ПЛОВДИВСКИ УНИВЕРСИТЕТ
„ПАИСИЙ ХИЛЕНДАРСКИ“

ФИСН
ФАКУЛТЕТ ПО ИКОНОМИЧЕСКИ И СОЦИАЛНИ НАУКИ

kamegpa
ПННС

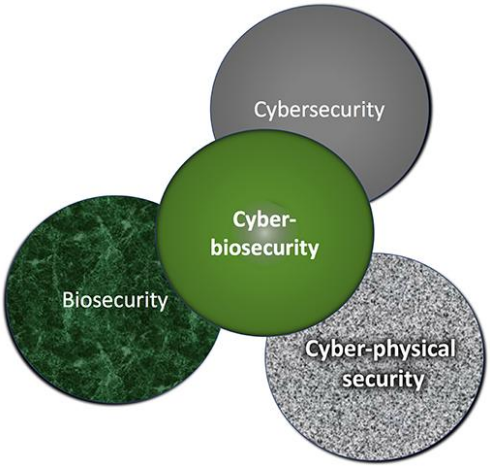
КОСТАДИН РАНГЕЛОВ БАКОВ

КИБЕРБИОСИГУРНОСТТА КАТО ЕЛЕМЕНТ ОТ СИСТЕМАТА ЗА НАЦИОНАЛНА СИГУРНОСТ

АВТОРЕФЕРАТ

за придобиване на образователна и научна степен „Доктор“

Област на висше образование: 9. Сигурност и отбрана, Професионално направление: 9.1. Национална сигурност, докторска програма Национална сигурност



Научни ръководители: проф. д-р Илия Илиев, доц. д-р Иван Станчев

Пловдив, 2025

Дисертационният труд е обсъден на заседание на катедра „Политически науки и национална сигурност“ при ФИСН на ПУ “Паисий Хилендарски“, проведено на 27.06.2025 г., на което е взето решение да бъде насочен за публична защита.

Дисертационният труд е в обем 221 страници и съдържа Увод, шест глави, Заключение и Използвана литература. Включени са 69 таблици и 63 фигури. Библиографията включва 35 бр. източници на кирилица и 160 бр. латиница.

По темата на дисертационния труд са представени три авторски публикации на английски език.

Материалите във връзка с предстоящата публична защита са достъпни в отдел „Развитие на академичния състав и докторантури“ на ПУ „Паисий Хилендарски“, както и в Централна университетска библиотека.

Публичната защита на дисертационния труд е насрочена за 19.09.2025 г. от 11.00 ч. в ПУ „Паисий Хилендарски“, гр. Пловдив, ул. „Цар Асен“ 24, зала „Компас“, на заседание на Научно жури в състав:

1. **проф. д.н. Николай Маринов Николов** – ПУ „Паисий Хилендарски“,
2. **доц. д-р Нина Димитрова Димчева** – ПУ „Паисий Хилендарски“,
3. **проф. д. н. Илин Александров Савов** – Тракийски университет, гр. Стара Загора
4. **проф. д-р Георги Василев Камарашев** – Великотърновски университет, гр. Велико Търново
5. **доц. д.н. Петър Господинов Маринов** – Военна академия „Г. С. Раковски“, гр. София

Автор: Костадин Рангелов Баков

Заглавие: Кибербиосигурността като елемент от системата за национална сигурност

СЪДЪРЖАНИЕ

ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

ГМО – Генетично модифицирани организми

ДНК – дезоксирибонуклеинова киселина

ЕИП – Европейско икономическо пространство

ЕК – Европейска комисия

ЕС – Европейски съюз

ЖМО – живи модифицирани организми

ИКТ – информационни и комуникационни технологии

ИТ – Информационни технологии

КБР – Конвенция за биологично разнообразие

КБТО – Конвенция за биологичните и токсични оръжия

КЗХО – Конвенцията за забрана на разработването, производството, натрупването и употребата на химическо оръжие и за неговото унищожаване

КТ – Квантова точка

МКРЗ – Международната конвенция за растителна защита

НС – Национална сигурност

ОЗХО – Организация на забрана на химическото оръжие

ООН – Организация на обединените нации

РКИ – рандомизирани контролирани изпитвания

РНК – рибонуклеинови киселини

САЩ – Съединени американски щати

СОКСРС – Система за оценка и контрол на стратегическите ресурси за сигурност

СССР – Съюз на съветските социалистически републики

ССФМ – Споразумение на Световната търговска организация за прилагането на санитарни и фитосанитарни мерки

СТО – Световна търговска организация

ФБР – Федерално бюро за разследване

ХИВ – синдром на придобития имунен отговор

ЦРК – Циркулиращи ракови клетки

AAAS – Американска асоциация за напредък на науката

AI – Изкуствен интелект

AHL – ацил-хомосеринови лактони

ASSURED – достъпен, чувствителен, специфичен, удобен за потребителя, здрав и бърз, без оборудване, доставящ се

BCG – ваксина БЦЖ

УВОД

Кибербиосигурността е нововъзникваща област в пресечната точка на киберсигурността и биосигурността. Целта на кибербиосигурността е описана като насочена към „потенциала или действителното злонамерено унищожаване, злоупотреба или използване на ценна информация, процеси и материали в интерфейса на науките за живота и цифровите светове“. Кибербиосигурността е част от система от мерки, които колективно имат за цел опазване на биоикономиката.

Редица публикации от последните десет години подчертават сложността на начинанието, което наричаме „кибербиосигурност“ и опасенията относно сигурността, стабилността и устойчивостта. Те включват сигурността на личните геномни данни, когато чуждестранни компании, които са закупили всички или част от американски компании или са сключили договор за услуги за геномни или здравни данни и предоставят достъп до чувствителна лична информация; продължаващата уязвимост на електронните здравни досиета и системите за здравеопазване, налагащи контрол върху секвенирането на ДНК чрез ДНК-кодиран зловреден софтуер; уязвимостта на веригата за доставки на материали от синтетичната биология, кибер компрометирането на голямата промишлена биофармация и проучванията на високо ниво, които систематично изследват програмите и възможностите за биозащита на САЩ.

Най-ярка демонстрация от въвеждане на система от правила за кибербиосигурност е пандемията на Коронавирус-19. Актуалността на темата за биосигурността и кибербиосигурността е породена от една страна от еволюцията на развитието на тероризма и междудържавни конфликти показваща тенденция към нарастване на терористични атаки с използване на биологично оръжие, а от друга значителните научни постижения през последните 30 години на молекулярната биология и молекулярните биотехнологии, които доведоха до възможността за почти безпрепятствено използване на молекулярно-биологичните техники и методи в рутинни лаборатории. Допълнително съществуват все още нерешени проблеми свързани с рискове от инфекциозни заболявания, пренасяни умишлено през границата в условията на миграционен натиск и осъществяването на доктрината за свободно придвижване на хора и стоки по целия свят.

Органите, отговорни за националната сигурност, трябва да имат готовност да отговорят адекватно на динамичните промени на международната обстановка.

Едно от основните направления за съсредоточаване на академичните усилия следва да е задачата да се разработят стратегии, принципи, правила, алгоритми и методологии, които да положат основите на концепция за кибербиосигурността на територията на България, като член на ЕС.

Към настоящия момент на национално ниво отсъстват доктрина, концепция и програми за кибербиосигурност. По предложената тема на дисертационния труд не са известни научни публикации и разработки от други български автори, разглеждащи детайлно аспектите на кибербиосигурност в условията на споделяне на чувствителни бази от данни.

