения в изтичане на данни, 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.

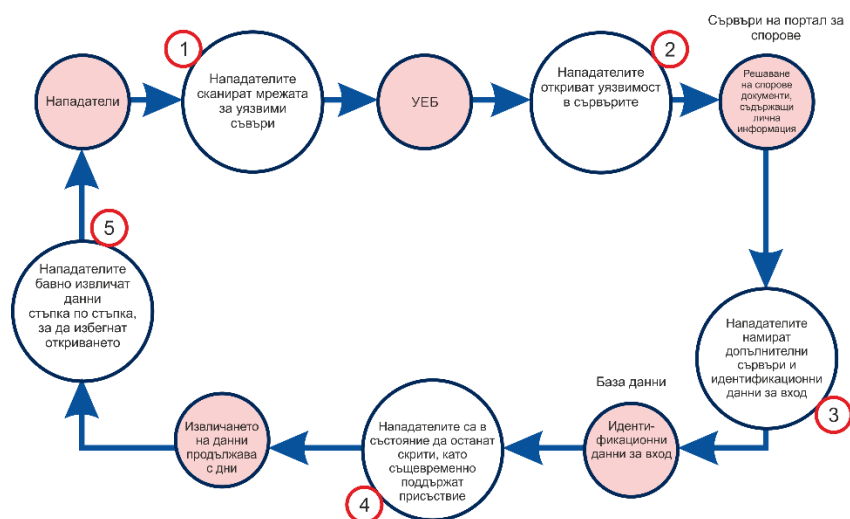
¹⁴² Jang-Jaccard J., Nepal, S. (2014). A survey of emerging threats in cybersecurity. In: Journal of Computer and System. // Sciences, Aug. 80(5), pp. 973–993.

¹⁴³ Закон за защита на личните данни. Достъпно на: <https://cpdp.bg>

¹⁴⁴ Регламент 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година. Достъпно на: <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016R0679>.

¹⁴⁵ Guide on Managing and Notifying Data Breaches under the PDPA. (2021). Available on: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-on-Managing-and-Notifying-Data-Breaches-under-the-PDPA-15-Mar-2021.pdf>, p. 8.

- 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 12
Модел на хакерска атака при пробив и кражба на лични данни
 Източник: Адаптирано по: GAO, Equifax¹⁴⁶

Предотвратяването на неоторизиран достъп, изисква цялостен подход, който съчетава няколко стратегии¹⁴⁷:

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

¹⁴⁶ 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>.

¹⁴⁷ Sammons, J., Cross, M. (2015). The Basics of Cyber Safety. Elsevier Inc. pp. 75–86; 117–137.

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

2. Двухфакторна 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.

2.2. Подходи и методи на изследване – сравнителен анализ

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

Спрямо анкетното проучване се използва количествен метод за събиране на данни - анкетата. Извеждат се основни блокове въпроси и тяхната интерпретация.

Концептуалният модел за ограничаване на уязвимостите и заплахите на информационната сигурност в университетите се разработва на базата на систематичния подход за идентифициране на информацията и сравнителен анализ. Показва се Референтен модел за киберсигурност, апробиран от докторант на УНСС, който задава рамката за разкриване основните параметри на авторски изградения модел. Моделът се основава на кумулативни данни и информация, както и да бъдат изведени критерии, показатели и компоненти.

Сравнителният анализ на състоянието на ИС в българските университети е изграден въз основа на чуждестранни и български научни трудове, благодарение на които се създава ландшафт на подобрението на визията, архитектурата и сигурността.

Методите за сравнение могат да бъдат качествени и количествени. Качественото сравнение се извършва с помощта на номиналната и ординалната скала на измерванията. В този случай сравнението се основава на намирането на двоична връзка между сравняваните обекти или техните свойства. Сравнението води до качествена характеристика. Простото сравнение се основава на сравнение по двойки на два обекта¹⁴⁸. Той използва една двоична релация и описва предикати от втори ред. Комплексното сравнение допълнително използва сравнение на обект и група от обекти. Той използва два типа релации: релация между два обекта и релации в група от обекти.

Много видове сравнения не вземат предвид концепцията за съпоставими отношения и не изследват тези отношения. В същото време такова изследване дава възможност за

¹⁴⁸ Cavallo, B. et al (2019). Comparing inconsistency of pairwise comparison matrices depending on entries. // Journal of the Operational Research Society. 70(5), pp. 842–850.

автоматизиране и алгоритмизиране на формулирането на проблем за сравнение и неговото решение. Във всички видове сравнения има оценъчни отношения, независимо дали включват някакви измервания или само качествена оценка. Оценъчните отношения са типични за всяко сравнение. При количествено сравнение отношенията на оценка могат да бъдат трансформирани в отношения на измерване или допълнени от тези отношения. В неявна форма тринитарното сравнение присъства в системите и методите на аргументация¹⁴⁹, както и в системите за оценка на съответствие/несъответствие¹⁵⁰. Аргументацията може да се разглежда и като метод за качествено сравнение. Понастоящем обаче методите на аргументация и сравнение се считат за различни области на изследване.

Триадата е структурната основа за сравнение и може да се разглежда като най-простата комплексна система. Тринитарните отношения определят целостта на тринитарния модел. Изключването на едно от отношенията или един от обектите от тринитарния модел, нарушава целостта и качеството на сравнението. При сравняване се използват два вида модели: фиксиращи фактите и интерпретативни. Моделите за фиксиране на факти улавят фактите, които служат като база за сравнение. Това е известна конвенция, тъй като всичко в света се променя и сравнението се прави на базата на факти за определен период от време. Фактите могат да остарееят и като така отношението на съпоставимост изисква използването на факти, които са сравними в определен период от време.

Интерпретативните модели също са условни, тъй като методите за интерпретация се променят и се свързват с развитие на науката и технологиите.

Сравнителният анализ позволява да се свържат новите знания с възгледа за света¹⁵¹. Сравнението може да се разглежда като интелигентна процедура, която позволява да се изследва набор от обекти, за да се открият връзките им или да се оцени степента на техните различия и прилики. На епистемологичен език това се определя като интелигентна операция, чрез която състоянията на един (или повече) обект, се проверяват въз основа на

¹⁴⁹ Gordon, T., Prakken, H., Walton, D. (2007). The Carneades model of argument and burden of proof. // *Artificial Intelligence*. 171(10-15), pp. 875–896.

¹⁵⁰ De Bona, G. et al. (2019). Classifying Inconsistency Measures Using Graphs. // *Journal of Artificial Intelligence Research*. 66, pp. 937–987.

¹⁵¹ Tsvetkov, V. (2014). Worldview Model as the Result of Education. // *World Applied Sciences Journal*. 31(2), pp. 211–215.

поне едно общо свойство. Следователно, актът на сравнение предполага обекти (които очевидно могат да бъдат субекти, групи, градове, държави и т.н.), свойства на обекти, състояние на обектите в конкретния момент.

Внася се уточнението, че се предоставя обстоятелствено обяснение какво се прави и се цели да се постигне в хода на изследването благодарение на сравнителния анализ, анкетния метод и прилагането на концептуален модел за ограничаване на заплахите и уязвимостите на информационната сигурност.

Логиката, която се следва при разработването на Модела, се подчинява на научни факти, регистрирани като доказателства в главата, посветена на методологията, от една страна, а от друга - на изложените допълнителни научни сведения в трета глава. Моделът е замислен, за да помогне на ръководителите на сектора за ИС към университетите да вземат адекватни решения и мерки за сигурност с цел да се намали вероятността от компрометиране на чувствителна информация. В началото е изведен Референтният модел за киберсигурност на Е. Павлова, в който се посочват основните обекти, функции, заложи в политиките и стратегиите за управление на ИТ. Този модел е знаков за реализирането на авторския модел, тъй като са положени основни взаимовръзки и процедури, свързани с организационната структура.

В представянето на Модела на първо място се поставят критерии, показатели и компоненти, които внедряват същността на изложената концепция: риск мениджмънт, имплементиране, киберпространство и архитектура, процес на реагиране и киберсигурност. Те са съществени звена, за да се изгради качествено нова структура - функционална и прагматична. В нея се залагат целевите, организационните, образователните, информативните, човешките компоненти. Анализът и мониторингът на системата за ИС са от фундаментално значение за разкриване слабостите и уязвимостите. Важно място заема киберсигурността като компонент на ИС, като към този критерий се причислява събирането на данни, разпознаването на лошите и добрите метрики, ресурсите и капацитета.

Във фрагментарен вид се извеждат компонентните ядра на Модела. Първият засяга рисковия мениджмънт, при който от съществено значение е да се определят целите на управление, да се идентифицират физическите и информационните активи, да се определи

оценката на заплахите и уязвимостите, да се предостави оценка на категориите и нивата на риск, да се превантират и/или премахнат атаките. На следващ етап са целевите категории към критерия за имплементиране, като в него се залагат: план за действие (абсолютно необходим за правилното прогнозиране), остатъчният риск, прави се контролна оценка, оценка на риска (включва се тук), оценка на уязвимостта, мерките за противодействие, както се правят и оценки на активите и заплахите. Казва се, че Моделът ще послужи за комплексното управление на кризи в случай на атака, като се засягат вертикалните оси: хора и идентичност, данни и информация, сигурност на приложението, инфраструктура. Тези компоненти попадат в критерия за киберпространството на Модела. Критерият за киберпространство се основава на научните изследвания на Тагарев, като се залагат основните метрики: оценка на вътрешната среда, измерими бизнес стойности, обективно представяне на проблемите, обосновка за нови инвестиции, подобрения. Към този критерий се залагат и добрите/лошите метрики, изложени в трудовете на Тагарев. Показват се и целевите категории за метриките, като се отчитат: времето между откриването на инцидента и ограничаването му, броя на информационните активи, брой дни за преодоляване на 50% от заплахите, брой кръпки на сървъра и процент от трети страни, чиито привилегии са прегледани през отчетен период.

Извежда се опростен модел на архитектурата на ИС, в който нагледно се представя механизма за сигурност, службата, отговаряща за сигурността и атаките срещу сигурността. Представя се архитектурата на модела, която обхваща материални носители, връзка за данните, мрежов достъп, транспортиране, приложение, представяне. Маршрутизирането е свързано със сегментирането и транспортирането на данните, с мрежата и логическата инфраструктура. Мрежовата сигурност се дефинира като защита на мрежовата инфраструктура на организацията с помощта на защитни стени, системи за откриване и предотвратяване на проникване (IDPS) и виртуални частни мрежи (VPN) за контрол и наблюдение на мрежовия трафик. Защитата на крайните точки се извежда като защита на отделни устройства - компютри и смартфони. Сигурността на данните и приложенията е насочена към защита на софтуера посредством криптиране на масиви информация. Важно условие е да има съответствие с нормативната уредба, както и разузнаване на заплахи чрез актуализиране и бърза реакция при създаден проблем.

Показва се структурата на сигурността на модела, като в нея присъстват компонентите: разузнаване на заплахи; автоматично управление на правилата; унифицирано управление на заплахите; засичане на проникване. Извеждат се също на отделен визуален елемент функционалностите на CFW, като е доказано, че тази технология 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. Изброяват се съответните защиты, които трябва да бъдат вградени: фърмуер, вътрешната защитна стена за сегментиране, Virtual Firewall, защитна стена на центъра за данни.

За по-голяма пълнота и представителност на изведената информация се представят видовете заплахи, които има предвид Модела, като тези заплахи са идентифицирани спрямо научните изследвания на Пудин и Павлов. Поделят се на вътрешни и външни от гледна точка на източника на заплахата; по произход са естествени и социални, като тук неизменно се включва човешкият фактор, отчетен както в проведеното анкетно проучване, така и в чуждестранни източници. По характер са икономически, политически, финансови и демографски, по времетраене - временни, периодични и перманентни, а като намерение се поделят на случайни и умишлени.

Разгръща се визуална интерпретация на имплементиране концепцията на Модела, като в хода на този процес се набелязват основните параметри, които се вграждат и съблюдават: източник на информация, приоритет на информация, източник на заплахата, цел на заплахата, заплахи, методи за достъп, насоки за защита, защитни средства, методи на защита. Разкриват се и процесите на реагиране при инциденти, като се детерминират по следните параметри: подготовка, идентификация, ограничаване, изкореняване, възстановяване и поуки.

Извежда се цялостна технология за подобряване на системите за ИС, основана на работната рамка на COBIT. Систематизират се и нивата на развитие на самата технология, като се прави и авторска диаграма на оптималното управление на процесите. Важност представляват и необходимите инвестиции за подобряване на ИС, както и се определят очакваните ползи от внедряването на модела.

Съществените ползи за разработването на Модела са изведени и онагледени в трета глава.

2.3. Специфика на анкетното проучване. Основни блокове въпроси

Анкетното проучване е ефективен количествен метод за събиране на данни, който е подходящ за изследване на различни проблеми и е особено практичен при работа с големи извадки. Основните стъпки, свързани с провеждането на анкетно проучване са:

1. Формулиране на методика за провеждане на проучването;
2. Разработване на анкетни карти;
3. Създаване на организация по разпространяване и попълване на анкетите;
4. Събиране, обработка и анализ на получените резултати¹⁵².

Предимствата на анкетата са свързани със следните силни страни:

- ⇒ позволява анкетирането на голям брой лица и по този начин набавянето на повече статистически данни;
- ⇒ възможно е достигането до повече и различни географски региони, което обогатява получените резултати;
- ⇒ анкетите могат да се провеждат анонимно и по този начин да предразположат респондентите да се включат в попълването им, давайки безпристрастни и откровени отговори;
- ⇒ получаването на данните и тяхното кодиране, се осъществява сравнително лесно като процес.

Наред с предимства, анкетният метод има и определени **недостатъци**, като например:

- ⇒ обикновено отнема значително време за изготвяне и провеждане;
- ⇒ набавянето на необходимата информация, е сложен и трудоемък процес;

¹⁵² Комисия „Публична комуникация“. (2014). Анкета за проучване на общественото мнение за дейността на ВСС и съдебната власт сред ключовите общности според комуникационната политика на ВВС. Анализ на резултатите, Достъпно на: <http://www.vss.justice.bg/root/f/upload/8/analiz-anketa-vss-2014.pdf>.

- ⇒ нужно е ангажираните анкетъори да бъдат обучени;
- ⇒ ако е необходим по-голям брой анкетъори, това би оскъпило провеждането на анкетното проучване;
- ⇒ възможно е в резултат на неправилен анализ или предубеден такъв да се получи изопачаване на резултатите.

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.

Събраната с помощта на анкетното проучване информация, в т.ч. и необходимите за анализа демографски данни, следва да бъдат използвани само за целите на дисертационния труд и да бъдат надеждно съхранявани и опазвани. Освен това, за постигане на максимално безпристрастие в анализирането на резултатите, анкетите са проведени анонимно. По този начин се очаква да се даде и по-голяма свобода и увереност на самите анкетирувани лица.

Моделът, който се представя в настоящата дисертация, емпирично изследва качеството на информационната сигурност във висшето образование, като посреднически фактор между отношенията институция – потребител, с цел изграждане на доверие и лоялност.

Доверието, удовлетвореността и качеството на комуникацията се влияят положително от измеренията за качество на услугата. Потребителите формират възприятията си въз основа на гореспоменатите фактори. Резултатът (технически) и взаимодействието (функционален) са адаптирани от изследванията на Gronroos¹⁵³, при които качеството на услугата се оценява според оценките на клиентите на резултатите и взаимодействията със служителите в обслужването.

¹⁵³ Gronroos, C. (1984). A service quality model and its marketing implications. // European Journal of Marketing. 18(4), pp. 36–44.

Обектът на изследователски интерес са работещите в сферата на висшето образование в България.

Предметът на изследователски интерес е сигурността на информацията във висшето образование.

Както обекта, така и предмета са продиктувани от **актуалността** на проблема в XXI век – дигитализирането на обществото и рисковете, пред които е поставена информацията.

Целта на проучването е свързана с това да се установи състоянието на информационната сигурност във висшите учебни заведения чрез мнението, нагласите, възприятията на работещите в сферата.

Задачите, които си поставя проучването, са изцяло от емпирико-приложен характер:

- 1) Да се изготви анкетна карта, свързана с темата, обекта и предмета на изследователския интерес.
- 2) Да се разпространи посредством формата Google forms, за да може по-лесно и по-бързо да бъде разпратена към респондентите чрез онлайн канали.
- 3) Да се събере нужната извадка, характерна за непредставително проучване.
- 4) Да се обработят статистически резултатите.
- 5) Да се анализират резултатите от проучването.
- 6) Да се направят изводи въз основа на изнесените данни в проучването.

Методите са анкета, анализ и синтез, статистически метод.

Основният инструмент за изследване, използван при събирането на необходимите данни за това проучване, е **въпросникът**. В обзор на 30 различни проучвания за качество на услугите, Ladhari¹⁵⁴ установява, че количественият метод (въпросник за проучване) е основният подход за събиране на данни, за да се тества предложеният модел на изследване на три променливи (качество на услугата, удовлетвореност и лоялност, доверие на потребителите).

¹⁵⁴ Ladhari, R. (2008). Alternative measures of service quality: a review. // Measuring Service Quality. 18(1), pp. 65–86.

Анкетното проучване обхваща 56 респонденти, като условието, което е спазено, е те да работят в български университети. Споделена е анонимността на анкетиранияте участници, както и им е известно, че резултатите от изследването ще се използват единствено за целите на дисертационния труд.

Анкетата е разпратена посредством онлайн социални канали и обхваща периода април 2024 г. – септември 2024 г.

Анкетата се състои от 16 въпроса – 15 са с избираем отговор, 1 – с отворен.

Въпросите са групирани на три основни принципа – демографски характеристики, професионални характеристики и лично мнение.

По-долу в схематичен вид е представена информацията на изследователския инструмент, която може да бъде разделена на три основни блок въпроси. Те са затворени по своята специфика и всеки от тях е разработен с цел да се проследи нивото на удовлетвореност/неудовлетвореност спрямо качеството на ИС във висшето образование.



Фигура 13
Основни блокове въпроси
Източник: авторска интерпретация

Блок I: Въпроси, свързани с персонална анонимна информация на анкетирания

Блок I въпросите покриват от 1 до 4 въпрос включително и целят да се снемат социална и демографска характеристика на анкетираните. Тези въпроси спомагат да се получи информация за пола и възрастта, трудовия стаж в сферата на висшето образование, професионалния статут. По този начин се придобива косвена информация за профила на респондента. Такъв тип въпроси спомагат за определяне опита на служителя – ценен източник на достоверна информация.

Блок II: Въпроси, свързани с качеството на системата за информационна сигурност

Блок II въпросите се отнасят до степента на удовлетвореност/неудовлетвореност на служителите от предлаганото качество на системата за информационна сигурност. Мненията, чувствата, впечатленията, които споделят респондентите, спомагат за изграждането на атмосфера на сигурност/несигурност на работното място, което тясно кореспондира с нивото им на удовлетвореност. Колкото по-спокоен и сигурен се чувства служителът, толкова по-качествени ще са неговите работни ангажименти и психическа дееспособност.

Блок III: Въпроси, свързани с компетентностите на служителите

Блок III въпросите се отнасят до постигането на едно високо ниво на опит и знания, които изграждат общата компетентност на служителите. Повишаването на квалификацията, знанието как да се реагира при кризисни ситуации, застрашаващи информационната сигурност на работното място, чувството за развита интуиция, са показателите за адекватност на работното място и за подготвеност при евентуални проблеми на сигурността.