На основание посочените обстоятелства можем да формулираме научноизследователският проблем, който решава настоящият труд: В системата за НС липсва елемент, отговорен за биосигурността и кибербиосигурността. Също така, липсва структура, функционално отговорна за защита на биосигурността и кибербиосигурността, както и концепция за нейното осигуряване.

Обект на изследване е *кибербиосигурността като елемент на системата за национална сигурност.*

Предмет на изследване са *правни и техническите аспекти на кибербиосигурността, като съчетание на познания и умения в три различни области – национална сигурност, информационните технологии и молекулярните биотехнологии, които трябва да се съгласуват с охранителните и оперативно-издирвателните аспекти.*

***Цел** на настоящия дисертационен труд е **да се създаде концепция за защита на кибербиосигурността в Република България**.*

*За постигането на поставената цел, в процеса на изследване се определят за решаване следните **научноизследователски задачи:***

1. Да се анализират съвременното състояние на кибербиосигурността и нейното място в системата на националната сигурност.

2. Да се изследват биологичните оръжия и извърши тяхната класификация през призмата на научните постижения в областта на молекулярните биотехнологии.

3. Да се идентифицират опасностите и заплахите и да се определи степента на риска при кибербиоатаки).

4. Да се систематизират получените резултати и да се предложи модел на концепция за кибербиосигурност.

5. Да се определят насоките за развитие и усъвършенстване на дейността за противодействие на кибербиоатаки.

6. Да се анализира ефективността при прилагане на бързи методи за диагностика на заболявания като рисков фактор за биосигурността.

Изследователска хипотеза:

На базата на констатираното отсъствие на концепция, доктрина и програми за кибербиосигурност в България, както и предвид нарастващата взаимосвързаност на информационните системи с биомедицинските и биотехнологични данни, се формулира хипотезата, че разработването и внедряването на интегриран модел за кибербиосигурност, обхващащ правни, технически и организационни аспекти, значително ще повиши устойчивостта на националната сигурност на Република България срещу кибербиоатаки и ще минимизира рисковете, произтичащи от споделянето на чувствителни бази данни в контекста на членството в Европейския съюз (ЕС). Този модел следва да включва стратегия за противодействие на биологични оръжия, систематизиране на заплахите и рисковете, както и насоки за развитие и усъвършенстване на дейностите по превенция и реагиране при кибербиоатаки.

Теоретико-методологическа основа на изследването

За теоретична и методологическа база на изследването са използвани концептуалните основи на *системния подход; теорията на управлението, конфликтологията; теория и практика на създаване на биосензори, теоретични основи на молекулярните биотехнологии.*

В дисертационното изследване са използвани национални, институционални и образователни нормативни документи, енциклопедична и справочна литература, учебно-методически материали.

Методология и методика на изследването

В хода на изследването за решаването на изследователските задачи е използван комплекс от:

– **теоретични методи**: анализ и синтез на общите характеристики на кибербиосигурността, изискваща интердисциплинарен подход на планираните изследвания.

– **емпирични методи**: наблюдение на средата за откриване рисковете при защита и пренос на чувствителни биологични данни, анкета на различни групи от населението за отчитане индивидуалния и обществен риск при пренос и съхранение на чувствителни биологични бази данни, експертна оценка за приложимостта на биосензори и техники за бърза диагностика на потенциални причинители на биологична заплаха на населението.

– **статистически методи**: за обработка, обобщаване и анализ на резултатите ще се използват различни методи за обработка и анализ на чувствителните биологични бази данни.

За по-голяма целенасоченост, конкретност и задълбоченост на разработката се приемат следните **ограничения**:

1. Детайлно се обследват източниците, които изследват определени модели на биосензори и диагностични тестове за откриване на потенциални биологични заплахи.

2. Дейностите на други участници в противодействието като част от системата за национална сигурност не са предмет на настоящото изследване.

3. Времевият обхват на изследването е 2022 г. – 2025 г.

4. Пространствен (териториален) обхват включва на територията на Република България по отношение на анкетните проучвания и международна среда при съпоставка и анализа на данни, проведени в международна среда.

5. Нормативна база е актуална към 01.01.2025г.

Методика на изследването

През **първия (подготвителен) етап на изследването** (2020-2022 г.) се анализира изследваният проблем от гледна точка на техническото и технологичното ниво в двете основни области – информационни технологии и молекулярни биотехнологии (биосензори). Разкриват се ключовите характеристики на двете динамично развиващи се области на науката и техниката в една интердис-

циплинарна област. Определят се обектът и предметът, целите и задачите на изследването, както и да се формулира работната хипотеза.

През **втория (основен) етап** (2023-2024г.) се разработват концептуалните основи на платформа за изграждане на система за кибербиосигурност. Едновременно се внасят корекции в методиката за изследване, формулират се прецизни стратегии за научното изследване на нови биосензори, както и прилагането на комплект от съществуващи апаратура и биосензори за провеждане на биомониторинг.

През **третия (заключителен) етап** (2025г.) се обобщават резултатите, формулират се основните изводи и препоръки, представени в дисертационния труд.

Достоверността и обосноваността на резултатите от дисертационния труд е осигурена: от логиката на изследването и от приложената концептуална и теоретико-методологическа основа.

Значимост на резултатите

Научната новост *на изследването се състои в разкриване на взаимовръзките между биосигурността, киберсигурността и международната среда за сигурност, конструирането на модел за кибербиосигурност като елемент на системата за националната сигурност.*

Теоретичната значимост на изследването се състои в решението на научната задача – *формулиране на концепция за кибербиосигурност.*

Практическата значимост на изследването се състои в предлагане на система от апарати и биосензори, които могат да се използват за провеждане на бърз анализ на агентите на потенциална биотерористична атака.

ГЛАВА ПЪРВА:
НАЦИОНАЛНАТА СИГУРНОСТ И НЕЙНОТО РЕСУРСНО ОБЕЗПЕЧАВАНЕ

1.1. Общи положения

В първа глава се разглежда същността на националната сигурност с акцент на факторите, които оказват влияние върху нейното ниво. Изследва се значението на информационния ресурс и състоянието на екосистемите за защитата на националната сигурност. В модерния свят с развитието на технологичната революция, изкуствения интелект и молекулярните биотехнологии е необходимо да се разгледа концепцията за националната сигурност през призмата на решаване на задачи с интердисциплинарен подход.

Националната сигурност (НС) е приоритет на всяка държава, независимо от нейното устройство, политическа система и икономически статус. За нейното обезпечаване е необходимо да се отделят необходимите ресурси – човешки, финансови, технически, правни. Един от основните въпроси при постигане на максимална ефективност на дейностите по НС е да се намери баланса между възможностите на държавата и оценката от необходимото ниво на защита.

Постигането на баланс между необходимост и наличност на стратегически ресурси в държавата е основна предпоставка за състоянието на националната ѝ сигурност. Намирането на този баланс на практика се осъществява основно чрез бюджета на всяка страна. Тази предпоставка сама по себе си включва субективния фактор, който най-общо може да се определи от взаимодействието на икономическите процеси и политическото управление на страната. Бюджетът на всяка държава е функция на компромисите между нивото на икономиката в държавата и нивото на политическата зрялост на обществото.

Държавата все още е най-важният фактор при осигуряване на НС. Това обстоятелство поражда и факта, че пределегирането на правомощията ѝ относно ресурсното осигуряване и операциите на критичната инфраструктура е несъстоятелно и генерира неоправдани рискове от гледна точка на настоящия момент.

1.2. Информацията като стратегически ресурс и контролът върху нея

В ерата на глобалния свят, който в момента се трансформира информираността е ключов фактор за сигурността на както на държавите, така и на отделния човек.

Според определението на проф. Стоян Денчев (2019): „Информацията, в цялото разнообразие, в което се проявява, е ценен ресурс, също както финансовите, материалните и човешките ресурси. Най-общо казано, концепцията за информационните ресурси може да се изрази по следния

начин: всички налични ресурси на една система и тяхната трансформация в използваема информация. Други автори, детайлизирайки горното определение, дават следната дефиниция: „Информационните ресурси са всички физически и логически компоненти на системата за обработка на информация, като компютри, програми, данни, информация, операционни системи, комуникационни връзки, системи и програмисти, програмни анализатори, оператори и мениджъри“.

В условията на динамичното развитие на света като цяло и в частност развитието на технологиите определението за информационните ресурси трябва да се разглежда и през призмата на AI. Според Христо Чаушев (2024) AI се налага като значителна трансформираща сила в социалните медии, подобряваща създаването на персонализирано съдържание и увеличаваща ангажираността на потребителите.

1.3. Ресурсите в условията на глобалната екологична криза и комплексен риск

Природните ресурси са в основата на функционирането на икономиката като тяхното наличие и начините, по които се усвояват, предопределят качеството на човешкия живот. Суровини, като горивата, минералите и металите, но също и храната, почвата, водата, въздуха, биомасата и екосистемите са ограничени. Голямата опасност, която крие експлоатацията на природни ресурси е свързана с фактори като икономическо развитие, прираст на населението и урбанизация, както и все по-широката експлоатация на екосистемните ресурси.

Екосистемните услуги са интердисциплинарно направление в науката между екология и икономика. Екосистемите се явяват живото-поддържащи системи, които са доставчици на екосистемни услуги и икономически ползи.

Основният извод, който се налага, е, че съществува почти пълно припокриване между частите от планетарната екосистема, притежаващи висок риск от екологична катастрофа, и съвременните региони с най-многобройно население в света.

Всички планетарни ресурси са крайна величина, съизмерима със съществуването на планетата и самата Слънчева система. Самите ресурси нямат никакво значение, ако цивилизацията ни изчезне поради различни причини – просто няма да има кой да потребява ресурси, да превръща материално-веществената и енергийната същност на планетарната среда в подходящи за оцеляване и развитие. Съвременните реалности в отношението на човешкото общество към природоресурсния потенциал показват закостенялост, тежък и необоснован традиционализъм.

1.4. Ключови проблеми на функциониране на Система за оценка и контрол на стратегическите ресурси за сигурност (СОКСРС)

Системата за оценка и контрол на стратегическите ресурси за сигурност обследва националните човешки, икономически, финансови, технологични и информационни ресурси и включва следните основни принципи за оценка:

- Баланс между потребностите на системата за сигурност и възможностите на страната;
- Ефикасност и ефективност;
- Удовлетворяване на необходимите оперативни способности.

Най-ефективното използване на финансовите ресурси е чрез реализиране на дългосрочна концепция и стратегия, а не просто чрез финансиране във всеки отделен проект. С най-голямо въздействие върху сигурността на обществата е финансирането на модернизацията на индустриалната и технологичната база на държавите. Необходима е увереност относно цялостното въздействие на взиманите решения върху реализацията на проектите за разработване и внедряване на високотехнологични решения в перспективните индустрии. Необходимо е и ефективно управление на технологичния риск. Високотехнологичните решения могат да окажат както положително, така и негативно въздействие върху развитието на отделните държави и на света като цяло. Изповядвайки принципа на конкурентоспособност, днес обществата се развиват изпреварващо технологично и с много по-бавни темпове социално въпреки прокламирания принцип на хуманността. Изпреварващото развитие на модерните технологии в дигиталното общество предполага използването им едновременно както за положително развитие на обществото, така и за налагане волята на част от обществото на народите над останалите в ущърб и подчинение на последните. Последните технологични постижения в двете най-бързо развиващи се области – информационните технологии и молекулярните биотехнологии предоставят за първи път в историята на човечеството възможност

да се използват неконтролируемо от различни групи от хора, дори от отделни индивиди. Този факт поставя сигурността на обществото като цяло в изцяло нова ситуация. Ето защо не можем да си позволим да разглеждаме предпоставките за възникване на риск за сигурността на обществото, на отделните държави и на съюзите от държави фрагментирано по сектори и индустрии. Днес все по-наложително е да се прилага интегриран подход при изграждане на системата за оценка и контрол на стратегическите ресурси за сигурност, като в центъра на тази система се поставят киберсигурността, биосигурността и кибербиосигурността като обединяващи цялата дейност на отделните общества чрез въвеждането в употреба на високотехнологични процеси. Те се явяват пресечна точка на проблемите с недостига на суровини и енергия от една страна и екологичните катастрофи, наблюдавани особено в отделни региони.

Изводи от първа глава

Светът днес се променя с висока скорост. Развитието на процеса на глобализация се противопостави на развитието на националната държава особено при очертаващото се противопоставяне на световните хегемони. Последните събития след пандемията от Ковид-19 и конфликта между Русия и Украйна от една страна, а от друга страна технологичния прогрес във всички области на науката, дигитализацията като процес и навлизането на AI показаха ясно, че индивидите и общностите търсят и очакват сигурност, във всичките й измерения, най-вече в рамките на националната държава. Подобна е ситуацията и при протичането на миграционните процеси, промяната на климата и екологичните кризи. Необходимо е да се въведе нова доктрина на националната сигурност, включваща киберсигурността и биосигурността при новите международни отношения.

ГЛАВА ВТОРА:
АКТУАЛНИ ПРАВНИ ВЪПРОСИ ПРИ РЕГУЛИРАНЕ НА ПРОЦЕСИТЕ ЗА ОЦЕНКА И ЗАЩИТА ОТ БИОЛОГИЧНИ ЗАПЛАХИ

2.1. Нормативни актове, касаещи защита от биологични заплахи

В съвременните условия биологичните заплахи могат да се илюстрират като спектър, в който влизат умишлени огнища на болести, възникващи инфекциозни болести, от една страна, и огнища на природни болести, от друга страна.

Дефинирани са общи критерии за различните биологични агенти, включително патогени за тяхното класифициране по степен на опасност, като те са групирани в три категории, посочени подолу.

В категория А се включват средствата с висок приоритет като организми, които представляват риск за националната сигурност на държавите, тъй като те могат лесно да се разпространяват или предават от човек на човек; водят до високи нива на смъртност и имат потенциал за голямо въздействие върху общественото здраве; могат да предизвикат паника в обществото и социални смущения; и изискват специални действия за подготовка за общественото здраве.

Такива агенти/болести са: Антракс (*Bacillus anthracis*); Ботулизъм (*Clostridium botulinum* токсин); Чума (Yersinia pestis); Едра шарка (*Variola vera*); Туларемия (*Francisella tularensis*); Вирусни хеморагични трески, включително Филовируси (Ебола, Марбург) и Аренавируси (Lassa, Machupo).

В категория Б се включват агенти, които са умерено лесни за разпространение; водят до умерени нива на заболеваемост и ниски нива на смъртност и изискват специфични подобрения на диагностичния капацитет на лабораториите и засилено наблюдение на заболяванията.