Методът за събиране на данни за целите на емпиричното изследване, е методът на интернет анкетата с едностраничен въпросник. Изборът на метод за целите на проучването се основава на типологията на методите за събиране на данни. Може да се представи в четири основни стъпки, които разгръщат идейната основа на настоящия изследователски експеримент:

⇒ избор на вида данни, които ще бъдат събрани;

- ⇒ избор на конкретен метод за събиране на първични данни;
- ⇒ избор на конкретен количествен метод за събиране на данните;
- ⇒ избор на разновидност на анкетите.

Вторичните данни се дефинират като такива данни, *„които са събрани и обработени по друг повод, съхранени са на подходящ носител и са достъпни за използване“*¹⁵⁵, като Желев е на мнение, че логиката на един изследователски подход следва да бъде, че *„едва след като изследователят бъде строго убеден, че не съществуват нужните вторични данни, които да вършат работа, той следва да се обърне като правило към по-сложните, по-скъпите, по-трудоемките и по-тромавите процедури за събиране на първични данни“*¹⁵⁶. За целите на изследователския проблем относно установяването на състоянието на информационна сигурност във висшето образование се използват вътрешни и външни вторични данни:

- ⇒ вътрешни вторични данни – една част са готови за използване, а друга се нуждае от по-нататъшна обработка;
- ⇒ външни вторични данни – произвеждат се и са налични при източници, извън дадена организация, като към тях се причисляват количествените данни от Националния статистически институт, например.

¹⁵⁵ Желев, С. (2008). Маркетингови изследвания: Методология и организация. София: УИ „Стопанство“, с. 65.

¹⁵⁶ Пак там.



Фигура 14
Видове вторични данни
Източник: Адаптирано по Желев, С.¹⁵⁷

Предимствата и недостатъците при използването на вторични данни са ^{*}:

- ✓ по-евтини от първичните данни;
- ✓ осигуряването на данни е по-бързо;
- ✓ набавянето им е свързано с по-малко усилия и по-малко заетост;
- ✓ по-малко рискове крие в сравнение с първичното набиране на данни;
- ✓ трудности в откриването на подходящите за целите на изследването данни;
- ✓ липса на показатели за точността на данните.

Основните причини за пристъпване към събирането на първични данни са следните:

¹⁵⁷ Пак там.

^{*} Вж. Желев, С. Пак там, с. 71–72.

1. До този момент в България не е правено подобно проучване, което да установи състоянието на информационната сигурност във висшите учебни заведения чрез проучване на мнението, нагласите, възприятията на работещите в сферата.
2. Характерът на необходимите за настоящото проучване данни е такъв, че изисква провеждане на специално проучване. Става дума за това, че необходимите емпирични данни не съществуват събрани в готов вид и никоя управленска информационна система в дадена институция не може да предостави и/или генерира подобен вид информация.
3. Отсъствието на вторични данни, които да спомогнат за провеждането на проучването.

Следва да се направи извода, че е налице основанието да се подходи към събиране на първични данни чрез специално емпирично проучване.

За избор на метод за събиране на данни трябва да се има предвид, че се срещат две най-чести грешки: когато чрез прилагането на качествени методи се правят опити да се решават проблеми, характерни за количествените изследвания, и обратно – когато чрез количествени методи се правят опити за решение на качествени изследвания. Особеност на качествените методи е, че те отговарят на въпросите „какво“, „как“ и „защо“, но не и на „колко“. В таблицата по-долу са представени основните различия на двата вида методи, синтезирани и обобщени от Желев.

Таблица 4

Основни характеристики на качествените и количествените методи за събиране на данни

Характеристика	Качествени методи	Количествени методи
Типология на проблема	неструктуриран или слабо структуриран	структуриран
Цел	да разбере потребителските очаквания и възприятия	да измери потребителските намерения, предпочитания
Събиране на данни	Неструктурирано	Структурирано
Основни техники	открити въпроси, проективни техники, стимулни материали	закрити и полузакрити въпроси
Извадка	непредставителна, малка	представителна, голяма

Тип на анализа	Логически	статистически
Свобода на изследователя	голяма, изисква се творчество	малка, изисква се точно познаване на стандартните методи и техники
Интерпретация	екстензивна – извършва се по време на целия изследователски процес	фокусирана – на отделни фази от изследването
Резултат	начално разбиране	препоръка за управленски решения

Източник: адаптирано по Желев¹⁵⁸

Предимствата при използването на количествените методи се обобщават по следния начин:

- 1) Информацията е структурирана и фокусирана на отделни фази от изследването, като се прилагат стандартизирани методи и техники за извеждане на резултатите и даване на препоръки за ефективни управленски решения.
- 2) Въпросите са закрити и/или открити, което не изисква ерудираността на изследователя, необходима му при полева работа за събиране на данни при качествени изследвания.
- 3) Информацията се обработва статистически, което изключва субективния фактор при анализирането на променливите.

Дескриптивните методи за събиране на данни се делят на два големи класа – методи на допитването и методи на наблюдението. За настоящето изследване се използват методите на допитването, като за тази цел се изготвя предварително разработен въпросник, който да отговаря на нуждите на изследователския експеримент. Въпросите са структурирани (стандартизирани), писмени*.

¹⁵⁸ Пак там, с. 76 – 77.

* Повече по темата вж. Желев, С. (2012). Маркетингови изследвания. // Маркетинг. София: ИК УНСС, с. 113–140.

Изборът на изследователска практика е електронният въпросник, като методите, които се основават на използването на компютър, се наричат САРІ*. Анкетата се характеризира със „самостоятелно разчитане, разбиране и попълване на въпросника от страна на респондента“¹⁵⁹.

Групират се в четири различни категории¹⁶⁰:

- ✓ персонална анкета – анкетаторът посещава респондента в собствения му дом, като след решаването на въпросника, е задължен да провери дали е коректно попълнен.
- ✓ пощенска анкета – анкетите пристигат по пощата, като през последните години този тип допитване е изчезнал.
- ✓ анкета в търговските обекти – въпросниците се раздават от специално наети лица в различни обекти, като спецификата на самата анкета е, че въпросите в нея са много кратки.
- ✓ интернет анкета – представител на анкетния метод, който все по-често се застъпва в практиката. Въпросникът се изпраща по email и респондентът бива помолен да се включи в допитването.

В настоящото изследване, събирането на данните, е извършено чрез интернет анкета в разновидността ѝ на онлайн анкета в едностраничен въпросник. Причините за този избор са следните:

- бързина и ефективност на извадковия материал;
- събиране на данни от организации;
- високо ниво на поверителност;
- интернет е предпочитано място за комуникация на съвременния човек;

* Пак там, с. 126.

¹⁵⁹ Пак там, с. 126.

¹⁶⁰ Пак там, с. 126–127.

- ниското ниво на разходи.

Извадковият модел на изследването се състои в:

- 1) **Първични единици.** Първичните единици на настоящото изследване са работещите в сферата на висшето образование, които към момента на проучването са активни. Генералната съвкупност е от 56 респонденти.
- 2) **Наблюдавани единици.** Наблюдавани единици са представителите на средно управленско ниво в първичните единици, състоящи се от персонал, изпълняващ административни и/или преподавателски дейности.
- 3) **Тип извадка.** Използвана е целева неслучайна типологична извадка. Причината е в обстоятелството, че *„подборният процес съответства на целите на изследването“*¹⁶¹ и определена категория единици отговарят на даден критерий – изследваните фирми извършват дигитален маркетинг за нуждите на техния бизнес.
- 4) **Обем на извадката.** Обемът на извадката е 56 респонденти.

В тази точка от дисертацията се направи обзор на избора на метод за събиране на информацията, като се установи, че ще се използва онлайн анкета с едностраничен въпросник. За избор на метод за събиране на данни се прилага количественият за по-прецизно статистическо изпълнение.

¹⁶¹ Пак там, с. 135.

ИЗВОДИ ОТ ВТОРА ГЛАВА

Втора глава изгражда методологическата рамка и нейния инструментариум на проведените проучвания. Съсредоточава се върху видовете сигурност на информацията, като се прави сравнителен анализ. GDPR влиза в сила през 2018 г., което дава възможност за по-добра ефективност и осигуряване на по-големи възможности в дигиталният свят, но и по-голяма защитеност на масивите от база данни. Въвеждат се инструменти и техники за сигурност, които спомагат да се защитят по-благонадеждно цифровите активи и инфраструктури. Използването на цифрови ресурси в сектора на висшето образование създава неблагоприятни възможности за риск от киберзаплахи и в тази връзка се предприемат стъпки за защита на собствените ресурси.

Онагледява се и се обяснява категоризацията на ИКТ инструменти за сигурност: организационна, технологична, физическа сигурност и стандартни рамки, в които влизат всички нормативни и законови уредби, действащи на територията на държавата.

Представят се и технологичните канали на комуникация, които включват централизирани хост-базирани системи, персонални компютри и настолни системи, мрежов-базиран сървър, интернет-разпределен компютърен модел и интранет/екстранет-разпределен компютърен модел, като се уточняват и възникващите проблеми със сигурността на данните.

Методите на организационна сигурност включват прилагане на различни видове политики - за сигурност, пароли за достъп, хардуерни политики и политики за съхранение, споделяне и предаване на данни. Мерките, които се предприемат при нарушено управление на достъпа на информация, са: мониторинг на организацията, план за управление на набор от данни, извършване на оценка за нарушение на данните.

Онагледява се и се интерпретира модел на хакерска атака при пробив и кражба на лични данни, като предотвратяването на неоторизиран достъп изисква прилагането на цялостен подход, който съчетава стратегиите: политика за силни пароли, двуфакторна автентификация и многофакторна автентификация, мониторинг на потребителската активност, внедряване защита на крайната точка, редовни софтуерни актуализации и управление на корекции.

В разглежданата точка за подходите и методите на изследване се акцентира, че спрямо анкетното проучване се използва количествен метод за събиране на данни - анкетата. Извеждат се основни блокове въпроси и тяхната интерпретация. Спрямо концептуалният модел за ограничаване на уязвимостите и заплахите на информационната сигурност в университетите се разработва на базата на систематичния подход за идентифициране на информацията и сравнителен анализ. Сравнителният анализ на състоянието на ИС в българските университети е изграден въз основа на чуждестранни и български научни трудове, благодарение на които се създава ландшафт на подобреното на визията, архитектурата и сигурността. Прави се аналитичен прочит за видовете методи за сравнение, като такова изследване дава възможност за автоматизиране и алгоритмизиране на формулирането на проблем за сравнение и неговото решение. Аргументацията и интерпретацията на данните може да се разглеждат като метод за качествено сравнение. При сравняване се използват два вида модели: фиксиращи фактите и интерпретативни. Моделите за фиксиране на факти улавят фактите, които служат като база за сравнение. Интерпретативните модели също са условни, тъй като методите за интерпретация се променят и се свързват с развитие на науката и технологиите.

Внася се уточнението, че се прави обстоятелствено обяснение какво се прави и се цели да се постигне в хода на изследването благодарение на сравнителния анализ, анкетния метод и прилагането на концептуален модел за ограничаване на заплахите и уязвимостите на информационната сигурност. Логиката, която се следва при разработването на Модела, се подчинява на научни факти, регистрирани като доказателства в главата, посветена на методологията, от една страна, а от друга - на изложените допълнителни научни сведения в трета глава. Моделът е замислен, за да помогне на ръководителите на сектора за ИС към университетите да вземат адекватни решения и мерки за сигурност с цел да се намали вероятността от компрометиране на чувствителна информация. Анализът и мониторингът на системата за ИС са от фундаментално значение за разкриване слабостите и уязвимостите. Важно място заема киберсигурността като компонент на ИС, като към този критерий се причислява събирането на данни, разпознаването на лошите и добрите метрики, ресурсите и капацитета. Във фрагментарен вид се извеждат компонентните ядра на Модела. Първият засяга рисковия мениджмънт, при който от съществено значение е да се определят целите на управление, да се идентифицират физическите и информационните

активи, да се определи оценката на заплахите и уязвимостите, да се предостави оценка на категориите и нивата на риск, да се превантират и/или премахнат атаките. Извежда се опростен модел на архитектурата на ИС, в който нагледно се представя механизма за сигурност, службата, отговаряща за сигурността и атаките срещу сигурността. Представя се архитектурата на модела, която обхваща материални носители, връзка за данните, мрежов достъп, транспортиране, приложение, представяне.

При спецификата на анкетното проучване се отчита, че анкетата е ефективен количествен метод за събиране на данни, който е подходящ за изследване на различни проблеми и е особено практичен при работа с големи извадки. Представят се предимствата и недостатъците, като се споменава, че 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 възможните за внедряване на нова, по-добра система за управление на сигурността. Извеждат се предметът, обектът, целта и задачите. Представят се основните блокове въпроси, фигуриращи в анкетната карта: въпроси, свързани с персонална анонимна информация на анкетирувания; въпроси, свързани с качеството на системата за информационна сигурност; въпроси, свързани с компетентностите на служителите.

ТРЕТА ГЛАВА.

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

3.1. Анализ на резултатите от проведеното анкетно изследване

Внася се 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.

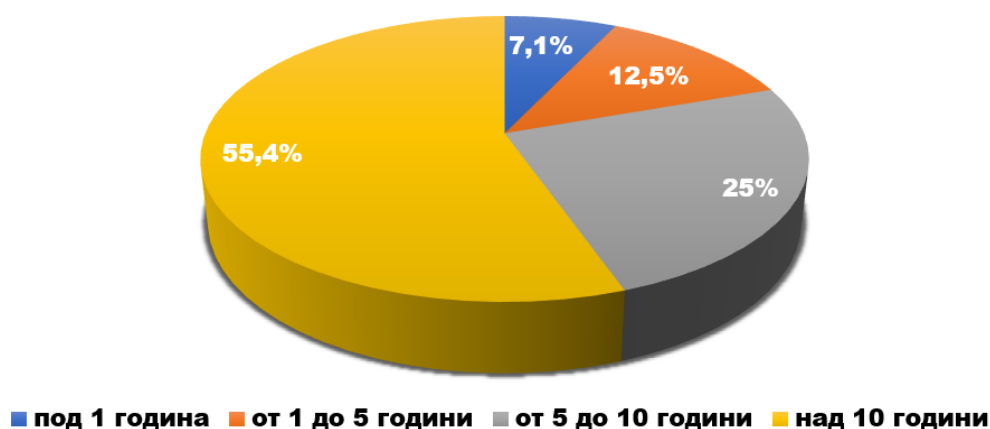
На въпрос № 1 *Вие сте*: анкетираните са посочили, че 44.6% са жени, а 55.4% - мъже. Това обстоятелство спомага пропорционално да са разпределени респондентите по полов признак, което спомага за равноправното споделяне на мнения и отношения спрямо зададените въпроси.



Фигура 15
Въпрос: Вие сте:

На въпрос № 2 *От колко години работите в сферата на висшето образование?* Най-висок процентен дял е получил отговорът „над 10 години“ (55.4%), което показва придобитият професионален опит на анкетираните, от една страна, а от друга – способността да отличават спецификите на работния процес и в частност – сигурността на информацията. Дългият професионален опит е вид вживяване в работния процес и осезателно вглеждане в процесуалността и организираността му. Втората група с най-висок процентен дял от 25%, или една четвърт, са работещите с трудов стаж от 5 до 10 години. На следващо място с 12.5% са служителите с 1 до 5 години, а на последно място – тези с най-нисък трудов стаж в сферата на висшето образование – под 1 година (7.1%). Може да се направи извода, че по-големия процентен дял на регистрираните участници в анкетното проучване са служители с трудов стаж от 5 до 10 години и над 10 години, което прави 80.4% сумарно. Опитът е водещ показател за изразяване на професионално отношение спрямо процесите на организация и контрол в институцията.

От колко години работите в сферата на висшето образование?



Фигура 16
Въпрос: От колко години работите в сферата на висшето образование?

На въпрос № 3 *Какъв е Вашият професионален статут?* 35,7% от запитаните са отговорили, че са преподаватели на шат, следвани с еднакъв пропорционален процент от 23.2% за служител, занимаващи се с административни дейности и хонорувани преподаватели. Този въпрос оформя картината на професионалната обвързаност на респондентите с висшето учебно заведение, като облика ѝ е оформен от преподавателски екип. Може да се направи извода, че преподавателите са в основата на сигнализирането в проявата на нередности в информационната сигурност, тъй като те работят едновременно с информационни ресурси, със студенти и с база данни, възможностите на които представляват потенциални заплахи за сигурността на институцията. Включеният в проучването административен персонал (23.2%), също е основателно компетентно звено при сигнализирането и/или разрешаването на проблемни ситуации, свързани с информационната сигурност.

Какъв е Вашият професионален статут?



Фигура 17
Въпрос: Какъв е Вашият професионален статут?

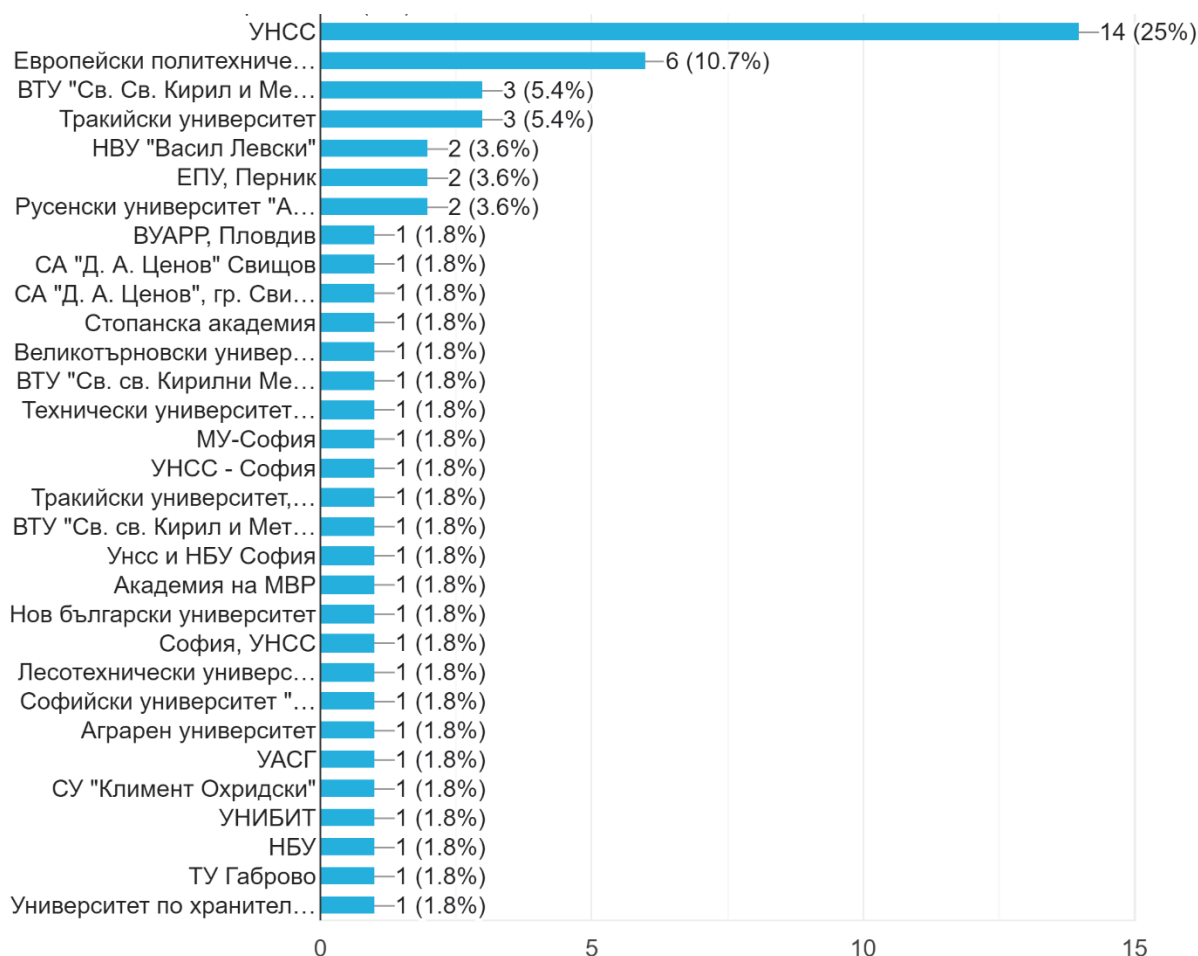
На въпрос № 4 *Вашата възраст е:* 67.9% са отговорили между 35 и 54 години, което дава основание да се твърди, че екипът от служители е сравнително млад, на трудоспособна възраст. 16.1% са между 55 и 64 години, което показва опитността и натрупаният професионализъм в годините. 14.3% са млади специалисти между 18 и 34 години, а най-малкият процент на взелите участие в проучването е на респонденти над 65 години (1.7%). Няма респонденти, които да са отговорили с „предпочитам да не отговарям“.