В категория Б влизат следните агенти/болести: Бруцелоза (видове *Brucella*); Epsilon токсин от *Clostridium perfringens*; Заплахи за безопасността на храните (салмонелози), Мелиоидоза (*Burkholderia pseudomallei*); Пситакоза (*Chlamydia psittaci*); Q треска (*Coxiella burnetii*); Рицинов токсин от *Ricinus communis* (рицинови зърна); Стафилококов ентеротоксин B; Тифусна треска (*Rickettsia prowazekii*); Вирусен енцефалит (алфавируси като източен конски енцефалит, венецуелски конски енцефалит и западен конски енцефалит; Заплахи за безопасността на водата (*Vibrio cholerae, Cryptosporidium parvum*).

В категория С се включват нововъзникващи патогени, които биха могли да бъдат проектирани за масово разпространение в бъдеще поради тяхната наличност; лекота на производство и разпространение; и потенциал за висока заболеваемост и смъртност и голямо въздействие върху здравето. В категория С се включват възникващи инфекциозни заболявания като вирус Nipah и хантавирус.

В природата постоянно се откриват нови инфекциозни агенти, за които все още няма разработени средства за лечение и профилактика.

Специално внимание заслужават и генетично-модифицираните организми (микроорганизми, растения и животни) наричани още „химерни организми“, изкуствено създадени чрез разнообразни генетически манипулации. Научният напредък дори прави възможно синтетичното конструиране на генетичен материал (геном), който да се вгради в приемащи микроорганизми, както и да се постигне възстановяване на изчезнали патогени като например вируса на вариолата, който причинява едра шарка чрез използване на молекулярно-биологични методи за синтезиране на ДНК. От друга страна, постиженията в молекулярната биология могат да се използват и при създаването на изцяло нови патогени, които никога не са съществували в природата, чиито патогенни свойства не са познати на медицинската наука и няма никакъв реален опит при предизвикване на епидемии. Те се наричат още суперпатогени, в които се комбинират характеристики на два или повече патогена.

2.2. Съвременните биологични изследвания и отражението им върху биологичната безопасност на човечеството

В съвременните условия се констатира бърз научен и технологичен прогрес в редица области, което дава своето отражение върху размиването на технологичните бариери за придобиване и използване на биологични оръжия. Развитие бележат технологиите с потенциал за намаляване на глобални катастрофални биологични рискове, например геномно сензориране, извънклетъчна диагностика, синтетична ваксинология. Въпреки че тези технологии не трябва да се разглеждат като панацея, те могат да бъдат критична част от отговора на тежки пандемии и глобални катастрофални биологични рискове.

В същото време известни са и примери за научни изследвания, предприети с потенциал за приложение с двойна употреба. Потенциалният характер на двойната употреба на определени технологии не служи като претекст за ограничаване на научния обмен и трансфера на технологии, особено за развиващите се страни. Важен аспект на въпроса е изграждането на капацитет, включително относно обучението на учени и лабораторни служители по програми за биобезопасност, биосигурност и лабораторна диагностика.

От особено значение за съвременните биоизследвания има практиката на други юридически инструменти и международни организации. Така например опитът от изпълнението на мандата на Научно-консултативния съвет на Организацията на забрана на химическото оръжие (ОЗХО) и Срещата на експертите на СЗО за процеса на прогнозиране на науката и технологиите, включително управление на риска от молекулярно-биологичните изследвания като цяло и тяхното приложение във високотехнологичните индустрии.

Изводи на втора глава: Прегледът на правната рамка показва необходимостта от осъвременяване и синхронизиране на законодателството на Република България през призмата на киберсигурността и биосигурността.

ГЛАВА ТРЕТА: БИОСИГУРНОСТ И ЕТИКАТА НА ОБЩЕСТВЕНОТО ЗДРАВЕ, ПОРОДЕНИ ОТ БИОЛОГИЧНИ ЗАПЛАХИ

3.1. Основни положения

Използването на биологични агенти като оръжие за война или терор има своите корени в древността, започвайки с използването на патогени за убиване на коне, които са били жизненоважни ресурси в епохата на директен бой. В наши дни също има опасения за биотероризъм, като например широко разпространената информация за откриването на изпратени писма, съдържащи *Bacillus anthracis* чрез Пощенската служба на Съединените щати през есента на 2001 г. Като резултат от тази био-атака бяха убити петима от двадесет и двама души, които бяха заразени. Така наречените атаки на „Америтракс“ бяха решаващи за изтласкване вниманието на системата за национална сигурност към заплахата от биологичен тероризъм.

Предхождащи събития преди атаките с антракс също са помогнали за оформяне на мислене и действия в посока биотероризъм. Например през 1984 г. поредица от салатени барове в Далас, щата Орегон на САЩ са заразени със салмонела от последователите на движението Bhagwan Shree Rajneesh (по-късно известно като Osho). Тези окултисти са имали за цел да фалшифицират окръжни

избори, като направят потенциалните избиратели заразно болни, за да не могат да се явят пред урните в деня на изборите. В средата на 1990-те години, следствие атаките с отровния газ зарин в метрото на Токио от култа Аум Шинрикьо са убити дванадесет души и стотици са били ранени. Нападателите също са направили опит да извършат серия от биологични атаки през годините предимно в метростанции, въпреки че нито едно от тези по-ранни усилия не е било успешно.

Притесненията относно организиране на биотеристични атаки се засилват от разширяване на изследванията в областта на науките за живота, които могат да бъдат използвани с „двойна употреба“. При тях полезните научни изследвания имат потенциала да бъдат злонамерено употребени от злонамерени участници с различни користни цели, включително от такива с компетенции за работа с биологични оръжия. За разлика от явните изследвания върху биологичните оръжия, които се провеждат от различни организации (например в миналото съветските програми за биологични оръжия, които работят незабелязано в продължение на десетилетия, за да произвеждат биологични оръжия за някои страни от бившия Съюз на съветските социалистически Републики (СССР), изследванията със стоки с двойна употреба са типични особено за страни с малък финансов ресурс, които не могат да развиват програма за ядрено оръжие). Посочените изследвания с биологични обекти са предназначени и за благородни цели, като например лечение на генетични заболявания и трудно лечими болести.

Реална е възможността биотехнологията като индустрия на бъдещето в XXI век да бъде използвана за производство на биологично оръжие и като алтернатива за решаване на значими проблеми на човечеството от намиране на лекарства срещу нелечимите заболявания през активни компоненти за превенция на заболявания включително и пандемии до получаването на нови материали, които да заместят продуктите, получавани на базата на петрола. Всичко зависи от целите на изследователските програми, от една страна и от научния потенциал на съответните лаборатории. В този контекст ние бихме могли да опишем **биосигурността като политики и действия, предназначени да предотвратяване на развитието или появата на сериозни биологични заплахи или смекчаване на последствията от тях – умишлени биологични оръжия, пандемии, възникващи инфекциозни заболявания или резултатът от авариите, предизвикани от дейността на големи лабораторни комплекси.**

В настоящата глава събраната информация се анализира през призмата на потенциалните приложения на биотехнологиите за био-терористични цели и се фокусира върху отговора на националните държави на умишлени биологични заплахи. Принципите и предизвикателствата, свързани с проучване на потенциалните заплахи при биотехнологичните производства с цел био-тероризъм имат значително припокриване с по-широкия набор от биологични заплахи.