Вашата възраст е:



Фигура 18
Въпрос: Вашата възраст е:

На въпрос № 5 *Вашата месторабота е /моля да посочите университет и град/*: най-висок процент са работещите в УНСС, гр. София (28.6%), следвани от Европейския политехнически университет, гр. Перник (14.3%). Част от университетите, включили се в проучването, са Великотърновският университет „Св. св. Кирил и Методий“ (10.8%), Тракийския университет (7.2%), НВУ „Васил Левски“ (3.6%). Донякъде разнородната организационна среда на висшите учебни заведения спомага за получаването на обективни мнения относно информационната сигурност.



Фигура 19
Въпрос: Вашата месторабота е /моля да посочите университета и град/:

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 съвременното. 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.

Спокоен/Спокойна ли сте за информационната си сигурност и за сигурността във Вашата организация?



Фигура 20

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 борава с данните – разгласяване, модифициране, унищожаване или отказ от достъп¹⁶². Извеждат се и видовете кибератаки, например: малуер, софтуер за изнудване, тип „отказ от обслужване“, уеббазирани атаки, като комплексните устойчиви

¹⁶² 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.

атаки са класифицирани, като „най-злонамереният вид заплахи“¹⁶³. Човешката грешка се състои най-вече в неправилен избор на парола, случайно разкриване на информация и използване на неподходящ или вече остарял софтуер¹⁶⁴. 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 данни¹⁶⁵.

В Насоките на ЕС относно примерни случаи, свързани с нарушение на сигурността на личните данни¹⁶⁶ се споменава, че нарушенията по сигурността, свързани с човешка грешка, могат да бъдат избегнати посредством:

- ⇒ задължително въвеждане на програми за обучение, образование и повишаване на осведомеността;
- ⇒ намаляване на изпращането на файлове по e-mail, като алтернативата за това, е използване на системи за обработване на клиентски данни;
- ⇒ извършване на двойна проверка преди изпращане на файлове;
- ⇒ разделяне на опции при създаване и изпращане на файлове.

Повишаването на осведомеността на потребителите, като компонент, е засегнато в Наредба за минималните изисквания за мрежова и информационна сигурност¹⁶⁷. Там се отбелязва, че субектът е обезпечител на сигурността посредством:

- ⇒ подходящо професионално обучение за повишаване квалификацията на служителите в съответствие с използваната техника и технологии;
- ⇒ провеждане на периодичен инструктаж с цел повишаване на вниманието.

¹⁶³ Пак там, с. 13.

¹⁶⁴ Стоицов, Г. (2020). Информационна и комуникационна сигурност. ПУ „Паисий Хилендарски“, с. 15.

¹⁶⁵ Пак там.

¹⁶⁶ Насоки 01/2021 относно примерни случаи, свързани с уведомяването за нарушение на сигурността на личните данни. Достъпно на: https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_bg.pdf.

¹⁶⁷ Наредба за минималните изисквания за мрежова и информационна сигурност. Достъпно на: https://www.mtc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf.

Благодарение на тези мерки се създават възможности за адекватно реагиране при инциденти, свързани с мрежовата и информационна сигурност¹⁶⁸.

**Според Вас на какво предимно се дължат
различните пробиви и проблеми с
информационната сигурност?**



Фигура 21

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 сринове на

¹⁶⁸ Танев, Я., Митев, М. (2024). Предизвикателства пред приложение на новата европейска политика за киберсигурност в българската администрация. София: Институт по публична администрация, с. 30.

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, 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.

**Колко често Ви се е случвало да има срив в
информационната система, докато упражнявате
своите работни дейности?**



Фигура 22

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.

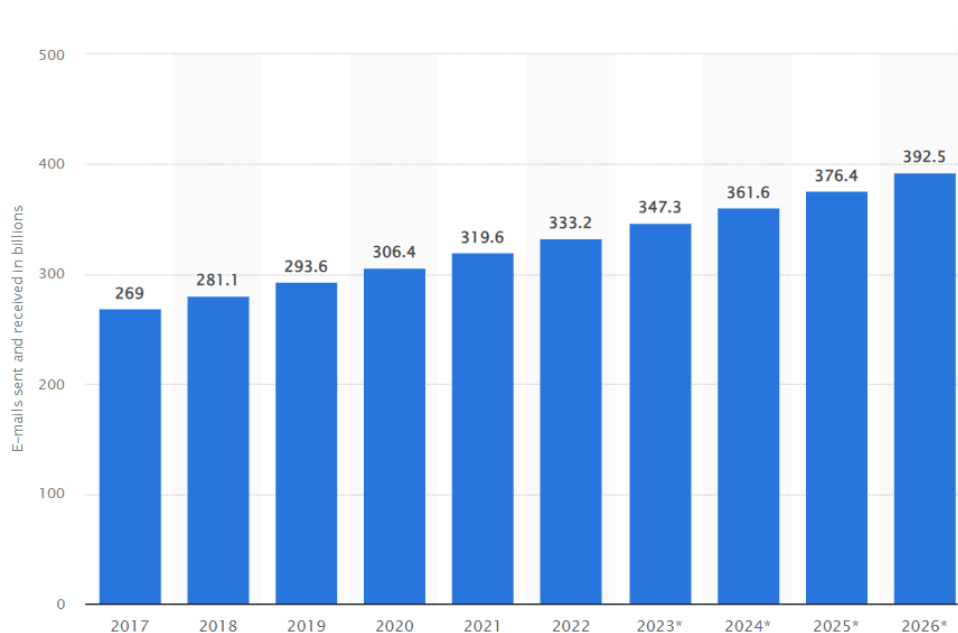
Всеизвестно е, а и в анкетата се потвърждава, че имейла е една от най-популярните форми на комуникация, която хората използват, но е и една от най-злоупотребяваните такива. В края на миналата година Sinch Mailgun¹⁶⁹ анкетира повече от 2000 потребители в САЩ, Великобритания, Франция, Германия и Испания, 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 канал¹⁷⁰.

Повече от петдесет години от изпращането на първия имейл през 1971 г., потокът от имейл трафик нараства с всяка изминала година. Над четири милиарда потребители на електронна поща изпращат повече от 300 милиарда имейли всяка година според Statista.

¹⁶⁹ 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/>.

¹⁷⁰ 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/>.



Фигура 23
Изпратени и получени имейли в периода 2017 – 2026 според Statista
Източник: Statista¹⁷¹

¹⁷¹ Number of sent and received e-mails per day worldwide from 2017 to 2026 (in billions). Available on: <https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/>.

**По кой канал най-често получавате информация,
за да може да извършвате ежедневните си
работни задължения?**



Фигура 24

По кой канал най-често получавате информация, за да може да извършвате ежедневните си работни задължения?

На въпрос № 10 *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?* 60.7% отговарят с „Да, може да се каже“, а 25% убедително с „Да, на много високо ниво“. 8.9% изразяват полярно мнение, като твърдят, че не са изобщо на високо ниво. 2% изразяват колебание, а 1.4% не могат да дадат мнение. Може да се направи извода, че висок процент от анкетираните споделят положителното схващане и убеждение, че служителите, които отговарят за поддържането на системите за ИС са на достатъчно добро ниво, за да могат да се справят в ситуации, които изискват предотвратяване на инциденти по сигурността. Респондентите считат, че този персонал има възможностите да предприеме адекватни действия в напрегнати моменти на кризи.

Спазването от страна на служителите на контролите за информационна сигурност е основно предизвикателство пред управлението в организациите. Докато инвестициите в

тази посока се увеличават, организациите не успяват да избегнат заплахи за сигурността и пробиви на данни поради „*несъответстващи служители*“¹⁷².

Защитата на информацията и активите на организациите изисква повече инвестиции в информационната сигурност за постигане на техните цели и защита¹⁷³, като служителите, отговарящи за тази дейност, трябва да бъдат на високо ниво. Учените обръщат по-малко внимание на редица важни фактори, свързани със служителите, което открива нови възможности за изследване в областта на културата на информационната сигурност¹⁷⁴. Silic et al. установяват, че само 5% от изследванията на информационната сигурност между 1993 г. и 2012 г. се фокусира върху човешките аспекти на информационната сигурност¹⁷⁵, а Karlsson et al. отбелязват, че изследователите обръщат относително по-малко внимание на корелацията между местната култура на служителите и тяхното поведение в областта на информационната сигурност¹⁷⁶.

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 включва¹⁷⁷:

- ⇒ откриване, наблюдение и посредничество в различни аспекти на сигурността – включително физическа сигурност, софтуерна сигурност и мрежова сигурност;
- ⇒ извършване на тестове за контрол на съответствието;

¹⁷² AlGhamdi, S., Win, K., Vlahu-Gjorgievska, E. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. // *Government Information Quarterly*. 39(4).

¹⁷³ Posey, C., Roberts, T., Lowry, P. (2016). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. // *Journal of Management Information Systems*. 32(4), pp. 179–214.

¹⁷⁴ Da Veiga, A. et al. (2017). Defining and identifying dominant information security cultures and subcultures. // *Computers & Security*. 70, pp. 72–94.

¹⁷⁵ Silic, M., Back, A. (2014). Information security: Critical review and future directions for research. // *Information Management & Computer Security*.

¹⁷⁶ Karlsson, F., Åström, J., Karlsson, M. (2015). Information security culture–state-of-the-art review between 2000 and 2013. // *Information & Computer Security*. 23(3), pp. 246–285.

¹⁷⁷ Force, J. (2020). Security and Privacy Controls for Information Systems and Organizations. U.S. Department of Commerce: National Institute of Standards and Technology.

- ⇒ 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

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

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?



Фигура 25

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.

Едно от най-значимите предимства на обучението по киберсигурност за служителите е повишената осведоменост относно заплахите. За съжаление, голяма част не са наясно с потенциалните рискове, свързани с тяхната дигитална дейност, и могат по невнимание, да изложат организацията си на риск.

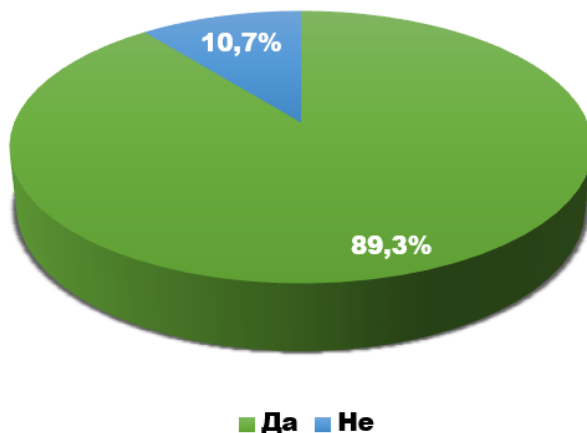
Чрез обучение по киберсигурност служителите могат да научат за различните видове киберзаплахи, как да ги идентифицират и как да ги избягват. Това може да включва обучение за фишинг, зловреден софтуер, социално инженерство и пробиви на данни. В резултат на това, организациите могат да намалят вероятността от успешни кибератаки чрез повишаване на информираността на служителите за тези заплахи¹⁷⁸.

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 ежедневието 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 ръководители¹⁷⁹.

¹⁷⁸ Haney, J., Lutters, W. (2020). Security Awareness Training for the Workforce: Moving Beyond “Check-the-Box” Compliance. // Computer. 53(10).

¹⁷⁹ Ibidem.

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



Фигура 26

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“.

**При възникване на инцидент, свързан с
информационната сигурност, Вие първо ще:**



Фигура 27

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.

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

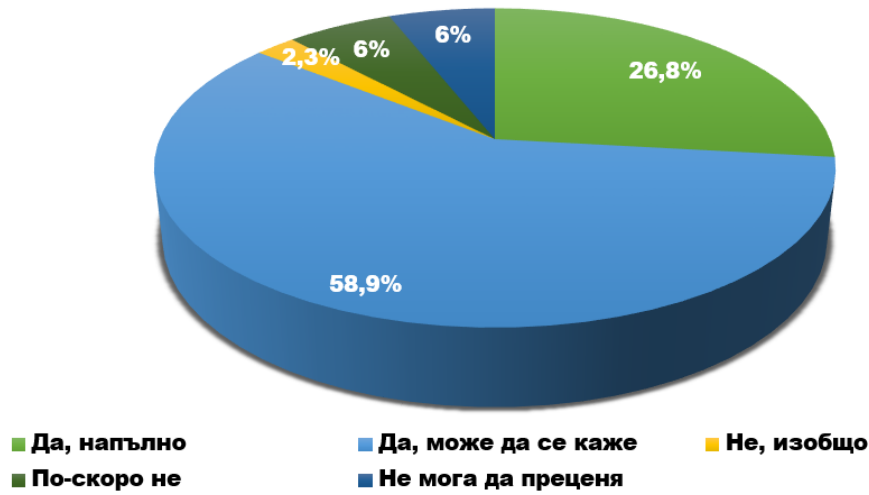


Фигура 28

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.

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



Фигура 29

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“.

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



Фигура 30

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.

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



Фигура 31

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 изведените 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 системи¹⁸⁰. 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 ресурси¹⁸¹.

3.2. Концептуален модел за ограничаване на уязвимостите и заплахите на информационната сигурност в университетите

Предложеният модел се основава на систематичния подход за идентифициране и вземане на решение кои контрмерки са необходими да се предприемат, за да се защити информацията, както и ресурсите и спомагателните източници въз основа на оценката на заплахите и уязвимостите. За да се разработи и приложи модел за информационна сигурност с цел да се ограничат уязвимостите и заплахите, е необходимо „да се реализира рентабилна система за сигурност“¹⁸², като се има предвид, че инвестираните разходи няма да бъдат възстановени¹⁸³.

Модерният университет изцяло е насочен към „интернационализация, конкурентоспособност и иновации“¹⁸⁴, което показва, че „приоритетни теми са дигиталната трансформация, киберсигурността, както и законовономативната

¹⁸⁰ 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.

¹⁸¹ Edgar, T., Manz, D. (2017). Research Methods for Cyber Security. Elsevier Inc.

¹⁸² Павлов, Г. (2012). Информация и сигурност. София: Авангард Прима, с. 147.

¹⁸³ Пак там.

¹⁸⁴ Павлова, Е. (2023). Референтен модел за киберсигурност при проектирането на онлайн услуги във висши учебни заведения в България. Автореферат. София: УНСС, с. 17.

база“¹⁸⁵. Той си посредничи с т.нар. *умни градове*, които се изграждат посредством „умни технологии“, насочени към определени сектори¹⁸⁶.

Целта на разработването на модела е да помогне на ръководителите на сектора за ИС към висшите учебни заведения при вземането на решения за мерки за сигурност срещу заплахи за ИТ средата с цел намаляване на вероятността от компрометиране на чувствителна информация.

Важно е уточнението, че дисертационният труд се придържа към формулираната от Тагарев цел на ИС, а именно „*да осигури защитата на критичната информация, като осигури цялостност, наличност и поверителност на информацията.*“¹⁸⁷. По своята същност цялостността/интегритетът на информацията съставляват нейната достоверност и надеждност¹⁸⁸. Наличността представлява способността на информацията и свързаните с нея ресурси да бъдат налични¹⁸⁹.

Анализът на заплахите за сигурността се занимава с въпроси като принципи и отговорности, оценка на заплахите за сигурността, управление на риска и използвания метод за неутрализиране на заплахите. Управлението на риска за сигурността предполага планиране, организиране, управление и контрол на ресурсите, за да се гарантира, че рисковете се поддържат в приемливи граници. Whitten счита, че управлението на риска е интерактивен, непрекъснат процес между текущото и желаното състояние на сигурност чрез оценка и управление на съществуващите рискове¹⁹⁰.

¹⁸⁵ Пак там.

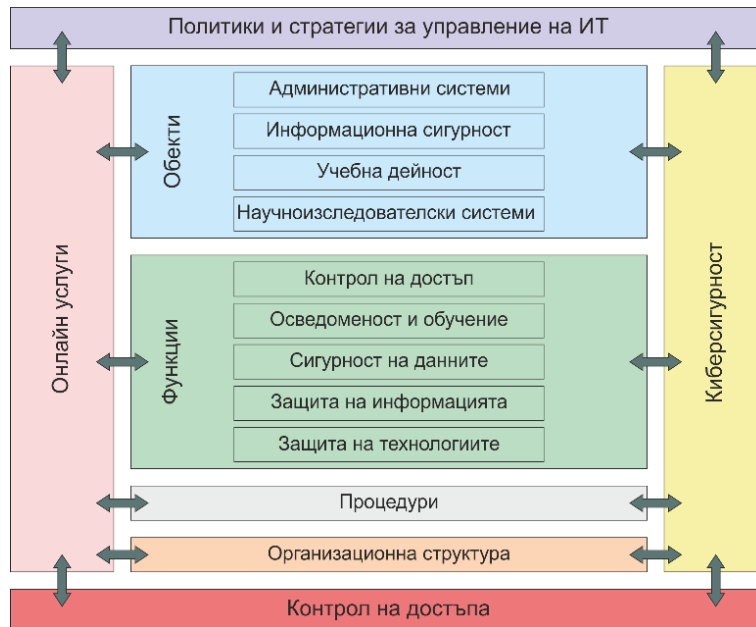
¹⁸⁶ Тагарев, Н. и др. (2021). Модел на умните градове и проблеми с киберсигурността. // Тагарев, Н. и др. Икономически аспекти на модели за оценка на киберсигурност в умни градове. София: ИК – УНСС, с. 15.

¹⁸⁷ Тагарев, Н. (2021). Съвременни подходи при управлението на киберсигурността. София: Авангард Прима, с.13.

¹⁸⁸ Пак там, с. 17.

¹⁸⁹ Пак там.

¹⁹⁰ Whitten, A. (1999) Information resources management. Ediția 1. Londra: Ideea Group Publishing.



Фигура 32
Референтен модел за киберсигурност
Източник: Адаптирано по Павлова, Е. (2023). Цит. съч., с. 34

Гореизложеният референтен модел се основава в своята структура на следните взаимовръзки¹⁹¹:

- ⇒ контрол на достъпа;
- ⇒ обект – ИС;
- ⇒ функции;
- ⇒ процедури;
- ⇒ организационна структура.

Референтният модел за киберсигурност представя една „абстрактна рамка за разбиране на значими взаимоотношения между обектите на дадена среда, и за разработване на последователни стандарти или спецификации, поддържащи тази среда“¹⁹², което е помощно средство за разработването на авторския модел за подобряване на информационната сигурност, като се има предвид цялостната концептуална рамка, която

¹⁹¹ Павлова, Е. (2023). Цит. съч., с. 34.

¹⁹² Пак там, с. 12.

е изложена и която рамка изгражда „комуникация и разбиране за елементите на системата и техните значими взаимоотношения в рамките на дадена общност“¹⁹³.

Успехът на една организация да предпази своите възпитаници и персонал от злоумишлени атаки зависи до голяма степен от ролята на висшето ръководство в процеса. Трябва да има съгласие на ръководството относно поставената цел, с подкрепа на всички нива на организацията, преразглеждане на определени принципи и цели на управление.

Оттук следва да се изведат съвременните практически критерии за защита и криптиране на информацията в ИС¹⁹⁴:

- ⇒ секретност – изцяло зависи от работния фактор, т.е. от наличните времеви и изчислителни ресурси, които може да компрометират използвания криптографски механизъм;
- ⇒ функционалност – съгласуваност между елементите и задачите за достигане ниво на ефективност;
- ⇒ методи за опериране – оценка на поведението като фактор за сигурността;
- ⇒ производителност и бързина – скорост на криптиране на информацията;
- ⇒ внедримост – сложността на хардуерна и софтуерна реализация.

Разработването на ефективен модел за ограничаване на уязвимостите и заплахите на информационната сигурност, следва да се основава на кумулативни данни и информация, а дейността по оценката на неговата функционалност, трябва да включва действия като¹⁹⁵:

- ⇒ идентифициране на домейна и целите;
- ⇒ идентифициране на физическите ресурси и информация, които подпомагат изпълнението на мисията на организацията, както и тяхната важност (стойност);
- ⇒ идентифициране на заплахата и уязвимостта във връзка с рисковата среда и ниво;
- ⇒ идентифициране на нивото на риска.

¹⁹³ Пак там.

¹⁹⁴ Павлов, Г. (2012). Информация и сигурност. София: Авангард Прима, с. 125–126.

¹⁹⁵ ISO/IEC 27005: 2011 Information technology — Security techniques — Information security risk management. Available on: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en>.

Изграденият модел се основава на следните критерии, показатели и компоненти:

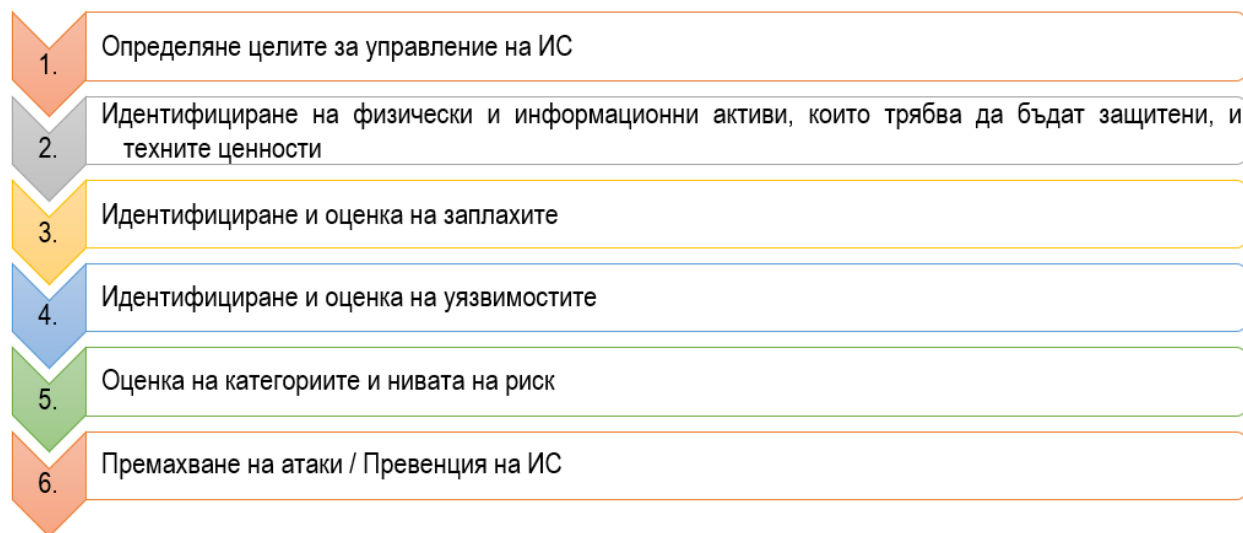
Таблица 5

Критерии, показатели и компоненти на Модела

КРИТЕРИИ	ПОКАЗАТЕЛИ	КОМПОНЕНТИ
Риск мениджмънт	1. Цели 2. Заплахи 3. Оценка на риска 4. Анализи	- цели; - организационни; - рискови; - аналizationsонни.
Имплементиране на ИС	1. Област на образование 2. Цели на сигурност 3. Критични активи 4. Оценяване на заплахи 5. Ниво на прогнозния риск 6. Мерки и процедури	- образователни; - цели; - критичност; - оценка; - прогнозируемост; - процедурност; - процесуалност.
Киберпространство	1. Човешки ресурс 2. Данни и информация 3. Сигурност 4. Инфраструктура	- човешки капацитет; - информираност; - внедряване; - дигитализация; - архитектура.
Архитектура на ИС	1. Удостоверяване 2. Контрол на достъпа 3. Поверителност на данните 4. Цялост на данните 5. Мрежова сигурност 6. Защита на крайни точки 7. Нормативна уредба	- човешки капацитет; - контролираност; - идентификация; - липса на модификация; - сигурност на данни, приложения; - законови механизми.
Процес на реагиране/разкриване на заплахи	1. Подготовка 2. Идентификация 3. Ограничаване 4. Премахване на евентуални атаки 5. Възстановяване 6. Анализ и поука от опита	- политики и процедури; - мониторинг; - превантивност; - първопричина; - изходяща точка/ниво; - декомпозиция.
Киберсигурност	1. Събиране на данни 2. Разпознаване на „лоши“ метрики 3. Познаване на потребителите 4. Добри метрики 5. Ресурси	- вид на използваната метрика; - ефективност на системата; - анализ на потребителите; - измерване; - капацитет.

Източник: авторска разработка

Компонентите на Модела се състоят от шест стъпки, показани по-долу на диаграмата.



Фигура 33
Целеви категории към критерий за рисков мениджмънт на Модела
Източник: авторска разработка

Въз основа на тези целеви категории трябва ясно да се посочи нивото на приетия риск за ИС на висшето учебно заведение, както и времевата рамка и инвестициите, които потенциално ще бъдат изразходени.

Риск мениджмънтът е съществен елемент от цялостната архитектура на ИС, тъй като се измерва оценката на риска, като най-простият метод, който може да бъде приложен, е „умножение на вероятността от осъществяване на заплахата и предполагаемите щети.“¹⁹⁶. Ценно правило е, че „*рискът се появява там, където има заплахата.*“¹⁹⁷.

Димитров разработва метод на сценарийното планиране и прогнозиране, като счита, че това „*е по същество иконометрична дейност, която се състои в търсене на законите за развитието, обясняване на дадено явление и прилагане на наученото към бъдещето.*“¹⁹⁸. Всъщност моделът за ограничаване на уязвимостите и заплахите по

¹⁹⁶ Павлов, Г. (2012). Цит. съч., с. 145.

¹⁹⁷ Цит. съч., с. 144.

¹⁹⁸ Димитров, Д. (2012). Приложение на сценарийното планиране в бизнеса, избраната и сигурността. София: УНСС, с. 15.

презумпция си взаимодейства със сценарий за ясно и конкретно планиране и прогнозиране на процесите, за да положи в основата си качествено ефективна архитектура на ИС.

Разработването и прилагането на метода за сценариите, допринася за стратегическото мислене и планиране, като същевременно се постига¹⁹⁹:

- ⇒ систематичност в проучването на алтернативи, които съдържат тенденции и ключови области на стратегическо планиране;
- ⇒ редуциране на сложността в едно неопределено и противоречиво настояще;
- ⇒ осигуряване на възможности за интегритет на полярни позиции с цел взимане на прагматични решения;
- ⇒ интегриране на статистически данни от количествени проучвания с информация, получена от качествени такива.

Въз основа на сценарийното планиране се постига отчетност, отговорност и прозрачност; сигурност, безопасност, автономия и свобода; идентичност и неприкосновеност на личния живот и данни²⁰⁰. Според учения икономическият анализ не е единственият важен фактор, благодарение на който може да се вземат адекватни решения, но *„от съществена важност е той да се използва по подходящ начин“*²⁰¹, защото *„наличието на много добре дефинирани процедури и организации, които извършват специализиран анализ“*²⁰² спомага за адекватното взимане на решения и подхождането към прогнозируем резултат; за определяне на целите и задачите; за верифициране на опита.

Във втория етап трябва да се идентифицира цялата чувствителна информация в определена област на риск за сигурността, независимо дали е чувствителна или не, информация, която може да застраши интересите на организацията, когато бъде компрометирана, както и всички активи – оборудване, приложения, съоръжения, процедури – критични към нормалното функциониране на организацията. Оценката на информационните активи може да се извърши чрез консултация със собствениците на

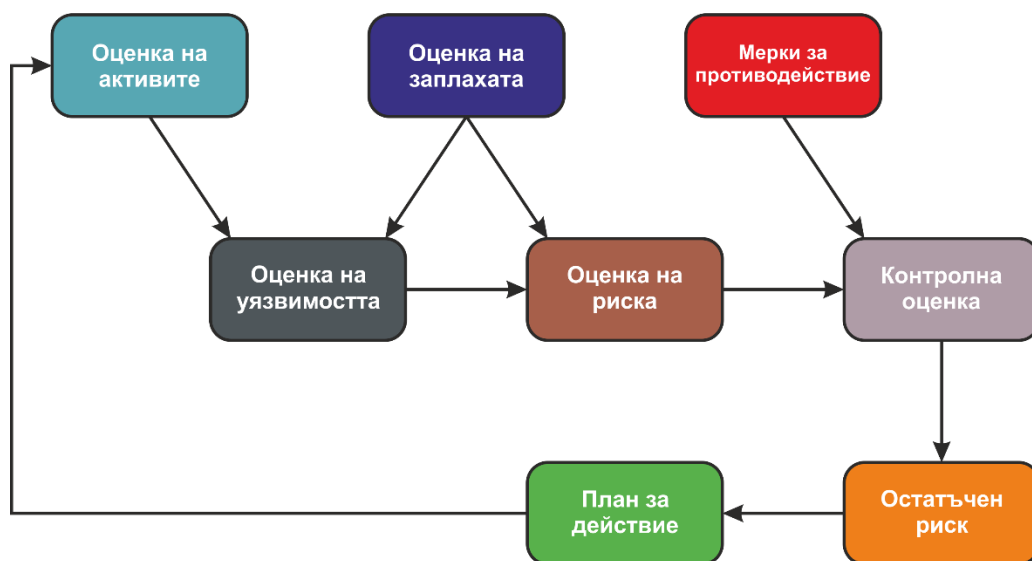
¹⁹⁹ Пак там, с. 20.

²⁰⁰ Пак там, с. 26.

²⁰¹ Димитров, Д. (2015). Икономически анализ „разходи – ползи“ в отбраната и сигурността. София: УИ „Стопанство“, с. 14.

²⁰² Пак там.

такава информация или други лица, които имат упълномощено мнение относно информационните активи. Оценката, която може да бъде качествена (например ниска, средна или висока), може да бъде получена от оценката, направена от „собствениците на информация“ или техните представители, използвайки възможно най-лошия сценарий, който може да доведе до действия спрямо нейното унищожаване, недостъпност, предоставянето ѝ на неоторизирани лица и модифицирането на информацията от неупълномощени субекти²⁰³.



Фигура 34
Целеви категории към критерий за имплементиране на Модела
Източник: авторска интерпретация

Резултатите от оценката на ИС, предприетите действия за постигане и поддържане на минималните стандарти за защита са процесуални и включват:

- 1) Областта и целите на оценката на ИС.
- 2) Целите за сигурност на организацията по отношение на поверителността, целостта, наличността и надеждността.
- 3) Списък на критичните активи, които трябва да бъдат защитени.
- 4) Анализ на оценените заплахи за критичната архитектура на сигурността.
- 5) Анализ на оценените уязвимости.

²⁰³ Haimes, Y. (1998) Risk Modeling, Assessment, and Management. Ediția 1. New York: Wiley

- 6) Нивото на прогнозния риск и неговите характеристики.
- 7) Мерки и процедури, които трябва да се предприемат за намаляване нивото на риска;

Разработването на модел пряко се подчинява на рисковите фактори и уязвимостите, които може да провалят системата за сигурност.

Модел на информационна сигурност, който ще служи за комплексно управление на кризи в случай на атака от киберпространството, има четири основни вертикални оси:

1. Хора и идентичност – всяка организация трябва да е сигурна, че оторизираните потребители в организацията и извън, нея ще имат достъп до данните и инструментите, от които се нуждаят, във време, когато е необходимо. Неоторизираният достъп трябва да бъде блокиран. Големите организации имат голям брой различни потребители, така че това означава, че контролът на достъпа е много важен и сложен поради многокомпонентност. Важна част от контрола на достъпа и проверката на самоличността е наблюдението на привилегировани потребители, като например администратори.

2. Данни и информация – организациите и лицата трябва да защитават неструктурираните и структурирани данни, за да управляват обхвата. Определя се нивото на поверителност, стойността на данните и информацията, също – контрола на риска. Ефективният план за защита на данните и информацията включва каталог, съответно инвентаризация на тези файлове с атрибути, политики и услуги, които управляват достъпа, трансфера и трансформацията на данни и информацията, включена в архивите на данни. За много организации поверителността е най-важното нещо за функциите за безопасност. Шифроването и защитата на ключовете за криптиране е от решаващо значение за осигуряване на защита на данните и за спазването на новото входящо законодателство на ЕС²⁰⁴.

3. Сигурност на приложението – най-ефективната предпазна мярка срещу проникване е подходът на организацията, който изисква потребителите да използват приложения, които са предложени и внедрени. Организациите и хората трябва проактивно да защитават своите критични приложения срещу външни и вътрешни заплахи през целия им жизнен

²⁰⁴ EU Cyber defence Policy framework. Available on: <https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf>.

цикъл, т.е. от проектирането, разработването, тестването и производството. Автоматични проверки на изходния код на приложението и тест на операционните системи дава възможност за идентифициране на уязвимости, които могат да бъдат използвани от нападатели. За да се предпазят нападателите от вътрешната защитена зона на институциите и едновременно с това да се предоставят услуги за потребителите от незащитен интернет, трябва да се използва специализирана демилитаризирана зона²⁰⁵, за да се използват приложения, които са предложени и внедрени с оглед на сигурността. Защитната стена е основен компонент на технологията за мрежова сигурност, която наблюдава и контролира входящия и изходящия поток от данни в съответствие с предварително установени правила за безопасност.

4. Инфраструктура – инфраструктурата на организациите и лицата, която се състои от мрежа, сървъри, рутери, носители за съхранение, храняващи уреди и други компоненти, трябва да бъде физически и електронно проектирана и внедрена сигурно, за да се предотвратят физически и електронни прониквания. Физическо проникване може да бъде елиминирано чрез адекватно наблюдение на достъпа и биометрични системи. Електронните прониквания се елиминират от защитни стени и антивирусни програми с предимно ежедневни актуализации и с нови сигнатури на вируси и разпознаване на зловреден софтуер.

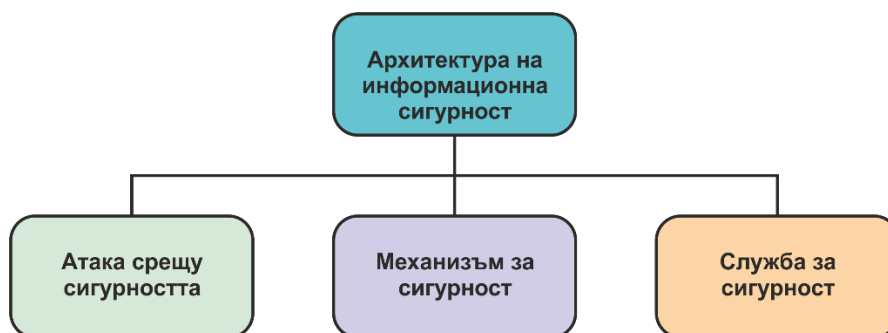


Фигура 35
Целеви категории към критерий за киберпространство на Модела

²⁰⁵ EU International Cyberspace Policy. (2014). European Union External Action. Available on: http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm.

По своята същност критичната инфраструктура представлява „свкупност от ключови сектори на модерното общество, които са жизненоважни за националната сигурност.“²⁰⁶.

Архитектурата, наречена демилитаризирана зона, се използва за справяне с безопасността на настоящите компютърни системи, която е основно физическа или логическа компютърна подмрежа, разделена със специализирани защитни стени от интернет и защитена инфраструктура на организацията. Управлява се от организации, които трябва да направят своите услуги и данни достъпни за оторизирани интернет потребители. Целта е да добави още един слой за подобряване на сигурността на защитената локална мрежа на организацията. Достъп ще имат само външни потребители към устройства, сървъри и бази данни в демилитаризираната зоната.



Фигура 36
Опростен модел на архитектура на сигурността
Източник: авторска интерпретация

ИС е обработка или комуникация, която подобрява надеждността и валидността на системите за обработка на данни чрез защита на потока от информация. Това включва: удостоверяване, контрол на достъпа, поверителност на данните, интегритет на данните и достъпност.

⇒ удостоверяване – потвърждава, че потребителят, който се опитва да получи достъп до системата, е този, за когото се представя. Това може да бъде постигнато чрез комбинация от пароли, потребителски имена, токени, биометрични данни и т.н.

²⁰⁶ Тагарев, Н. (2021). Цит. съч., с. 23.

- ⇒ контрол на достъпа – ограничава достъпа до система или информация до упълномощени лица. Може да се основава на потребителски идентификационни данни, потребителско местоположение, потребителски роли или други критерии.
- ⇒ поверителност на данните – поддържа поверителността на информацията, докато се предава. Това обикновено се постига чрез криптиране, използване на защитен софтуер за споделяне на файлове, прилагане на политики за поверителност и/или други.
- ⇒ цялост на данните – гарантира, че данните не се променят или модифицират при пренасяне или съхранение. Освен това, че данните, получени от приемника, са от доверен източник.



Фигура 37
Целеви категории към критерий за архитектура на Модела
Източник: авторска интерпретация

Рамката на архитектурата за сигурност е набор от последователни насоки и принципи за прилагане на различни нива. Организацията може да избере да създаде своите рамки чрез комбиниране на международни стандартни рамки, като например: TOGAF, SABSA, OSA. Данните, съхранявани в облак, също се нуждаят от защита от неоторизиран достъп, злонамерени атаки и други потенциални заплахи. Архитектурата за сигурност в облака е комбинация от стратегии, политики и контроли, използвани за защита на базираните в облак данни, които организациите съхраняват и обработват. Това включва контролите за физическа, мрежова и хост сигурност за данни в облака.

Архитектурата за облачна сигурност е критичен компонент поради нарастващата зависимост от облачните изчисления за съхранение и обработка на данни.

Архитектурата на киберсигурността се фокусира върху това, което е налице, за да защити цифровите активи, данни и системи на бизнеса от различни заплахи и уязвимости. Тя трябва да включва рамка и стабилни политики на различни нива на организацията.