Изводи от трета глава:

Събития като атаките с антракс през 2001 г. и предшестващите инциденти, като заразата със салмонела в САЩ, и атаките с отровен газ в Токио, подчертават, че биотероризмът е нарастваща заплаха, съпроводена от увеличени опасения за последствията от биологичните атаки.

Политиките за биосигурност, проучванията с двойна употреба и развитието на биотехнологиите поставят нови предизвикателства пред националната сигурност и общественото здраве. Класификацията на биологичните заплахи се основава на принципи на свобода, сигурност, справедливост и полезност, които наложиха нови етични норми в отговор на ситуацията. Съществува необходимост от баланс между защитата на общественото здраве и индивидуалните права на гражданите, особено в контекста на биологични атаки и пандемии.

Възможността за злоупотреба с биотехнологиите наложи да се въвеждат нови правила и политики, гарантиращи безопасността на обществото, предотвратяването на биологични заплахи и насърчаването на етични практики в научните изследвания. Заинтересованите страни трябва да работят заедно, за да покрият празнотите в законодателството и да предотвратят евентуални атаки, основаващи се на биологични агенти, съхранявайки приоритетите на сигурността, свободата и справедливостта.

В контекста на предотвратяване, подготовка за и реагиране на биологични заплахи, етичните въпроси, които възникват преди, по време и след криза, са от решаващо значение за обезпечаване на общественото здраве и националната сигурност. Според Директива (ЕС) 2017/541, различни действия, които могат да доведат до сериозни последствия, трябва да бъдат класифицирани като терористични престъпления. Етичните дилеми подчертават необходимостта от балансиране между научната свобода и обществената сигурност.

Подготовката преди криза включва оценка на рисковете, свързани с изследванията на стоки с двойна употреба, които могат да доведат до потенциално разрушителни пандемии. Провеждането на такива изследвания поставя учението пред дилеми относно безопасността и ползите за общественото здраве. Организациите трябва да се стремят да финансират изследвания, които минимизират риска от биологични заплахи.

В случай на биотерористична атака, разпределението на оскъдни ресурси също създава конфликти между принципите на справедливост и ефективност. Необходимо е да се установят ясни приоритети при разпределянето на ресурси, които да вземат предвид както спасяването на животи, така и поддържането на социалната структура на обществото. Въпросите за процедурна честност и обществено участие в процеса на вземане на решения по тези теми са също толкова важни, но и сложни.

Публичната ангажираност при формулиране на стратегии за готовност може да доведе до изграждане на доверие, но в същото време рискува да издаде информация, която би могла да се използва от умишлени противници. Обществото трябва активно да участва в създаването на плановете за превенция и реакция на биологични заплахи, като взима предвид както етичните, така и практическите аспекти на тези процеси.

В условията на биологична заплаха, етичните норми стават ключови за организирането на адекватни мерки за безопасност и обществено здраве. По време на криза е важно отговорите на биотерористични атаки да бъдат основани на принципи на справедливост, прозрачност и бърза комуникация. Развитите държави имат морално задължение да помагат на по-слабите нации, докато задълженията за ограничаване на разпространението на епидемии също играят роля в глобалната безопасност.

Комуникацията при епидемии трябва да бъде прозрачна, за да запази доверието на обществото, а принудителните мерки за обществено здраве трябва да бъдат пропорционални и необходимостта от тях да може да бъде оправдана. Изолацията на заразените е допустима, докато карантината на потенциално изложени лица е рядко оправдана и може да доведе до загуба на доверие. Разработването на нови терапевтични средства трябва да бъде извършвано с внимание към етичните норми, като рандомизираните контролирани изпитвания (РКИ) предизвикват особени дебати в контекста на общественото доверие и безопасността на участниците.

След овладяване на кризата, платформата за възстановяване трябва да гласува за подкрепа на засегнатите общности, като предостави нужните ресурси и реновиране на инфраструктурата. Основните принципи на справедливост и реципрочност трябва да ръководят усилията за възстановяване, което е от полза не само за пострадалите общности, но и за глобалната безопасност.

Етичните стандарти при реакция на биологични заплахи изискват балансирано управление между общественото здраве и сигурността, с ясна правна и регулаторна рамка, която да насочва вземането на решения на всички етапи от подготовката, реакцията и възстановяването.

Етичните въпроси, свързани с биосигурността и биотероризма, изискват внимателно разглеждане и баланс между научната свобода, общественото здраве, ефективността и справедливостта, за да се осигури безопасност и устойчивост на обществото в лицето на биологични заплахи.

ГЛАВА ЧЕТВЪРТА:
КИБЕРБИОСИГУРНОСТ ЗА ЗАЩИТА НА БИОИКОНОМИКАТА

4.1. Общи положения

Биоикономиката и свързаните с нея биотехнологии предлагат нови технологични решения за много от предизвикателствата, свързани със здравето и ресурсите, пред които е изправен светът. Съвременната биотехнология може да увеличи предлагането и екологичната устойчивост на производството на храни, фуражи и влакна, да подобри качеството на водата, да осигури възобновяема енергия, да подобри здравето на животните и хората и да спомогне за поддържането на биологичното разнообразие чрез откриване на инвазивни видове.

Дефиницията на биоикономиката е обект на многобройни академични тълкувания и дефиниции, особено през последните 10 години. Бауер и съавтори през 2018г. предлагат следното тълкование на термина „Биоикономика“ под формата на класифициране на дейности:

1. „Нека фирмите да правят нововъведения със собственото си темпо“: Биоикономиката следва ръководени от бизнеса иновации, особено в аграрната промишленост, осигуряваща растеж и устойчивост;

2. „Енергията е ключов въпрос“: Биоикономиката, водена от предизвикателството на глобалното изменение на климата изисква държавни стимули и технологични инвестиции за заместване на петрола с биопродукти;

3. „На Биоикономиката, като една безкрайна граница“: Просто заместването на ресурсите няма да е достатъчно за управление на глобални проблеми; изискват се нови знания и научноизследователска и развойна дейност, особено в химическа промишленост;

4. „Програма за зелена интервенция“: Биоикономика чрез публични политически интервенции (изследвания, цели, политики, насочени към търсенето на биопродукти, финанси), които да доведат до трансформиране промишлени и икономически структури, тъй като пазарът сам по себе си не може да се справи.

За по-голяма прецизност в използваната терминология можем да цитираме две дефиниции за понятието „Биоикономика“ дадени от международни форуми:

„Биоикономиката включва онези части от икономиката, които използват възобновяеми биологични ресурси от сушата и морето – като култури, гори, риба, животни и микроорганизми – за производство на храна, материали и енергия. Това е съществена алтернатива на опасностите и ограниченията на сегашната ни икономика, базирана на изкопаеми вещества, и може да се счита за следващата вълна в нашето икономическо развитие. Тя предоставя големи възможности за иновации, работни места и растеж и като такава ще помогне за реиндустриализирането на Европа”.

Европейската комисия (ЕК) дават следната трактовка на биоикономиката: „От широка икономическа гледна точка, биоикономиката се отнася до съвкупността от икономически дейности, свързани с изобретяването, разработването, производството и използването на биологични продукти и процеси. Прилагането на биотехнологията към първичното производство, здравеопазването и промишлеността може да доведе до възникваща „биоикономика“, при която биотехнологията допринася за значителен дял от икономическата продукция. Биоикономиката през 2030 г. вероятно ще включва три елемента: напреднали познания за гените и сложните клетъчни процеси, възобновяема биомаса и интегриране на биотехнологични приложения в различните сектори“.