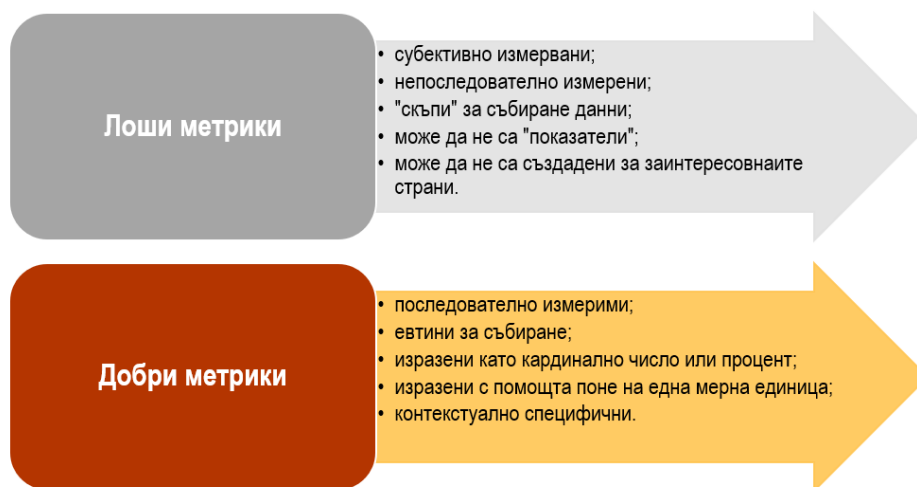
Последният критерий за киберсигурност се основава на изследването на Тагарев за добри и лоши метрики за измерване на киберсигурността²⁰⁷. Значението на използваните метрики се обуславят посредством²⁰⁸:

- ⇒ **оценка на вътрешната среда** – благодарение на компонентите споделяне на наученото, отбелязване на позитивите, подобрене в работата, използване на установеното, създаване на култура може да се приоритизират различни вариации за ефективен и качествен процес;
- ⇒ **измерими бизнес стойности** – междукulturна комуникация на добро ниво, за да се унифицират целите на организацията;
- ⇒ **обективно представяне на проблемите** – включва визуално представяне на стойността, конкретни примери за разходи;
- ⇒ **обосновка за нови инвестиции** – обсъждане на проблемите, свързани с ползите от киберсигурност, а също така използване на подходи за капиталово бюджетиране;

²⁰⁷ Тагарев, Н. и др. (2021). Добра срещу лоша метрика // Тагарев, Н. и др. Икономически аспекти на модели за оценка на киберсигурност в умни градове. София: ИК – УНСС, с. 79.

²⁰⁸ Пак там, с. 80–81.

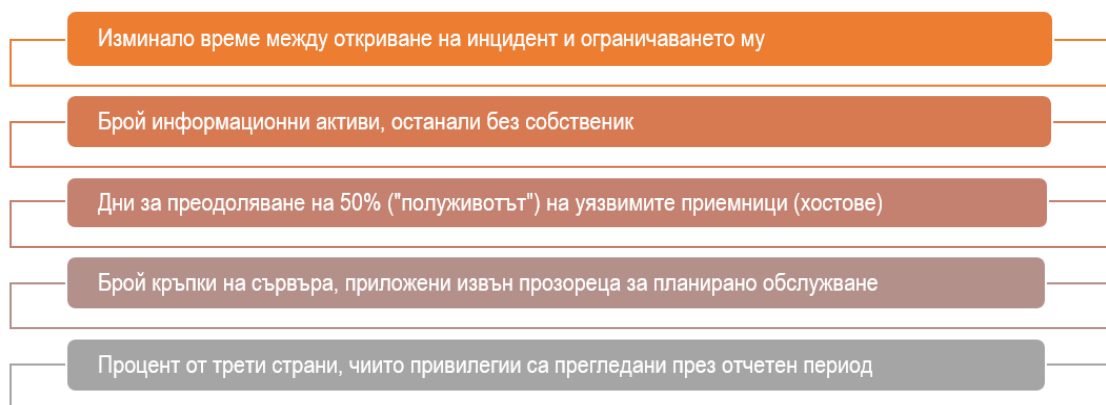
⇒ **подобрения** – одитиране, криптиране, обучение, внедряване на добри практики.



Фигура 38

Целеви категории за добри и лоши метрики към критерий за киберсигурност на Модела
Източник: Адаптирано по Тагарев, Н. и др. (2021). Цит. съч., с. 82

Добрите и лошите метрики трябва да се съгласуват с пет основни показателя за информационна сигурност, изложени на диаграмата²⁰⁹:



Фигура 39

Целеви категории за добри и лоши метрики към критерий за киберсигурност на Модела
Източник: Адаптирано по Тагарев, Н. и др. (2021). Цит. съч., с. 87

²⁰⁹ Тагарев, Н. и др. (2021). Модел на метрика чрез „Пет показателя за сигурност, които трябва да се вземат предвид“ // Тагарев, Н. и др. Икономически аспекти на модели за оценка на киберсигурност в умни градове. София: ИК – УНСС, с. 87.

Има много компоненти и слоеве в архитектурата на киберсигурността, включително:

1. Мрежова сигурност – защита на мрежовата инфраструктура на организацията с помощта на защитни стени, системи за откриване и предотвратяване на проникване (IDPS) и виртуални частни мрежи (VPN) за контрол и наблюдение на мрежовия трафик. Необходимостта от въвеждане на VPN е породена от *„нарасналите изисквания относно сигурността на системите за връзка.“*²¹⁰. Именно за да се установи гарантирана защита, съществуват пет критични елемента за сигурност²¹¹:

- ⇒ идентичност;
- ⇒ сигурност на периметъра;
- ⇒ сигурна връзка;
- ⇒ наблюдение на сигурността;
- ⇒ управление на политиката за сигурност.

VPN създава възможност за *„защитен канал за обмяна на информация между отдалечени потребители, което позволява сигурен достъп до ресурсите на основната система.“*²¹².

2. Защита на крайни точки – защита на отделни устройства като компютри, смартфони и сървъри с помощта на антивирусен софтуер, инструменти за откриване и реагиране на крайни точки (EDR) и системи за управление на мобилни устройства (MDM). Също така включва защита срещу зловреден софтуер и неоторизиран достъп.

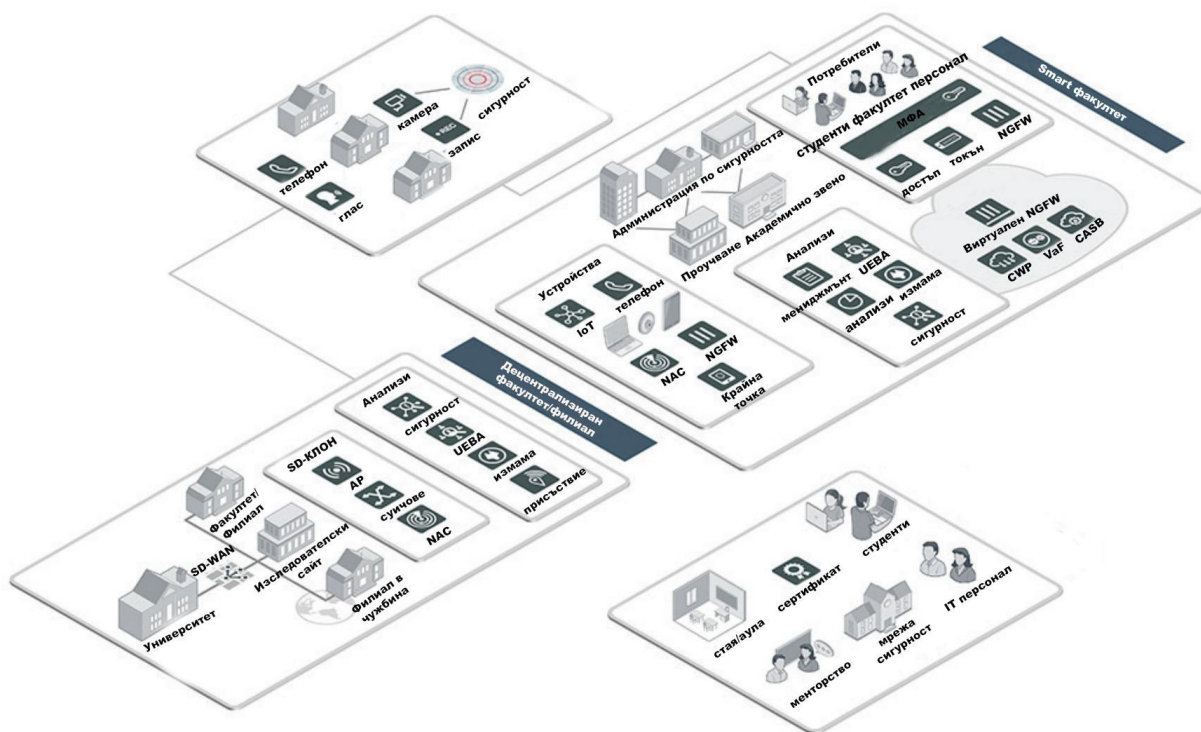
3. Сигурност на данните – шифроване на данни за предотвратяване на нарушения на данните. Тук се използват инструменти за предотвратяване на загуба на данни (DLP) и протоколи за криптиране, за да се защити чувствителната информация от неоторизиран достъп или кражба.

²¹⁰ Павлов, Г. (2012). Цит. съч., с. 135.

²¹¹ Пак там.

²¹² Пак там.

4. **Сигурност на приложенията** – защита на софтуера и приложенията чрез редовни прегледи на кодове, оценки на уязвимости и защитни стени на уеб приложения (WAF), за да помогнете за идентифициране и смекчаване на уязвимостите на ниво приложение.
5. **Съответствие с нормативната уредба** – осигуряване на съответствие със съответните индустриални разпоредби и закони за защита на данните, тъй като неспазването може да доведе до сериозни правни и финансови последици.
6. **Разузнаване на заплахи** – актуализиране и бърза реакция на възникващи заплахи и уязвимости, като предоставя на организацията ценна информация за проактивна защита.



Фигура 40
Модел за информационна сигурност
Източник: авторова интерпретация на архитектурата на Модела

Анализът на поведението на потребителите и субектите (UEBA) е решение за киберсигурност, което използва алгоритми и машинно обучение за откриване на аномалии

в поведението не само на потребителите в корпоративна мрежа, но и на рутери, сървъри и крайни точки в тази мрежа.

Решенията за контрол на достъпа до мрежата (NAC) поддържат видимостта на мрежата и управлението на достъпа чрез прилагане на политики на устройства и потребители на административни мрежи, но трябва да се има предвид, че *„процесът на разработване на информационна политика е като кръг, който винаги [...] връща в началната точка.“*²¹³.

IoT сигурност (защита на интернет на нещата) е технологичният сегмент, фокусиран върху защитата на свързани устройства и мрежи в IoT. Включва добавяне на интернет свързаност към система от взаимосвързани изчислителни устройства, механични и цифрови машини, обекти, животни и хора. Всяко нещо има уникален идентификатор и възможност за автоматично прехвърляне на данни през мрежа. Разрешаването на устройствата да се свързват с интернет, обаче, ги отваря пред сериозни уязвимости, ако не са правилно защитени.

CASB са решения за защита, които налагат правила за достъп за ресурси и приложения в облака, като предоставят видимост, контрол на данните и анализ.

VaF е сертифициран като признат технически експерт за Европейския печат за поверителност.

Защитата на облачните работни натоварвания (CWP) е процес на непрекъснато наблюдение и премахване на заплахи от облачни натоварвания и контейнери.

Моделът за информационна сигурност отговаря на три важни стандарта за изпълнение на най-добрите практики при защита на сигурността:

- 1) Разработване на политики.
- 2) Изпълнение на фаза 1 – разработване на политики, стандарти и най-добри практики на организацията според архитектурните рамки за киберсигурност.
- 3) Мониторинг на фаза 1 и фаза 2 – включва използване на градивните елементи на сигурността и прилагане на концепции за проектиране.

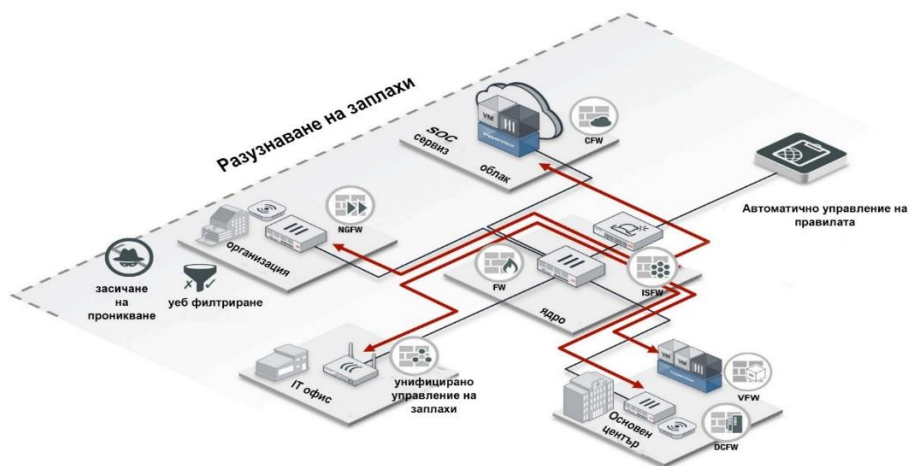
²¹³ Павлов, Г. (2012). Цит. съч., с. 146.

4) Използване на фаза 3 – наблюдение за промени, актуализации и внедряване.



Фигура 41
Фази на архитектурата за киберсигурност
Източник: авторова интерпретация

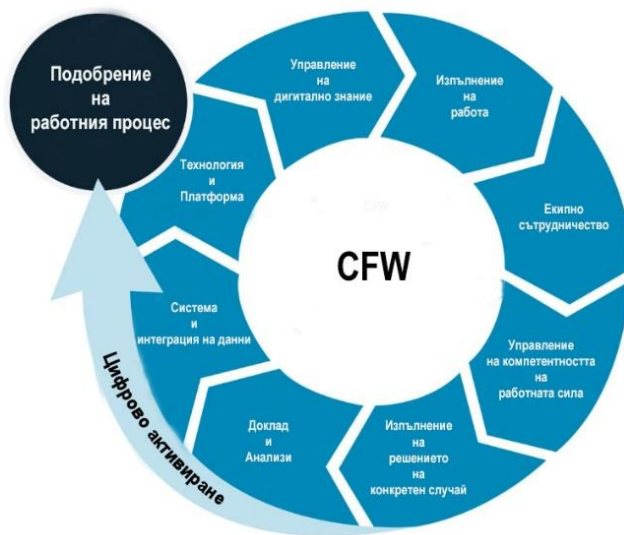
Структурата за сигурност, описана тук, може да помогне на ВУЗ да се справи с предизвикателства в сътрудничество със собствения си административен и ИТ персонал.



Фигура 42
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.



Фигура 43
Функционалности на CFW
Източник: авторова интерпретация

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 6
Видове заплахи за информационната сигурност

Критерии				
Източник	Произход		Характер	Време
Вътрешен	Естествен		Икономически	Временни
Външен	Социален	(включва	Политически	Периодични
				Намерение
				Случайно
				Умишлено

1. **Източник на заплахи** – вътрешната и външната среда е едновременно източник на заплахи и възможности. Това са външните и вътрешни условия за организациите на регионално ниво, които могат да бъдат благоприятни или не за тяхното съществуване, реализиране на техните интереси и определяне на тяхното поведение. Правната рамка, общите икономически условия в страната, политическата ситуация, развитието на местния пазар на труда и други регионални характеристики могат да се приемат като външни заплахи (или възможности). Управленски стил и умения, вид дейност, наличие или липса на иновации са сред вътрешните условия, които могат да застрашат организационните интереси. Хората могат да бъдат както вътрешни (необучени потребители, вътрешни хора), така и външни заплахи (престъпници, терористи, хакери, служители на разузнаването). Те са основните ресурси, но също така са основният източник на заплахи за информационната сигурност²¹⁵.
2. **Произход на заплахите** – могат да бъдат разделени в две основни групи. Първата група включва онези от тях, които са свързани с природата (всякакви природни бедствия, имащи потенциал да причинят щети: бури, наводнения, земетресения и др.). Към втората група могат да се отнесат различни събития и процеси, протичащи в обществото. Тези заплахи са пряко или косвено свързани с човешкото поведение във всички сфери на обществения живот на организационно, регионално, национално и международно ниво²¹⁶.
3. **Характер на заплахите** – отнася се основно до сферата на техния произход. Политическите заплахи са резултат от политическите процеси в обществото – политическа нестабилност, смяна на правителството, обществено недоволство и др. Друг вид заплахи са икономическите условия и тенденции. Демографските тенденции са много важни, особено на регионално ниво. Броят и качествената структура на

²¹⁴ Pavlov, G., Poudin, K. (2019). Challenges to information security at regional level. // Trends in Regional Development and Security Management, pp. 16–22.

²¹⁵ Ibidem.

²¹⁶ Ibidem.

населението е от решаващо значение за развитието на всички аспекти на обществения живот. Състоянието на пазара на труда зависи основно от наличието на мотивирани и добре подготвени кандидати, търсещи работа²¹⁷.

4. Време – отнася се главно до съществуването на заплахите и периода на тяхното въздействие. Повечето от заплахите са временни, но могат да имат много сериозни последици за бизнеса и публичните институции на регионално ниво, причинявайки загуби и щети²¹⁸.

5. Умисъл – показва наличието или липсата на съзнателни действия, насочени към увреждане²¹⁹.

Държавата осъзнава този проблем и затова има отделен закон за защита на класифицираната информация²²⁰, които предвиждат сериозни наказания за шпионаж и грешки при работа с класифицирана информация.

Концептуалният модел отговаря на три въпроса:

- ✓ какво се защитава;
- ✓ от кого да се защитава;
- ✓ как да се защитава.

При теоретичното изграждане на Модела е важно да се определят:

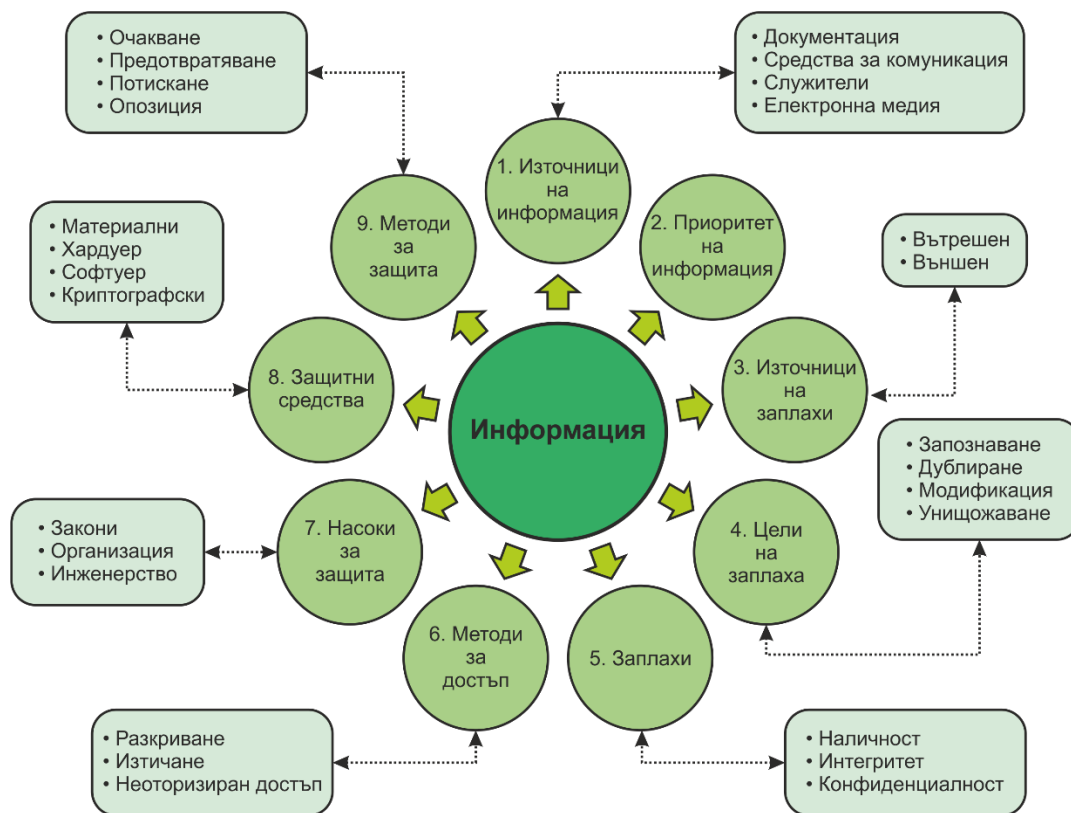
- ✓ източници на информация;
- ✓ приоритет или степен на важност на информацията;
- ✓ източници на заплахи;
- ✓ цели за заплаха;
- ✓ заплахи;
- ✓ методи за достъп;
- ✓ насоки на защита;
- ✓ средства за защита;
- ✓ методи за защита.

²¹⁷ Ibidem.

²¹⁸ Ibidem.

²¹⁹ Ibidem.

²²⁰ Закон за защита на класифицираната информация. Достъпно на: <https://lex.bg/laws/ldoc/2135448577>.



Фигура 44
Имплементиране на концепция за информационна сигурност към Модела
Източник: авторова интерпретация

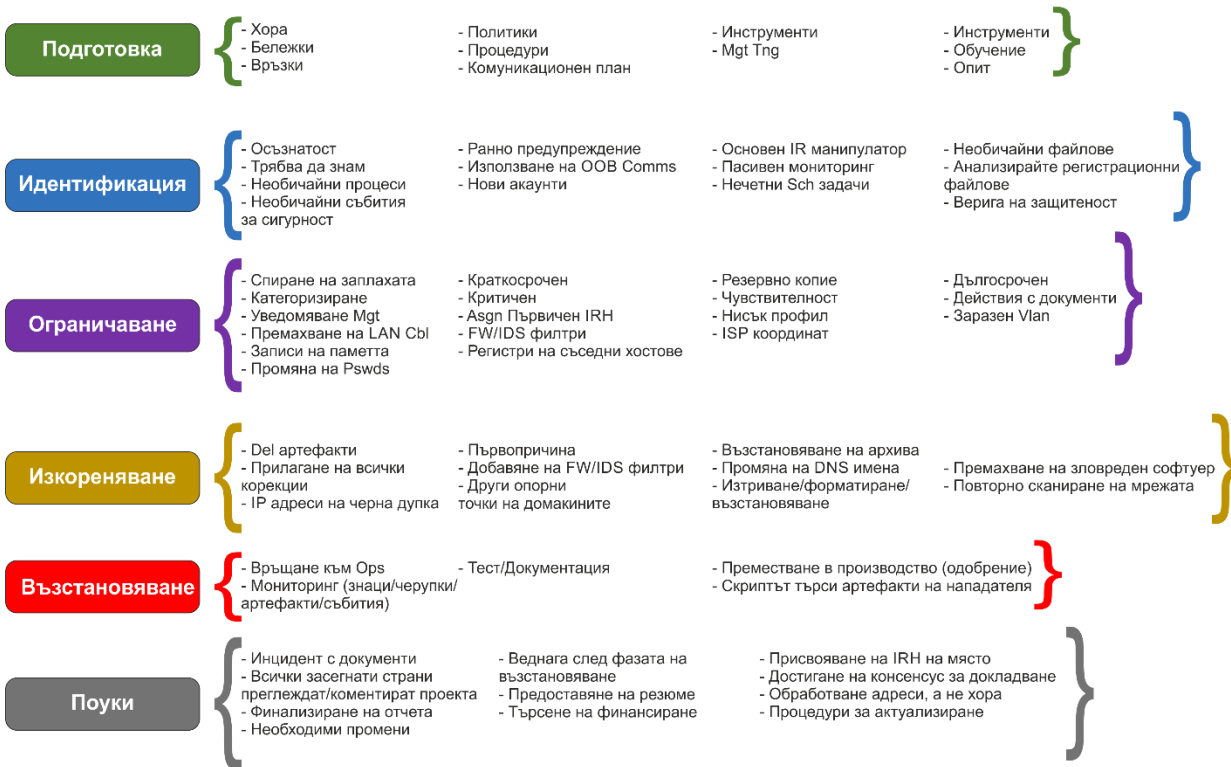
Като част от програмата от най-високо ниво се вземат стратегически решения за сигурността от типа на:

- 1) Стратегическо планиране.
- 2) Разработване и прилагане на политика за информационна сигурност.
- 3) Оценка на риска и управление на риска.
- 4) Координация на дейности в областта на информационната сигурност.
- 5) Контрол на дейностите в областта на информационната сигурност.

Основната цел или концепция на програмата от по-ниско ниво е да осигури надеждна и рентабилна защита на информационни подсистеми, специфични услуги или групи от услуги. На това ниво се вземат решения по следните въпроси: какви механизми, средства и методи за защита да се използват, закупуват се и се монтират технически средства, извършва се ежедневно администриране, мониторинг на системата за

информационна сигурност като цяло и проследяване и състояние на слаби места, извършва се първоначално обучение на персонала и др.

Подготовка - Идентификация - Ограничаване - Изкореняване - Възстановяване - Научени уроци (PICERL)

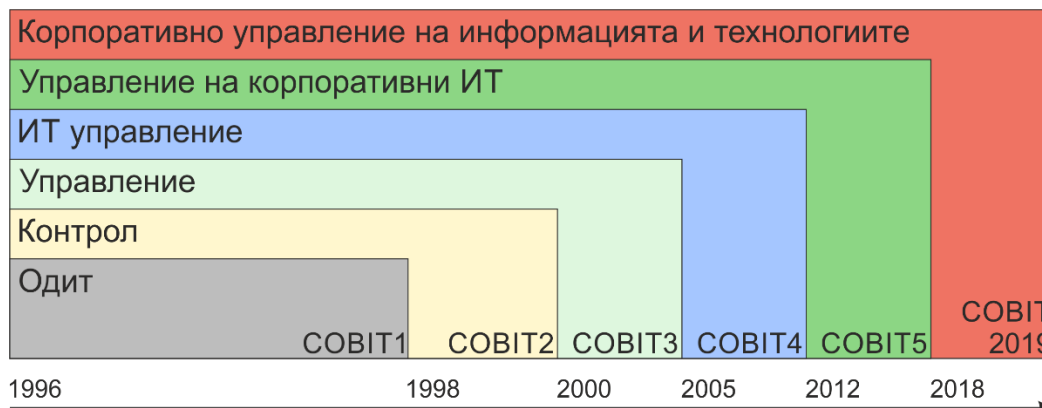


Фигура 45
Процес на реагиране при инциденти
Източник: авторова интерпретация

3.1.1. Технология за подобряване на системите за информационна сигурност

COBIT, или в превод Контролни цели за информационни и свързани технологии, представлява домейн на определени правила, регулиращи информационните технологии. Всички институции функционират с адекватни информационни системи. Акцентът е върху надеждността и функционирането на такива системи. За да се повиши нивото на успех, трябва да се подобри информационната система. Методологичната рамка на COBIT е един от начините за подобряването и усъвършенстването на ИС. Както подсказва името му, той

има за цел да развива, изследва, публикува и популяризира всичко, което влияе върху качеството, както и това, което администраторът иска да контролира.



Фигура 46
Времевата проекция на развитието на работната рамка на COBIT
Източник: Sikman et al. (2023)²²¹

В зависимост от контекста на приложението на ИС 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.

²²¹ 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.

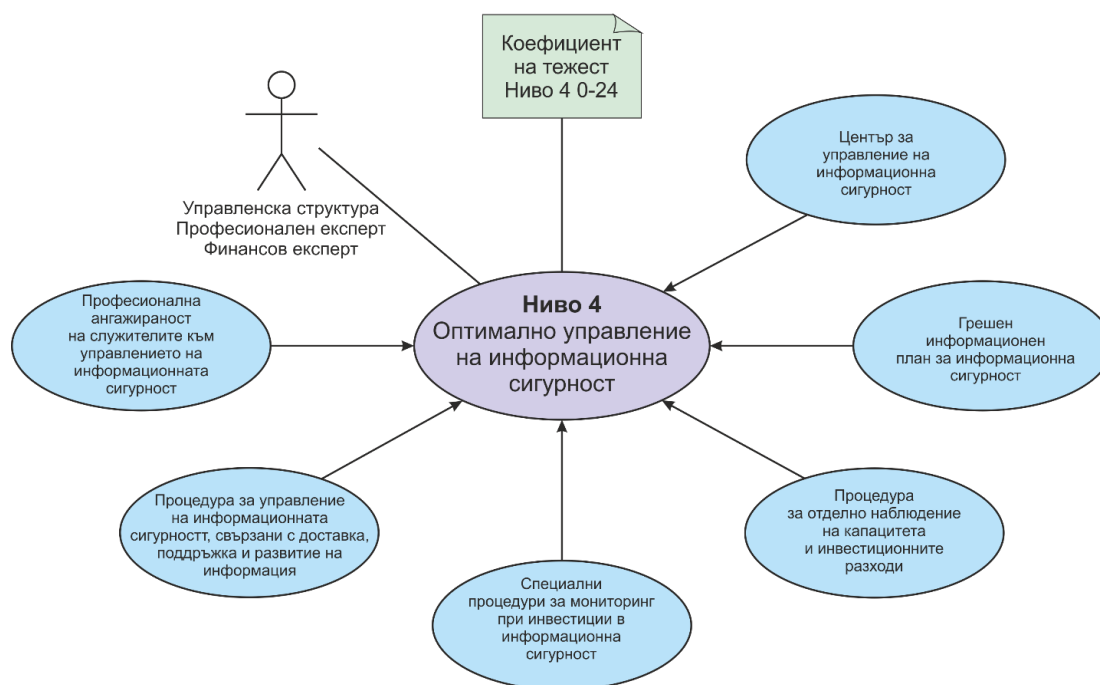


Фигура 47
Нива на развитие на технологията COBIT
Източник: Sikman et al. (2023)

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. Идеята за развитието е възможност да се оценят части от устойчивост, развитие и функциониране на отделни елементи на стопански субект (в конкретния случай – процеси, свързани с функционирането на ИС) и ги представя на цифрова и графична скала в университетите. Следователно, напредъка на дадена организация може да бъде показан с помощта на няколко основни части (нива на развитие), които формират количествено представяне на прогреса от първоначално до оптимално състояние. Концептуално развитие, както и функциониране на управлението на безопасността на информацията може да бъде разширено до концепцията за модела на управление на информационната сигурност. В тази връзка е необходимо да се определят основните елементи за създаване на механизъм за измерване, който да разграничава различните състояния на организация на ИС, работата на институцията или друга наблюдавана област.

1. **Ниво:** Нивото на пряко управление от мениджъра
2. **Ниво:** Ниво на управление, определено от процеси
3. **Ниво:** Различни измерими аспекти на управлението на информационната сигурност
4. **Ниво:** Оптимизирано управление на информационната сигурност
5. **Ниво:** Стратегическо управление на информационната сигурност

При създаване модел за управление на информационната сигурност във висшето образование, цялата система на елементите са първоначално зададени 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.



Фигура 48
Диаграма на оптимално управление на процесите на ИС
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.



Фигура 49
Съкратена версия на Модела
Източник: авторова интерпретация

3.1.2. Необходими инвестиции за подобряване на информационната сигурност

Изброяват се необходимите инвестиции, които са нужни за подобряване на ИС в сектора на висшето образование.

1. Инвестиране в хора – от решаващо значение, защото, както се казва, *„една верига е толкова силна, колкото е силна най-слабата ѝ брънка“*²²². Това важи и за киберсигурността, и като цяло – за ИС. Човешките уязвимости, независимо от технологичния напредък, често създават проблеми в сигурността. Независимо дали става въпрос за фишинг имейли или случайно изпращане на данни до грешния човек, хората несъзнателно въвеждат уязвимости в сигурността на организацията. Инвестицията в хората посредством необходимите знания и умения за вземане на информирани и сигурни решения спомага за подобрието на цялостната система. Служителите имат жизненоважна роля при откриването и докладването на подозрителни дейности, осуетяването на опити за социално инженерство и предотвратяването на пробиви в сигурността.

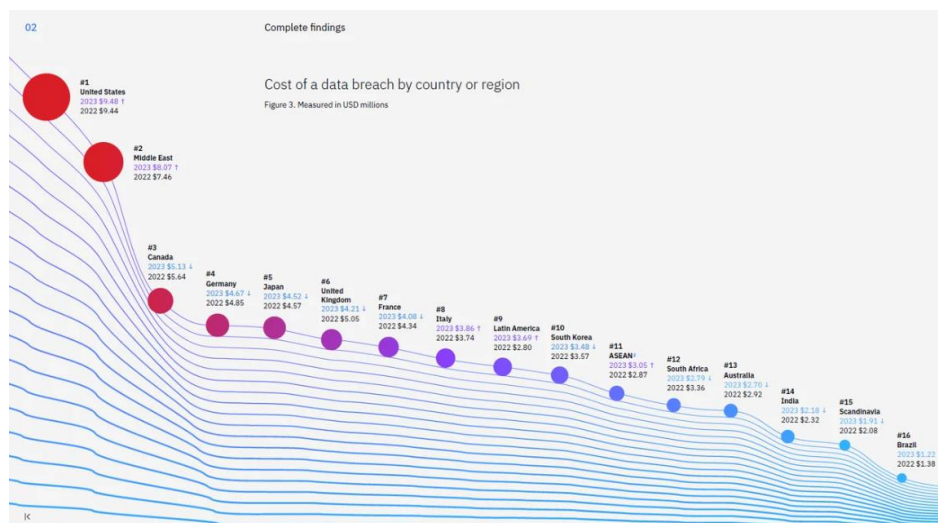
Тази инвестиция в хората може да приеме няколко форми:

- ⇒ обучение и образование по киберсигурност – когато екипът е добре информиран за най-новите заплахи, той може да забележи подозрителни дейности, намалявайки риска да станете жертва на кибератаки;
- ⇒ наемане на експерти по киберсигурност – пред лицето на сложни киберзаплахи, наличието на квалифицирани професионалисти, е жизненоважно. Те проактивно идентифицират уязвимостите, налагат мерки за сигурност и реагират ефективно на нарушения;
- ⇒ създаване на култура, съобразена със сигурността – култивирането на осведомеността относно киберсигурността в организацията, насърчава спазването на протоколите за сигурност и бързото докладване на подозрителни дейности, минимизирайки риска от вътрешни заплахи и пробиви на данни.

²²² Reid, Th. (1785). [*Essays on the Intellectual Powers of Man*](#). University Park, Pa.: Cambridge University Press.

2. Инвестиране в процеси – ефективните процеси за киберсигурност са в основата на сигурна бизнес среда, позволявайки на организациите проактивно да идентифицират и адресират уязвимостите, като по този начин намаляват риска от пробиви на данни и други инциденти. Извеждат се няколко основни процеса, които трябва да се имат предвид:

- ⇒ политики за контрол на достъпа, като многофакторно удостоверяване – изисква от потребителите да предоставят множество форми на потвърждение (напр. парола + SMS код или пръстов отпечатък), преди да получат достъп;
- ⇒ планове за реакция при инцидент – наличието на добре дефиниран план за реакция при инцидент е от съществено значение за минимизиране на щетите в случай на нарушение. Инвестирането в процеси, които очертават ясни стъпки, които да се следват по време на киберинцидент, може значително да намали времето за реакция и финансовите загуби. Според Cost of a Data breach 2023 на IBM, организациите с високи нива на IR планиране и тестване са спестили 1,49 милиона долара²²³ в сравнение с тези с ниски нива и са идентифицирали нарушенията с 54 дни по-бързо;



Фигура 50
Доклад на IBM за нарушаване на данните за 2023 г.
Източник: IBM доклад

²²³ IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs. Available on: <https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs>.

- ⇒ управление на пароли и рутинни промени на пароли – слабите или компрометирани пароли са обичайна входна точка за киберпрестъпниците. Внедряването на силен процес за управление на пароли, гарантира, че служителите създават и поддържат сигурни пароли;
- ⇒ редовно преглеждане на настройките на акаунта – редовните актуализации ограничават повърхността на атаката, повишавайки сигурността. Премахването на ненужните разрешения, деактивирането на неактивните акаунти и уверяването, че всеки акаунт има достъп само до това, което се изисква за неговата роля. Това помага за предотвратяване на вътрешни заплахи и ограничава повърхността за атака.

Изследване на Harvard Business Review²²⁴ показва, че стреса на служителите често води до незлонамерени нарушения на правилата, които са много по-чести от злонамерените такива. Всяка компания, независимо от размера си, трябва да даде приоритет на разработването и внедряването на стабилни процеси за киберсигурност, които работят с потребителите, вместо да ги претоварват.

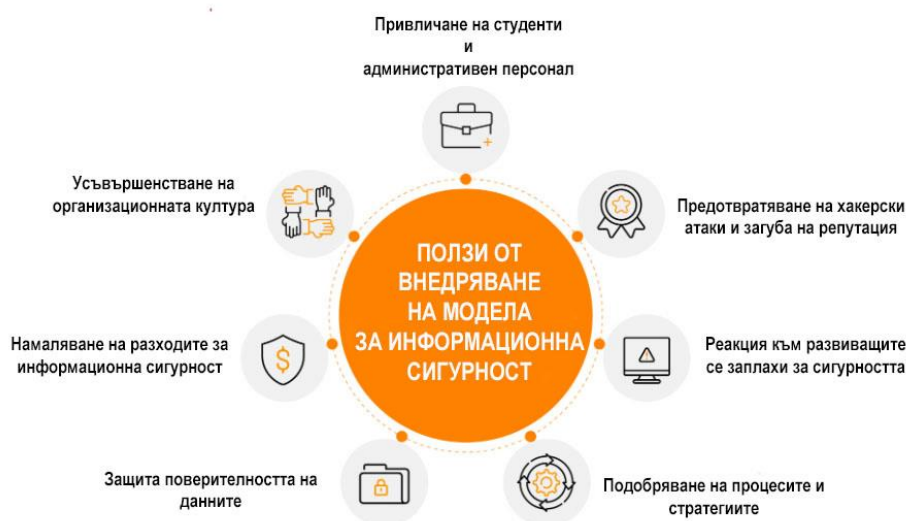
3. Инвестиране в софтуер – качественият софтуер действа като непроницаема бариера срещу киберзаплахи, работейки в tandem с админите. Инвестирането в софтуер е решаваща стъпка за укрепване на защитите за киберсигурност. Използвайки силата на технологиите, организациите могат ефективно да защитят активите си. Това включва използването на усъвършенствани инструменти като защитни стени, системи за откриване на проникване, антивирусен софтуер и технологии за криптиране на имейли за защита на мрежи и данни.

²²⁴ Posey, C., Shoss, M. (2022). Research: Why Employees Violate Cybersecurity Policies. Available on: <https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies>.

3.1.3. Очаквани ползи от внедряване на модела за подобряване на информационната сигурност във висшето образование

Ползите от внедряване на модел за подобряване на ИС 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.“²²⁵.



Фигура 51
Ползи от внедряване на модела
Източник: авторова интерпретация

Моделът на непрекъснато подобрене, който е в основата на стандартите на системата за управление на ISO, означава, че оценката и третирането на рисковете, както и другите процеси, които гарантират, че се провеждат ефективно, се извършват на повтаряща

²²⁵ 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.