4.2. Въвеждане на термина „кибербиосигурност“

Терминът „кибербиосигурност“ включва информация и научни изследвания от две научни области на киберсигурността и биосигурността и може да се определи като хибридна научна област с широко приложение. Първоначално някои автори дефинират този термин като „разбиране на уязвимостта към нежелано наблюдение, нахлуване и злонамерени и вредни дейности, които могат да възникнат в или на интерфейсите на биологични и медицински науки, кибер-, кибер-физичните и инфраструктурните системи и веригите за доставки, както и разработката и въвеждането на мерки за предотвратяване, защита срещу, смекчаване, разследване и определяне на такива заплахи, които се отнасят до сигурността, конкурентоспособността и устойчивостта“. Те подчертават, че това е първоначална дефиниция, която предстои да се развива.

Казано по-просто, от самото си създаване биосигурността е фокусирана основно върху намаляването на рисковете, свързани със злоупотребата с различни клонове на биологичната наука, която може да причини вреда на хората, животните, растенията и околната среда чрез създаване, производство и умишлено или случайно освобождаване на агенти на инфекциозни болести или техните странични продукти (например токсини). Киберсигурността е отделна област, която е фокусирана основно върху сигурността на системи, базирани на информационни технологии, от персонални компютри и комуникационни устройства до големи инфраструктури и мрежи. Само до последните няколко години припокриването на „кибер-“ и „биосигурността“ не е било осъзнавано. След анализа на данните за развитие на двете области поотделно ние можем да заключим, че двете области трябва да работят съвместно и няма да бъдат ефективни при развитието на съвременните технологии, ако работят поотделно. Допълнителен стимул за комбиниране на киберсигурността и биосигурността е задълбочаващия се интердисциплинарен подход в съвременната наука.

Кибербиосигурността всъщност започна с мисленето за определен набор от проблеми, пред които са изправени съвременните клонове на биологичната наука заедно с останалите природни

науки. Създаването на обединяващо научно направление, изработването на неговата систематика и идентифицирането на пътя на развитие напред се реализират с разширяване на интердисциплинарния подход в научните изследвания и иновациите.

Други публикации от последните години също подчертават сложността на начинанието, което наричаме „кибербиосигурност“ и опасенията относно сигурността, стабилността и устойчивостта. Те включват сигурността на личните геномни данни, когато чуждестранни компании, които са закупили всички или част от американски компании или са сключили договор за услуги за геномни или здравни данни и предоставят достъп до чувствителна лична информация; продължаващата уязвимост на електронните здравни досиета и системите за здравеопазване, налагащи контрол върху секвенирането на ДНК чрез ДНК-кодиран зловреден софтуер; уязвимостта на веригата за доставки на материали от синтетичната биология, киберкомпрометирането на голямата промишлена биофармация и проучванията на високо ниво, които систематично изследват програмите и възможностите за биозащита на САЩ. Тъмната мрежа/Dark Net също може да бъде включена, тъй като взаимодейства с дейности от науките за живота с потенциална двойна употреба, както и има достъп до биофармацевтични изследвания, разработки, интелектуална собственост и продукти и компромати на целостта на критичната наука за живота и здравето и до кибер поддържани технологии и инфраструктури. Поради развитието на биоинформатиката като съществена част от съвременната молекулярна биотехнология, сигурността на синтетичната ДНК също може да бъде включена. Ясно е, че тази бързо разширяваща се интердисциплинарна научна област наистина се нуждае от универсално приета дефиниция, общи задачи и определени граници за най-добра оценка, насочено развитие и въздействие.

4.3. Анализ на системи за кибербиосигурност в биотехнологични производства

С развитието на молекулярните биотехнологии можем да добавим друго измерение към кибербиосигурността и да възприемем подход, който според нас трябва да бъде включен към вече обсъдените по-рано аспекти на кибербиосигурността. Самата биофармацевтична индустрия има собствени значителни акции и инвестиции в изследванията, разработването, производството и продажбата на ваксини, терапевтични и профилактични средства за глобалния пазар. Същевременно експертите все повече признават, че самото биотехнологично производство е потенциално уязвимо към нежелани или незаконни дейности, които могат да доведат до вредни резултати. Те могат да включват кражба на интелектуална собственост, нарушаване на веригата за доставки, манипулиране на разработването на биопроцеси и биопроизводството, кибератаки върху ключови компоненти на информационните технологии и киберфизични интерфейси, повреда на критични данни и манипулиране на системи за сигурност и инфраструктура, от които зависят сигурността и безопасността. При предоставяне на резултати от проведения анализ за потенциална заплаха от срив на биотехнологични производства ползвателите (собствениците и управляващите биотехнологичните производства) не се задоволяват от обобщения или езотерични приближения (неприети от официалната наука) в докладите относно слабите места в сигурността на предприятията за биопроизводство, а поставят изискване за изчерпателен, подробен анализ, който може да се прилага на практика в конкретния случай или конкретните биопроизводства.

При реализирането на задълбочен, всеобхватен анализ на съществуващо биотехнологично предприятие е необходимо да се идентифицират пропуските и уязвимите места в сигурността, да се направят препоръки по отношение на тях и да се поставят основите за предприемане на по-конкретни и всеобхватни мерки, независимо дали съществуват или трябва да бъдат разработени и валидирани. Вече има разработен подход за системен анализ, който е предназначен да оцени състоянието на сигурността в момента, да определи какво би било приемливото състояние на сигурност и да предостави насоки и препоръки за довеждане на предприятието от текущото му състояние в желаното състояние.

Това, което е много важно от направения анализ на проблема за кибербиосигурността, е, че стриктното проучване на всяко биотехнологично предприятие може да доведе до идентифициране и характеризиране на отделни уязвими места, пропуски, недостатъци и възможности, за които могат да бъдат приложени достъпни решения или нови могат да бъдат разработени, тествани и внедрени. Интерес представляват в бъдеще като обект на кибербиосигурността подробните проучвания относно това как геномиката може да бъде компрометирана, тъй като тя е свързана с молекулярни-

те биотехнологии при съвременното биопроизводство. Известни са правдоподобните сценарии при реализиране на кибербиоатаки и какви биха могли да бъдат ефектите.

Нашият анализ на подобна информация показва, че предприятията за биопроизводство могат да се възползват от изчерпателни, мултидисциплинарни анализи за идентифициране на уязвимите места в сигурността, водещи до решения за смекчаване или справяне с тях. Това от своя страна обръща налага перспективата за разработване и валидиране на набор от методи или протоколи, които биха могли да бъдат използвани от персонала на предприятията или външни доставчици на услуги за поддържане на отделни малки предприятия в областта на биотехнологиите до голямата биофармацевтична индустрия. Например реализирането на подобен анализ на фирма за производство на пробиотици или закваски е сравнимо с анализ на кибербиосигурността на фирма – световен лидер за производството на инсулин.

След това могат да бъдат разработени, установени и приети насоки или стандарти, за да се гарантира последователност и качество на извършените анализи, пълномощията на персонала, който го прави, и качеството и ефективността на предприетите мерки. Тъй като биотехнологичното производство изисква високоинтелигентни подходи, то реализирането на био-атаки изисква поне същото ниво на подготовка от страна на противниците, които биха могли да проектират и изпълняват сложни атаки. Има вероятност, обаче сравнително простите методи и практики да вдигнат значително летвата, за да намалят риска. И накрая, комбинирането на анализи от този вид може да се използва като основа за информирани инвестиции в изследвания, разработки, тестове и оценка за решения на най-тревожните настоящи и бъдещи заплахи.