се основа, така че с промяната на заплахите и уязвимостите, планът за третиране на риска се актуализира редовно, в резултат на което контролите остават подходящи за целта. ISO 27001 предоставя рамка на организациите за контрол и влияние върху начина, по който се управляват рисковете за ИС и как контролите се прилагат, управляват и подобряват. Има също така много репутационни, финансови, стратегически и вътрешни ползи от внедряването, като повишено доверие и възприятие на клиентите, по-големи бизнес възможности, тръжни предимства и подобрена осведоменост за сигурността във „включване“ на всички нива на организацията.

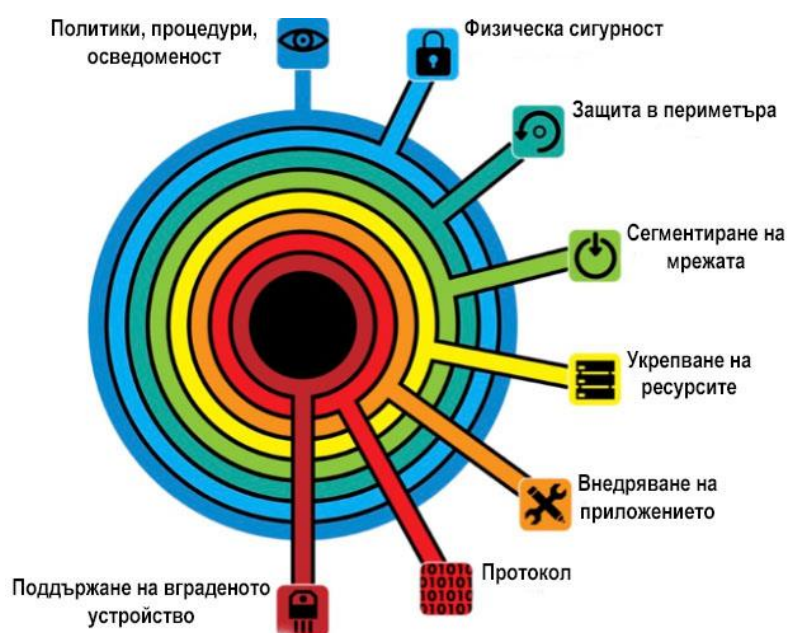
От друга страна, законите, разпоредбите и наредбите за ИС и поверителност са въведени, за да защитят гражданите. Регулаторните изисквания са от полза за организацията по следните начини:

1. Показват съответствие със законите и разпоредбите за информационна сигурност – наличието на програма за обучение за информираност относно ИС предоставя доказателство, че организацията спазва закона. Този тип обучение обикновено се изисква от всички служители, но може да има персонализирани курсове за ръководители.
2. Поддържа законите и разпоредбите за поверителност – вътрешните курсове могат да предоставят персонализирано обучение за информираност за поверителността в подкрепа на правителствените разпоредби. Примери за информация, която изисква защита, включват информация, позволяваща идентифициране на личността и защитена здравна информация²²⁶. Този тип обучение може не само да образова служителите, които пряко работят с информацията, но и тези, които са изложени на нея. Една от тревогите на всяка организация са вътрешните заплахи. За да се повиши нивото на осведоменост, обучението ще включва отрицателни резултати за организацията (напр. глоби за всяко нарушение) и личните последици от злоупотребата (напр. загуба на работа).
3. Защищава данните на служителите – ако не са въведени програми за сигурност и поверителност, ничия информация няма да е в безопасност. Ако данните са

²²⁶ Wlosinski, L. (2017). Key Ingredients to Information Privacy Planning. // ISACA Journal. 4.

достъпни за престъпници, те биха могли да намерят начини да вземат пари, да поемат самоличността на жертвата, да изнудват.

4. Защитава чувствителните данни на организацията – системата за осведоменост относно ИС може да включва инструкции за боравене с класифицирана, секретна, частна и чувствителна информация²²⁷. Специални инструкции за боравене с данни могат да бъдат включени в обучението за справяне с етикетването на медиите, съхранението на информация и други защитни мерки.



Фигура 52
Системата за осведоменост на ИС
Източник: авторова интерпретация

Програмата за информираност на организацията може да научи служителите как да подобрят сигурността и поверителността в личния си живот. Информираността относно сигурността може да има положителен ефект както върху тях, така и върху техните семейства, приятели, съседи и домове. Осъзнаването, че съществуват уязвимости в безжични преносими компютърни устройства, домашни мрежи и мобилни компютърни

²²⁷ Wlosinski, L. (2018). Data Loss Prevention—Next Steps. // ISACA Journal. 1.

устройства (напр. смартфон, лаптоп, компютърни таблети), предоставя на хората база, от която да прилагат защитни контроли. Някои предимства включват:

- 1) Юридически – съществува съзнание, че хората могат да бъдат държани лично отговорни за неправилно боравене с лични и чувствителни данни по време на работа. Санкциите варират според организацията.
- 2) Етични – хората могат да бъдат научени за последиците (напр. глоби, затвор) на пиратския софтуер.
- 3) Статут на заетост – неспазването на правилата за сигурност може да доведе до порицание и/или наказание на служителите, дори уволнение. Отговорност на всеки е да защити организацията и данните, които тя придобива.
- 4) Наставничество – като научат за изискванията на организацията за спазване на нормативните изисквания (и закона), служителите могат да станат по-спазващи закона и да бъдат наставници на другите. Информацията, която може да бъде споделена с други, включва как да се избегнат имейли и фишинг измами, трикове, използвани от киберпрестъпници, практики за лична безопасност, превантивни и реактивни действия, които да се предприемат при киберспешна ситуация и др.
- 5) Достъп до системата – програмата за информиране може да спомогне потребителите да научат правилата за достъп до системата и насоки, свързани със силата на паролата, дължината, състава (т.е. комбинация от знаци), броя на разрешените опити, продължителността на влизане и т.н. Контролите за достъп не се отнасят само за устройствата, които се използват, но и към мрежови устройства. Обучението за достъп, получено на работното място, е с цел да се предотврати проникване в личната информация.
- 6) Компютърни слабости – курс за информираност може да научи потребителите за уязвимостите в личните мобилни изчислителни устройства и настолните компютри и необходимостта от софтуерни корекции и надстройки.
- 7) Социални медии – софтуерните приложения за социални медии (напр. Facebook, Twitter, Skype, LinkedIn, блогове) могат да изложат потребителите на различни злонамерени заплахи, като кражба на самоличност, кибертормоз и други.

Предимствата на модела за ИС са изцяло заложени в поверителността и сигурността на информацията, с която се бори на работното място, а също така:

- 1) Установява политика и програма на организацията – най-добрата практика е една организация да има програма за осведоменост относно сигурността на информационните технологии. Информираността учи персонала на стратегията за информационна сигурност на ръководството, целите и задачите, подкрепя и насърчава ангажимента на ръководството да защитава организацията.
- 2) Създава сигурна среда – организационният ангажимент насърчава добрите практики за сигурност на информацията на работното място (напр. правилно изхвърляне на приложения за кредитни карти, данни на пациенти). Сигурната среда не само защитава организацията, в която работи дадено лице, и нейните чувствителни данни, но учи колко е важно да се отказва достъп до информацията на организацията на неоторизиран персонал.
- 3) Установява обща поза за сигурност – включва:
 - определяне на политиките за информационна сигурност и поверителност на организацията, които полагат основата за съответствие с нормативните изисквания;
 - осигуряване на отправна точка за текущото подобряване на програмата и практиките за информираност, тъй като заплахите продължават да се развиват и престъпниците се адаптират към контрамерките;
 - обучение на нови служители, неинформирани за заплахи за сигурността и поверителността, рискове и опасения.
- 4) Осигурява информация за точка за контакт – наличието на информация за контакт в програмата за обучение е важно, така че хората да знаят как да реагират в ситуация на спешно реагиране. Точките за контакт трябва да включват:
 - Екип за реагиране при инциденти, който отговаря за реакцията и обработката на инциденти в областта на информационната сигурност;

- Главен служител по информационна сигурност, който отговаря за корпоративните политики и процедури, както и персонала, който го поддържа;
 - Служител по поверителността, който отговаря за политиката за поверителност, процедурите, процесите, стандартите и реакцията при инциденти, свързани с поверителността.
- 5) Сигурност на сградата, тъй като ще информира служителите за защитни мерки и процедури, свързани със сградата, хората и работната среда
 - 6) Идентифицира типове чувствителни данни – в някои организации има нива и видове чувствителност на данните. Класифицираните, поверителни, интелектуални и частни данни изискват по-високо ниво на бдителност и по-силен защитен контрол. Данните, свързани с поверителността, изискват по-бързо отчитане и могат да означават разликата между падането или оцеляването на една организация в този конкурентен свят.
 - 7) Практики за предотвратяване на кражба на самоличност – ако организацията борава с номерата на социалното осигуряване, адресите, датите на раждане или медицинската информация на хората, то носи много важната отговорност да защитава тези данни.
 - 8) Защитава репутацията на организацията – информираността подсилва усилията и процедурите на организацията за защита на данните.

Поверителността на информацията е „един от петте стълба на информационното осигуряване“²²⁸, посредством които информацията бива запазена, а при различни случаи – засекретена.

²²⁸ Тагарев, Н. (2021). Цит. съч., с. 15.

ИЗВОДИ ОТ ТРЕТА ГЛАВА

Въз основа на проведеното проучване сред 56 участници, работещи в сферата на висшето образование, и по-конкретно – във висши учебни заведения, се извеждат в обобщен вид основните изводи, които могат да послужат и за препоръки относно повишаване нивото на информационна сигурност:

1. По-големият процентен дял на регистрираните участници в анкетното проучване са служители с трудов стаж от 5 до 10 години и над 10 години, което прави 80.4% сумарно. Това показва професионализма, опитността, вживяването в работния процес. Годишните опит са определящи за вникването в същността на процесите в дадена организация.

2. По-голямата част от респондентите са преподавателски състав - на щат или хоноруван, което е основание да се твърди, че благодарение на функционалността на преподавателите, могат да бъдат предотвратени проблеми, свързани с информационната сигурност, тъй като те работят както с масив от данни, с мейли, социални мрежи, база от информационни ресурси, така и със студенти.

3. Най-висок процент участие са взели преподавателския и административен персонал на УНСС, гр. София (28.6%). Многообразието на участници от различни университети в България спомага за получаването на обективно мнение по въпроси, свързани с информационната сигурност.

4. Респондентите отговарят, че са спокойни за своята информационна сигурност и за сигурността в организацията, в която работят, като 62.5% отговарят с „Да, може да се каже“, а 32.1% утвърдително с „Да, напълно съм спокоен/спокойна“. Това води до заключението, че системите за информационна сигурност са достатъчно ефективни, за да се справят с предизвикателствата на съвремието и да спомогнат за усещането за спокойствие и сигурност на работещите във висшите учебни заведения.

5. 57.1% от респондентите отговарят, че човешка грешка е в основата на пропускливостта на ИС, което твърдение има своята теоретична и емпирична обусловеност, доказана в дисертационния труд. Останалата част считат, че това се дължи на слабости на самата система за сигурност (30.4%) и на все по-умели хакери (10.7%).

6. 10.7% от анкетираните считат, че се наблюдават спорадични срывове на информационната система по време на упражняване на работни дейности на служителите, но като цяло, 66.1% са на мнение, че 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. Отбелязва се, че 19.6% никога не са попадали в такава ситуация.

7. 53.6% от респондентите отговарят, че най-предпочитаното средство за тях е запитването по e-mail, като най-подходящ канал за получаване на информация в контекста на изпълнение на работните им задължения. Това е показателно за дигитализирането на обществото, от една страна, а от друга - за стремежа към по-екосъобразен и природосъобразен начин на извършване на професионални ангажменти.

8. 85.7% от запитаните са на мнение, че знанията и компетентностите на обслужващия и административен персонал са на достатъчно високо ниво спрямо предприемане на адекватни действия за предотвратяване на рискови ситуации, свързани с информационната сигурност. 8.9% изразяват диаметрално противоположна позиция, като считат, че не са изобщо на високо ниво и не могат да се справят с подобни ситуации.

9. Пейоративен е изводът, който се прави на въпрос, свързан с посещаване на курсове, семинари за квалификация относно възникване на рискови ситуации, свързани с информационната сигурност в работна среда, като 89.3% признават, че през последната година не са посещавали такива мероприятия, което резонира върху цялостната архитектура на ИС. Подготвеният персонал е адекватен в предприемане на мерки за стопиране или предотвратяване на зловредни атаки. Липсата на инициативност и на инвестиции в този целесъобразен контекст води единствено до пукнатини в системата за информационна сигурност.

10. 92.9% от запитаните отговарят единодушно, че ще уведомят свой колега, който пряко отговаря за информационното обслужване при възникване на инцидент, свързан с информационната сигурност.

11. 94.7% от служителите са на единодушно мнение, че системата за информационна сигурност е ефективна.

12. 85,7% от респондентите са на мнение, че личните им данни са защитени добре в институцията, в която работят, което създава усещане за сигурност сред мнозинството от служителите.

13. 87,5% от респондентите са на мнение, че се чувстват защитени от атаки, извършвани в интернет пространството и нарушаващи личните данни и права на потребителите.

14. В свободният отговор се извежда общото твърдение, че работещите във висше учебно заведение считат системата за информационна сигурност за надеждна и качествена.

В трета глава на дисертацията се предлага концептуален модел за подобряване на информационната сигурност във висшето образование. Целта на проучването е да помогне на ръководителите на сектора за ИС към висшите учебни заведения при вземането на решения за мерки за сигурност срещу заплахи за ИТ средата с цел намаляване на вероятността от компрометиране на чувствителна информация. Разработването на ефективен модел за подобряване на информационната сигурност във висшето образование, следва да се основава на кумулативни данни и информация, а дейността по оценката на неговата функционалност, трябва да включва действия и закономерности.

Изграденият модел се основава на следните критерии: Риск мениджмънт, Имплементиране на ИС, Киберпространство, Архитектура на ИС.

В последващ етап трябва да се идентифицира цялата чувствителна информация в определена област на риск за сигурността, независимо дали е класифицирана или не; информация, която може да застраши интересите на организацията, когато бъде компрометирана, както и всички активи – оборудване, приложения, съоръжения, процедури – критични към нормалното функциониране на организацията.

Модел на информационна сигурност, който ще служи за комплексно управление на кризи в случай на атака от киберпространството има четири основни вертикални оси: Хора и идентичност, Данни и информация, Сигурност на приложението, Инфраструктура.

Архитектурата се използва за справяне с безопасността на настоящите компютърни системи, която е основно физическа или логическа компютърна подмрежа, разделена със специализирани защитни стени от интернет и защитена инфраструктура на организацията.

Архитектурата за облачна сигурност е критичен компонент поради нарастващата зависимост от облачните изчисления за съхранение и обработка на данни. Тя включва: мрежова сигурност, защита на крайни точки, сигурност на данните, сигурност на приложенията, съответствие с нормативната уредба, разузнаване на заплахи. ИС е обработка или комуникация, която подобрява надеждността и валидността на системите за обработка на данни чрез защита на потока от информация. Това включва: удостоверяване, контрол на достъпа, поверителност на данните, интегритет на данните и достъпност.

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

Извеждат се 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: несъществуващи процеси, неорганизиран процеси, повтарящи се процеси, дефинирано ниво на процеса, ниво на управляван процес и оптимално ниво. Технологиите 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. Идеята за развитието е възможност да се оценят части от устойчивост, развитие и функциониране на отделни елементи на стопански субект (в конкретния случай – процеси, свързани с функционирането на ИС) и ги представя на цифрова и графична скала в университетите. Следователно напредъкът на дадена организация може да бъде показан с помощта на няколко основни части (нива на развитие), които формират количествено представяне на прогреса от първоначално до оптимално състояние.

Инвестирането в хора, процеси и софтуер, е най-сигурния вариант за разработването и внедряването на модел за информационна сигурност.

Очакваните ползи от внедряването му са от изключително естество за опазване сигурността на институцията: привличане на студенти и административен персонал, предотвратяване на хакерски атаки и загуба на репутация, реакция към развиващите се заплахи за сигурността, подобряване на процесите и стратегиите, защита поверителността

на данните, намаляване на разходите за ИС, усъвършенстване на организационната култура.

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.

Анкетното проучване и създаденият Модел имат своята корелационна зависимост, тъй като спрямо човешките измерения на необходимостите и произлизащите от тях сигурност и защита е важно да се отчете мнението на работещите в университетите, за да се представи практико-приложен модел, който да улесни работата им по отношение на информационната сигурност.

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 умозаклучения, 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.

Извежда се твърдението, че съгласно Общия регламент за защита на личните данни (GDPR) правата и неприкосновеността на личните данни стоят на първо място, като в повечето държави правото на защита на личните данни е заложено в конституцията.

Представен е моделът Знание – Отношение – Поведение. Въз основа на модела се прави заключението, че когато знанията на служителите за безопасното поведение на информационната сигурност на работното място се увеличават, тяхното отношение се подобрява, което води до подобро поведение на информационната сигурност. Тоест, в основата на информационния колапс на сигурността на първо място стои човешката грешка и за да бъде сведена до минимум, знанието, отношението и поведението са триадата на човешкия ресурс в неговата ефективност и целесъобразност.

Информацията като ключов актив на организацията изисква повишаване нивата на сигурност, тъй като е изложена на предизвикателствата на съвременното дигитализирано общество.

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 киберзаstraшеност. 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.

Необходимите инвестиции за подобряване на информационната сигурност на първо място включват човека – неговата способност, знания, квалификация и опит. На следващо е инвестицията в процеси и на последно ниво – в софтуер.

Очакваните ползи от внедряване на модела за подобряване на информационната сигурност във висшето образование са укрепване на организацията срещу киберзаплахи чрез установяване на контроли, които минимизират риска от атака, както и спазване на всички регулаторни изисквания, свързани със сигурността на информацията.

Информацията – валутата на новото време, нейното опазване и ефективно съхраняване са приоритет за създаване на атмосфера на национална сигурност.

ПРИЛОЖЕНИЕ

АНКЕТА ЗА ИЗСЛЕДВАНЕ МНЕНИЕТО НА РАБОТЕЩИ ВЪВ ВИСШЕТО ОБРАЗОВАНИЕ ОТНОСНО СИГУРНОСТТА НА ИНФОРМАЦИЯТА ВЪВ ВИСШЕТО ОБРАЗОВАНИЕ

Уважаеми дами и господа,

Моля да попълните тази анкета, която има за цел да проследи мненията и нагласите Ви относно сигурността на информацията в сферата на висшето образование в България. Проучването е напълно анонимно и резултатите ще се използват единствено за целите на дисертационния труд.

Благодаря Ви!

1. Вие сте:

- Мъж
- Жена

2. От колко години работите в сферата на висшето образование?

- под 1 година
- от 1 до 5 години
- от 5 до 10 години
- над 10 години

3. Какъв е Вашият професионален статут?

- хоноруван преподавател
- преподавател на щат
- административни дейности
- управленски функции
- научно-изследователски дейности
- друго

4. Вашата възраст е:

- между 18 и 34 години
- между 35 и 54 години

- между 55 и 64 години
- над 65 години
- предпочитам да не отговарям

5. Вашата месторабота е /моля да посочите университет и град/

.....

6. Спокоен/Спокойна ли сте за информационната си сигурност и за сигурността във Вашата организация?

- Да, напълно съм спокоен/спокойна
- Да, може да се каже
- Не, изобщо не съм спокоен/спокойна
- По-скоро не съм спокоен/спокойна
- Не мога да преценя

7. Според Вас на какво предимно се дължат различните пробиви и проблеми с информационната сигурност?

- на човешка грешка
- на слабости в системата
- на все по-добри хакери
- на различни и разноречиви указания към административния персонал
- не мога да преценя

8. Колко често Ви се е случвало да има срыв в информационната система, докато упражнявате своите работни дейности?