4.4. Перспективи пред кибербиосигурността

Много други раздели на информатиката като наука се явяват критични за живота и биомедицинските технологии в частност. Тези допълнителни приложения естествено се включват в рамките на обучението за постигане на кибербиосигурност. Към тях спадат не само, персонализираната геномика и медицински технологии, 3-D отпечатването на критично важни персонализирани медицински устройства и медицинската лабораторна и хирургична роботика. Нужна е по-обширна система. Кибербиосигурността би могла да бъде разширена, за да включва кибер-биосистеми в селското стопанство и системите за производство, преработка и доставка на храни от фермата до масата, както и в управлението на природните ресурси и околната среда. Следва да се осъществи пряка и организирана ангажираност – общности за биосигурност и кибер-киберсигурност, за отнасящите се сектори на науките за живота. Академичните среди, индустрията, правителството или организациите с нестопанска цел (включително експерти по политика, регулаторни и правни въпроси) необходимо е да започнат да комуникират и да черпят опит едни от други, хармонично да идентифицират и развиват приоритети и възможности и да определят „следващите стъпки“. В момента съществува голяма възможност да се предложи единна структура и общ разбираем език. И накрая, докато се случва дефинирането и създаването на кибербиосигурността, е необходимо да се следват национални или международни стратегии за хармонизиране на нововъзникващата дисциплина и да се насърчи нейната важност, успех и устойчивост.

4.5. Биосензори и потенциално приложение при реализиране на превенции за биосигурност

При осигуряване на киберсигурност на клиничните изследвания с генетичен човешки материал е необходимо да се ползват апаратура и методи за анализ, осигуряващи висока скорост на анализа и надеждност на резултата при „полеви условия“. Едно от възможните решения е използването на биосензори.

Както е дефинирано от Международния съюз по чиста и приложна химия (IUPAC) биосензорът е „самостоятелно интегрирано устройство, което е в състояние да осигури специфично оборудване за количествено или аналитично отчитане на резултатите от реакциите, използвайки биологичен елемент за разпознаване (биохимичен рецептор), който е в директен пространствен контакт с преобразователен елемент”. Като цяло биосензорите са предназначени да превеждат физически, химични или биологични събития в измерими сигнали. В тази връзка, устройството на всеки биосензор се характеризира с няколко съставни части: 1) биомолекули (ензими, протеини, нуклеинови киселини, аптамери, антитела, органели, микроорганизми или клетъчни рецептори), отговорни за селективността спрямо целевия аналит; 2) преобразувател (оптичен, електрохимичен, пиезоелект-

ричен, механичен или термичен), който преобразува събитието на биоразпознаване, пропорционално на концентрацията на целевия аналит, в количествено измерим електрически сигнал, и 3) електронна система, включваща усилвател, процесор и дисплей, които допълнително ще обработват сигнала в удобна за потребителя визуализация.

Успешният биосензор трябва да притежава поне някои от следните полезни характеристики:

1. Ензимът трябва да проявява висока специфичност на ензимната реакция за целите на анализите, да бъде стабилен при нормални условия на съхранение и да показва добра стабилност на резултатите при голям брой тестове (т.е. значително по-голямо от 100).

2. Протичащата ензимна реакцията трябва да може да се осъществява в широк диапазон на физични параметри като разбъркване, pH и температура, което ще осигури независимост и надеждност на провеждания тест и би позволило анализ на проби с минимална предварителна обработка. Ако реакцията включва кофактори или коензими, те също трябва, по възможност, да бъдат съимобилизирани с ензима.

3. Резултатът от проведената реакция трябва да бъде точен, прецизен, възпроизводим и линеен в полезния аналитичен диапазон, без разреждане или концентрация. Той също така трябва да бъде свободен от електрически шум. Трябва да отговаря на следните изисквания:

а/ Линейност: Максималната линейна област на калибровъчната крива на сензора. Линейността на сензора трябва да бъде висока за откриване на високи концентрации на субстрат.

б/ Чувствителност: Стойността на отговора на сензора на единица концентрация на субстрат да покрива широк диапазон и да може да разграничава по-възможност много минимални разлики в концентрацията на субстрата.

в/ Селективност: Максимално ниската степен на повлияване от съпътстващи химикали е необходимо условие за получаване на правилния резултат.

г/ Време за отговор: Необходимото време за получаване на резултат да е максимално кратко.

4. Ако биосензорът ще се използва за инвазивно наблюдение в клинични ситуации, сондата трябва да бъде малка и биосъвместима, без токсични или антигенни ефекти. Ако ще се използва в биореактори, то трябва да бъде стерилизуемо чрез автоклавиране, но в момента ензимите в биосензорите не могат да издържат на такава радикална обработка с висока температура и влажност. При всякакви обстоятелства, биосензорът не трябва да е податлив на запушване или протеолиза.

5. Целият комплект на биосензора трябва да е евтин, малък, портативен и способен да се използва от неспециалисти в конкретната област, за да се осигури масовото му приложение.

6. Трябва да има пазар за биосензора. Ясно е, че развиването на биосензор няма особено значение, ако други фактори (например държавни субсидии, продължаваща заетост на квалифицирани анализатори или лошо възприемане от страна на клиентите) насърчават използването на традиционни методи за анализ и възпрепятстват децентрализацията на лабораторните тестове.

4.5.1. Приложение на биосензори чрез детекция на протеини

Разработването на чувствителни, лесни за използване и евтини биосензори за детекция на протеини е задължително, тъй като откриването на протеини е от огромен интерес за приложения за диагностични цели в различни области. Основната причина е, че протеините са най-консервативните молекули на живите организми заедно с нуклеиновите киселини и освен това са лесно достъпни за извличане от различни материали за диагностициране. Всъщност много заболявания могат да бъдат свързани до по-високото/по-ниското присъствие на протеин или до отчитане на различните им изомерни форми, както е например при изо-ензимите. Разработени са много хартиени сензори, използвайки различни стратегии. Основният формат, използван в хартиените нанобиосензори за откриване протеини е сандвич анализ, базиран на двойка антитела (образуване на имуно-сандвич), както е посочено по-долу.

Например латералните флуидни биосензори са устройства на основа хартия, които позволяват извършването на нискобюджетни и бързи диагностики с добра здравина, специфичност, чувствителност и ниски граници на откриване. Използването на наночастици като етикети играе важна роля в дизайна и производството на латерална поточна лента. Изборът на наночастици и съответният метод за откриване оказват пряко влияние върху представянето на тези устройства. Открити са и се прилагат на практика различни наноматериали (например, златни наночастици, въглеродни нанотръби, квантови точки, технологии за преобразуване на фосфори и латексови топчета и други) в латералните флуидни биосензори. Също така са разработени различни методи за детекция (коло-

риметрични, флуоресцентни, електрохимични, магнитни и т.н.) и стратегии за усилване на сигнала (осигуряващи вторични реакции или модифициращи архитектурата на латералните поточни ленти, както и използването на устройства като смартфони за разчитане на резултата от латералните поточни ленти. Подобен механизъм на подобряване фунцията на латерален биосензор е предложен от Choi et al.(2010), комбинирайки два типа златни наночастици с различен размер в същият сандвич за откриване на Тропонин I с граница на откриване от 10 pg mL^{-1} в серумни проби на пациенти с миокарден инфаркт.