- много често (веднъж седмично)
- често (един-два пъти месечно)
- не много често (веднъж на няколко месеца)
- не се е случвало скоро (веднъж годишно)
- никога

9. По кой канал най-често получавате информация, за да може да извършвате ежедневните си работни задължения?

- телефон
- запитване по e-mail
- запитване по различни социални интернет канали

- интернет страницата на висшето учебно заведение
- писмено запитване на хартиен носител

10. 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?

- Да, на много високо ниво
- Да, може да се каже
- Не, изобщо не са на високо ниво
- Не, не мога да кажа
- Колебая се

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

- Да
- Не

12. При възникване на инцидент, свързан с информационната сигурност, Вие първо ще:

- уведомите Ваш колега, отговарящ за информационното обслужване
- уведомите Държавната агенция за национална сигурност
- уведомите дирекцията за киберпрестъпност към ГДБОП
- запазете спокойствие и ще опитате да се справите сам/сама

13. Според Вас системата за информационна сигурност във висшето учебно заведение, в което работите, ефективна ли е?

- Да
- По-скоро да
- Не
- По-скоро не
- Не мога да преценя

14. Според Вас личните Ви данни защитени ли са добре в институцията, в която работите?

- Да, напълно
- Да, може да се каже
- Не, изобщо
- По-скоро не
- Не мога да преценя

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

- Да, напълно
- Да, може да се каже
- Не, изобщо
- По-скоро не
- Не мога да преценя

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

.....

НАУЧНИ ПРИНОСИ

Дисертационният труд извежда следните научни и научно-приложими приноси 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 умозаклучения, 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.

Научноприложни приноси:

1. Предложен е оригинален концептуален модел за подобряване на информационната сигурност във висшето образование.
2. Анализите се провеждат по авторски подход с избрани 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.

НАУЧНИ ПУБЛИКАЦИИ ПО ТЕМАТА

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

БИБЛИОГРАФИЯ

1. Арънсън, Е. (2009). Човекът – „социално животно“. София: Дамян Яков
2. Бошняку, А. (2023). Особенности на бизнес средата в контекста на Индустрия 4.0. // Диалог. 1
3. Георгиев, К., Георгиева, П. (2015). Предизвикателства пред иновационната парадигма за осигуряване на интелигентен, устойчив и приобщаващ растеж. // Устойчиво развитие
4. Димитров, Д. (2012). Приложение на сценарийното планиране в бизнеса, отбраната и сигурността. София: УНСС
5. Димитров, Д. (2015). Икономически анализ „разходи – ползи“ в отбраната и сигурността. София: УИ „Стопанство“
6. Димитров, Р. (2018). Насоки за оптимизиране счетоводното отчитане на паричните средства по сметки на бюджетни организации в банките. // Бизнес управление. 1
7. Димов, П., Здравков, З., Добрева, Х. (2021). Информационна сигурност. София: ВА „Георги Раковски“
8. Евгениев, Е. (2019). Бъдещето на труда и индустриалните отношения. // Труд и социална справедливост. Фондация „Фридрих Еберт“
9. 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.
10. Желев, С. (2008). Маркетингови изследвания: Методология и организация. София: УИ „Стопанство“
11. Желев, С. (2012). Маркетингови изследвания. // Маркетинг. София: ИК УНСС
12. Закон за висшето образование. Достъпно на: <https://lex.bg/laws/ldoc/2133647361>
13. Закон за защита на класифицираната информация. Достъпно на: <https://lex.bg/bg/laws/ldoc/2135448577>
14. Закон за защита на личните данни. Достъпно на: <https://cpdp.bg/>
15. Закон за киберсигурност. Достъпно на: <https://lex.bg/bg/laws/ldoc/2137188253>
16. Закон за управление и функциониране на системата за защита на националната сигурност. Достъпно на: <https://lex.bg/bg/laws/ldoc/2136588572>

17. 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/StrategicDocuments/View.aspx?lang=bg-BG&Id=655>
18. Комисия „Публична комуникация“. (2014). Анкета за проучване на общественото мнение за дейността на ВСС и съдебната власт сред ключовите общности според комуникационната политика на ВСС. Анализ на резултатите, Достъпно на: <http://www.vss.justice.bg/root/f/upload/8/analiz-anketa-vss-2014.pdf>
19. Концепция за цифрова трансформация на българската индустрия (Индустрия 4.0). Достъпно на: <https://www.mi.government.bg/files/useruploads/files/ip/Industry4.0.pdf>
20. Матеев, М. (2000). Анализ и оценка на риска при избор на инвестиционни решения. София: Стопанство
21. Младенов, М. (2018). Административните санкции на основания от GDPR. // Вътрешен одитор. 2
22. 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_.p
23. Наредба за общите изисквания за оперативна съвместимост и информационна сигурност. Достъпно на: <https://www.netlaw.bg/p/n/o/noiosis.rtf-677-91.pdf>
24. Наредба за сигурността на комуникационните и информационните системи. Достъпно на: https://www.dksi.bg/media/1619/naredba_za_sigurnostta_na_komunikacionnite_i_informacionnite_sistemi.pdf
25. Наредбата за минималните изисквания за мрежова и информационна сигурност. Достъпно на: https://www.mtc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf
26. Насоки 01/2021 относно примерни случаи, свързани с уведомяването за нарушение на сигурността на личните данни. Достъпно на: https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_bg.pdf
27. Национална рамка за оценка на възможностите. Достъпно на: <https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-bg.pdf>
28. Националната програма за развитие „България 2030“. Достъпно на: <https://www.minfin.bg/bg/1394>
29. Националната стратегия за киберсигурност „Киберустойчива България 2020“. Достъпно на: <https://www.strategy.bg/StrategicDocuments/View.aspx?Id=1120>
30. Общ регламент за защита на данните. Достъпно на: <https://gdprinfo.eu/bg>

31. Овчарова, Ж. (2019). Внедряване на индустрия 4.0 в малките и средни предприятия: минимизиране на рисковете и определяне на възможностите. // Индустрия 4.0. Предизвикателства и последици за икономическото и социалното развитие на България. София: ФФЕ
32. 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
33. Павлов, Г. (2010). Защита на информацията. София: УИ „Стопанство“
34. Павлов, Г. (2012). Информация и сигурност. София: Авангард Прима
35. Павлов, Г., Пудин, К. (2011). Информационна сигурност в организацията. София: УИ „Стопанство“
36. Павлов, Пл. (2022). Информационна сигурност. Стандарти от серията ISO 27000 – перспективи и проблеми. Велико Търново
37. Павлова, Е. (2023). Референтен модел за киберсигурност при проектирането на онлайн услуги във висши учебни заведения в България. Автореферат. София: УНСС
38. 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
39. Програма „Цифрова Европа“. Достъпно на: <https://digital-strategy.ec.europa.eu/bg/activities/digital-programme>
40. 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
41. Радев, К. (2018). Четвъртата индустриална революция – предизвикателства пред предприемачеството и управлението на бизнеса. // Научни трудове. 4. УНСС
42. РБ. Икономически и социален съвет. (2019). Предизвикателства пред труда в контекста на цифровизацията на икономиката. Достъпно на: <https://esc.bg/wp-content/uploads/2021/01/opinion-esc-3-060-2019-bg-1.pdf>
43. Регламент 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година. Достъпно на: <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016R0679>

44. Световна банка. (2019). Променящата се природа на работата. Доклад за световното развитие 2019. Washington, DC 2
45. Семерджиев, Ц. (2007). Управление на информационната сигурност. София: Софттрейд
46. Стефанов, Г. (2008). Теория на международната сигурност. София: Сиела
47. Стоицов, Г. (2020). Информационна и комуникационна сигурност. ПУ „Паисий Хилендарски“
48. 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
49. Тагарев, Н. (2021). Съвременни подходи при управлението на киберсигурността. Ч. 1. София: Авангард Прима
50. Тагарев, Н. и др. (2021). Добра срещу лоша метрика // Тагарев, Н. и др. Икономически аспекти на модели за оценка на киберсигурност в умни градове. София: ИК – УНСС
51. Тагарев, Н. и др. (2021). Модел на метрика чрез „Пет показателя за сигурност, които трябва да се вземат предвид“ // Тагарев, Н. и др. Икономически аспекти на модели за оценка на киберсигурност в умни градове. София: ИК – УНСС
52. Тагарев, Н. и др. (2021). Модел на умните градове и проблеми с киберсигурността. // Тагарев, Н. и др. Икономически аспекти на модели за оценка на киберсигурност в умни градове. София: ИК – УНСС
53. Танев, Я., Митев, М. (2024). Предизвикателства пред приложение на новата европейска политика за киберсигурност в българската администрация. София: Институт по публична администрация
54. Туджаров, Х. (2009). Въведение в информационната сигурност. Достъпно на: <https://www.tuj.asenevtsi.com/>: <https://www.tuj.asenevtsi.com/Sec2009/Sec01.htm>
55. Цветков, Цв. (2016). Съвременен инструментариум за оценяване на сигурността. // Икономически и социални алтернативи. 2
56. Цветкова, М. Внимателна употреба на понятието „информация“. // Медии и обществени комуникации. Достъпно на: <https://media-journal.info/?p=item&aid=155>
57. Цифрова трансформация на България за периода 2024-2030 г. Достъпно на: <https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1661>
58. AlGhamdi, S., Win, K., Vlahu-Gjorgievska, E. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. // Government Information Quarterly. 39(4)

59. Al-Rawas, A., Millmore, S. (2002). Information Security Risks on a University Campus. // Sultan Qaboos University Journal for Science. 7(1)
60. 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
61. Anderson, D., Abiodun, O., Christoels, A. (2020). Information security at South African universities – implications for biomedical research. // Int. Data Priv. Law. 10(2)
62. Arachchilage, N. et al. (2014). Security awareness of computer users: a phishing threat avoidance perspective. // Comput Human Behav. 38
63. Bandara, I., Balakrishna, C., Ioras, F. (2021). The Need for Cyber Threat Intelligence for Distance Learning Providers and Online Learning Systems. // 15th International Technology, Education and Development Conference
64. Bryson, J. (2016). Managing information services: an innovative approach. Farnham, Surrey, UK: Ashgate
65. Bulgurcu, B. et al. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. // MIS Quart. 34(3)
66. Burgin, M. (2003). The Essence of information: paradoxes, contradictions, and solutions. // tripleC. 1(1)
67. Cavallo, B. et al (2019). Comparing inconsistency of pairwise comparison matrices depending on entries. // Journal of the Operational Research Society. 70(5), pp. 842–850
68. Chandarman, R., Van Niekerk, B. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. // Afr. J. Inf. Commun. AJIC. 20
69. Cohney, S., Teixeira, R., Kohlbrenner, A. et al. (2020). Virtual Classrooms and Real Harms: Remote Learning at U.S. Universities. Cornell University
70. Da Veiga, A. et al. (2017). Defining and identifying dominant information security cultures and subcultures. // Computers & Security. 70
71. Dai, N., András, K., Zoltán, R. (2016). E-learning security risks and counter measures. // Engineering Research and Solutions in ICT. 1(1)
72. De Bona, G. et al. (2019). Classifying Inconsistency Measures Using Graphs. // Journal of Artificial Intelligence Research. 66
73. Edgar, T., Manz, D. (2017). Research Methods for Cyber Security. Elsevier Inc
74. 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/>
75. EU Cyber defence Policy framework. Available on: <https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf>

76. EU International Cyberspace Policy. (2014). European Union External Action. Available on: http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm
77. European Union Agency for Network and Information Security (ENISA). (2010). The new users' guide: how to raise information security awareness (EN). Available on: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide
78. Eze, T., Aroh, C. (2020). Management of Information Security in Public Universities in Nigeria. // *Int. J. Digit. Soc.* 11(1)
79. Force, J. (2020). Security and Privacy Controls for Information Systems and Organizations. U.S. Department of Commerce: National Institute of Standards and Technology
80. Furnell, S. et al. (2012) Power to the people? The evolving recognition of human aspects of security. // *Comput Secur.* 31(8)
81. Gang, L. (2007). An inquiry into the origin of the philosophy of information. Beijing: JinCheng Press
82. 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>
83. Ghazvini, A., Shukur, Z., Hood, Z. (2018). Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education. // *Int. J. Adv. Comput. Sci. Appl.* 9(8)
84. Guide on Managing and Notifying Data Breaches under the PDPA. (2021). Available on: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-on-Managing-and-Notifying-Data-Breaches-under-the-PDPA-15-Mar-2021.pdf>
85. Guide to Developing a National Cybersecurity Strategy. Available on: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf
86. Gordon, T., Prakken, H., Walton, D. (2007). The Carneades model of argument and burden of proof. // *Artificial Intelligence.* 171(10-15)
87. Gronroos, C. (1984). A service quality model and its marketing implications. // *European Journal of Marketing.* 18(4)
88. Haimes, Y. (1998) Risk Modeling, Assessment, and Management. Ediția 1. New York: Wiley
89. Haney, J., Lutters, W. (2020). Security Awareness Training for the Workforce: Moving Beyond “Check-the-Box” Compliance. // *Computer.* 53(10)
90. Hancock, J. (2022). Psychology of Human Error. Understand the Mistakes that compromise your Company's Cybersecurity. Tessian. Available on: <https://f.hubspotusercontent20.net/hubfs/1670277/%5BCollateral%5D%20Tessian-Research-Reports/%5BTessian%20Research%20Report%20-%20Psychology%20of%20Human%20Error.pdf>

91. Henno, J. (2014). Information and Information Security. // Proceedings of the 3rd Workshop on Software Quality, Analysis, Monitoring, Improvement, and Applications (SQAMIA)
92. Hermann, M., Pentek, T. Otto, B. (2015). Design Principles for Industrie 4.0 Scenarios: A Literature Review. // Working Paper. 01
93. 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)
94. IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs. Available on: <https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring->
95. IBM Security Services 2014 Cyber Security Intelligence Index. Available on: https://www.editoraroncarati.com.br/v2/phocadownload/ibm_security.PDF
96. International Organization for Standardization. (2005). ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management
97. ISO/IEC 27001: 2013. (2016). Информационни технологии. Методи за сигурност. Системи за управление сигурността на информацията. Изисквания. Техническа справка. 2
98. 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>
99. ISO/IEC 27005: 2011 Information technology — Security techniques — Information security risk management. Available on: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en>
100. Jang-Jaccard J., Nepal, S. (2014). A survey of emerging threats in cybersecurity. In: Journal of Computer and System. // Sciences, Aug. 80(5)
101. Joshi, C., Singh, U. (2017). Information Security Risks Management Framework – A Step Towards Mitigating Security Risks in University Network. // J. Inf. Secur. Appl. 35
102. Karlsson, F., Åström, J., Karlsson, M. (2015). Information security culture—state-of-the-art review between 2000 and 2013. // Information & Computer Security. 23(3)
103. Kissel, R. (Ed.). (2019). NIST Interagency or Internal Report (NISTIR). Glossary of Key Information Security Terms. 7298(2). Washington: U.S. Department of Commerce
104. Klein, J., Rice, C. (2014). US education reform and national security. Council on Foreign Relations

105. Kruger, H. et al. (2006) A prototype for assessing information security awareness. // Comput Secur. 25(4)
106. Krztoń, W. (2021). (In)security of the functioning of the information society in the Cyberspace. // Przegląd Europejski. 3
107. Kwecka, R. (2016). Information in the Area of Security. New Paradigms. // Journal of Defense Resources Management. 7(2)
108. Ladhari, R. (2008). Alternative measures of service quality: a review. // Measuring Service Quality. 18(1)
109. 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/>
110. 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
111. 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)
112. Makupi, D. (2019). A Design of Information Security Maturity Model for Universities Based on ISO 27001. // Int. J. Bus. Manag. 7(6)
113. Martimiano, L., Moreira, E. (2005). An OWL-based Security Incident Ontology. // Proceedings of the Eighth International Protege Conference
114. Number of sent and received e-mails per day worldwide from 2017 to 2026 (in billions). Available on: <https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/>
115. Orikpe, E. (2013). Education and national security: Challenges and the way forward. // Journal of Educational and Social Research. 10(3)
116. Oxford English Dictionary. Available on: <https://www.oed.com/search/dictionary/?scope=Entries&q=information>
117. Parsons, K. et al. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). // Comput Secur. 42
118. Parsons, K., Calic, D., Pattinson, M. et al. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. // Computers & Security. 66
119. 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)

120. Pavlov, G., Poudin, K. (2019). Challenges to information security at regional level. // Trends in Regional Development and Security Management. Sofia: UNWE Publishing Complex
121. Posey, C., Shoss, M. (2022). Research: Why Employees Violate Cybersecurity Policies. Available on: <https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies>
122. Posey, C., Roberts, T., Lowry, P. (2016). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. // Journal of Management Information Systems. 32(4)
123. Poudin, K. (2018). Developing and Maintaining business Security Culture. // Yearbook of UNWE. 1. Sofia: UNWE
124. PWC. Shaping our future. Global Annual Review 2015. Available on: <https://www.pwc.com/gx/en/about-pwc/global-annual-review-2015/campaign-site/pwc-global-annual-review-2015.pdf>
125. Qiao, T. (2011). Definition and Essence of Information. // triple. 9(2)
126. Sammons, J., Cross, M. (2015). The Basics of Cyber Safety. Elsevier Inc
127. Sidorkin, A., Iroshnikov, D. (2019). Theoretical issues of "security" concept. // Journal of Politics and Law. 3(12)
128. Sikman, L. et al. (2023). A model of sustainable information security management system in higher education institutions. // Journal of Physics: Conference Series. 2540
129. Silic, M., Back, A. (2014). Information security: Critical review and future directions for research. // Information Management & Computer Security
130. Singh, V., Margam, M. (2018). Information Security Measures of Libraries of Central Universities of Delhi : A Study. // DESIDOC J. Libr. Inf. Technol. 38(2)
131. Smith, S., Spafford, E. (2004). Grand challenges in information security: Process and output. // IEEE Security & Privacy, 2(1)
132. Tsvetkov, V. (2014). Worldview Model as the Result of Education. // World Applied Sciences Journal. 31(2)
133. Unger, R. The Knowledge Economy. Available on: <https://www.oecd.org/naec/THE-KNOWLEDGE-ECONOMY.pdf>
134. Vogel-Heuser, B., Hess, D. (2016). Guest editorial: Industry 4.0–prerequisites and visions. // IEEE Trans Autom Sci Eng. 13
135. Wang, J., Guo, M. (2009). Security Data Mining in an Ontology for Vulnerability Management. // Proceedings of the International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing

136. What are Industry 4.0, the Fourth Industrial Revolution, and 4IR? Available on: <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir>
137. Whitten, A. (1999). Information resources management. Ediția 1. Londra: Ideea
138. Wilson, T. (1993). Trends and Issues in Information Science – a General Survey. // Media, Knowledge and Power. Groom Helm, London/Sydney
139. Wlosinski, L. (2017). Key Ingredients to Information Privacy Planning. // ISACA Journal. 4
140. Wlosinski, L. (2018). Data Loss Prevention—Next Steps. // ISACA Journal. 1
141. Wu, K. (1981). The status and role of information in philosophy. // Potential Sci. J. 3
142. Wu, K. (2012). The Essence, Classification and Quality of the Different Grades of Information. // Information. 3(3)
143. Xu, X., Lu, Y. et al. (2021). Industry 4.0 and Industry 5.0—Inception, conception and perception. // Journal of Manufacturing Systems. 61
144. Xu, Y. (2013). Research on Computer Network Security Architecture of Universities in China. // Adv. Mater. Res. 765–767
145. Zhong, R., Xu, X., Klotz, E., Newman, S. (2017). Intelligent manufacturing in the context of Industry 4.0: a review. // Engineering. 3(5)