4.5.2. Приложение на биосензори при детекция на нуклеинови киселини

Откриването на нуклеинови киселини се използва за генетични тестове, но също и за откриване на патогени, произвеждащи тези молекули изключително важни в диагностиката. Използваните проби обикновено са предварително амплифицирани с помощта на PCR (Polymerase Chain Reaction) или изотермични техники, за да има достатъчно количество ДНК, което да бъде открито, или пробите са синтетични ДНК последователности. Освен това връзката на ДНК последователностите с хартията обикновено се появяват чрез употреба на двойка протеини, като биотин-авидин или антиген-антитяло, който прави мост между ДНК и хартията.

Дори когато в експеримента не се включва никакви наночастици, заслужава да бъде спомената, тъй като учените са проектирали хартиена лента, която е способна на амплификация на ДНК с помощта на техника на усилване на въртящ се кръг (RCA), друга изотермична алтернатива на PCR. Учените са се възползвали от и показаха, че поли (N-изопропилакриламидни) микрогелове, свързани с ДНК олигонуклеотиди, са съвместими с ензимни реакции. Накратко те могат да открият до 100 pM от ДНК мишена, която беше използвана като шаблон за ДНК лигаза, за да свърже последователност за улавяне с последователност на праймер. Новата ДНК молекула се амплифицира допълнително от RCA, което генерира изключително дълга ssDNA, която може да бъде открита с помощта на комплементарна ДНК, функционализирана с флуоресцентно багрило.

4.5.3. Устройства, базирани на клетки

Хартиени устройства, които интегрират клетки или като рецептори индиректно откриване на протеини или други видове, или за тяхното пряко откриване, също са разработени. Трябва да се отбележи, че повечето от клетките не могат да преминат непокътнати през порите на използвани мембрани, но те могат да бъдат прикрепени към повърхността на хартията.

Li et al. (2019) разработват LFA за откриване на цели клетки антигени на Pseudomonas aeruginosa и Staphylococcus aureus въз основа на използването на златни наночасици, функционализирани със специфични антитела като етикети. Авторите получават засичане на диапазон на бактериалните линии в рамките на 500–5000 CFU mL^{-1}; освен това в тази работа те описват производството на компактно преносимо устройство, което преобразува интензитета на цвета на златни наночастици в количествено отчитане на напрежението, пропорционално на бактериалната концентрация в пробата.

Liu et al (2019) развиват лентов аптамер-златни наночастици биосензор за откриване на циркулиращи ракови клетки, достигайки граница на откриване от 4000 Ramos клетки с невъоръжено око и 800 клетки Ramos с преносим лентов четец в рамките на 15 мин. Освен това клетките са открити и в човешки кръвни проби.

Разработен е лентов поточен биосензор, базиран на имуносандвич със златни наночастици за откриване на Salmonella typhi в човешки серум. LoD достигнато от авторите е 1,14 105 cfu mL1 в рамките на 15 минути, което е по-добро от дот блот имуноанализ.

Някои други интересни биосензори, въпреки че не използват никакви нано материали, но поради тяхната интересна иновация също са описани. Първата работа, извършена от Struss, описва разработване на преносим лентов биосензор на базата на филтърна хартия за откриване на сигнални молекули, чувствителни към бактериален кворум, N-ацил-хомосеринови лактони (AHL). Те достигат LoD от 10 nM AHL и те също биха могли успешно да използват устройството за физиологични проби. За кратко те изсушават върху лента от филтърна хартия генетично модифицираните бактериални клетки, които използват бета-галактозидаза като репортерен протеин. Пробите от слюнка се нанасят върху лентата.

4.5.4. Приложение на биосензори за детекция на инфекциозни заболявания

В борбата с инфекциозните заболявания често е важно да се постави точна и навременна диагноза, за да се вземе информирано решение относно плана за лечение. Бързата и точна диагноза позволява на клиницистите да предпишат правилното медицинско лечение и значително подобрява прогнозата на пациента като цяло. По-специално, когато става дума за инфекциозни заболявания, навременната диагноза е още по-важна и може да намали или предотврати по-нататъшна инфекция в популацията от пациенти.

Въпреки че има много ефективни методи за откриване на патогенни агенти, като култивиране в селективни среди, микроскопия, геномна амплификация (например PCR) и имуноанализ (например ELISA), всеки от тези подходи има свои собствени недостатъци и е по-малко приложим в условия с ограничени ресурси, където инфекциозните заболявания са по-разпространени. Други диагностични методи като полимеразна верижна реакция (PCR) и ензимно-свързан имуносорбентен анализ (ELISA) са по-ефективни по отношение на времето и обхвата, но имат няколко недостатъка. Имуноанализите могат успешно да се използват за откриване на инфекциозни заболявания, ако се определи правилното взаимодействие антитяло-антиген, но са трудни за разработване и използване за откриване на патогени с високи нива на епитопна мутация (например при високата изменчивост на бактериалиния и вирусния геном). Поради изброените недостатъци, необходимостта от разработването на иновативни методи за бърза и надеждна диагностика нараства неимоверно.

Докато всеки биосензор се характеризира с няколко предимства и недостатъци, базирани на целевото приложение, техният дизайн обикновено включва висока специфичност и селективност на лиганда, висок капацитет на пропускателна способност, динамичен обхват, бързо откриване, лекота на проектиране и работа, рентабилност и ниска мощност изисквания.

Изводи от четвърта глава

Биомаркерите, свързани с установяване на болестни състояния, могат да служат като индикатори на човешките заболявания. Клиничната диагноза на заболяванията може значително да се възползва от навременното и точно откритие на биомаркери, което е предмет на обширни изследвания. Например поради специфичността на разпознаването на антитела и антигени, електрохимичните имуносензори могат точно да открият множество биомаркери на заболявания, включително протеини, антигени и ензими. Конструирани са различни типове типовете електрохимични имуносензори. Фокуса на приложенията на тези имуносензори е върху възможностите за откриване на рак, болестта на Алцхаймер, новия коронавирусен пневмония и други заболявания. Бъдещите тенденции в електрохимичните имуносензори са свързани с постигане на по-ниски граници на детекция, подобряване на възможностите за модификация на електродите и разработване на композиции. Всички биосензори се свързват вече и със СМАРТ устройства, което дава възможност за споделяне на резултатите в различни посоки. Тук се демонстрира много ярко необходимостта за защита от една страна на личните данни за здравословното състояние на всеки човек, от друга страна защита на данните от злоупотреби при тяхното събиране, обработване и включване в големи бази данни. Ясно се очертава необходимостта от разработване на специализирани протоколи в направление кибербиосигурност. Демонстрацията на интердисциплинарния подход при решаването на поставения въпрос за осигуряване на защита на тези чувствителни данни изисква целенасочени усилия за съвместна работа на национални институции, отговорни за защита на националната сигурност.

ГЛАВА ПЕТА:
РЕЗУЛТАТИ ОТ ЕМПИРИЧНИ ИЗСЛЕДВАНИЯ

В рамките на дисертацията са проведени две отделни проучвания – едното, свързано с микробиома на кърмата, второто, разделено като две под изследвания, свързани с готовността на млади специалисти и специалисти в областите на киберсигурността, кибербиосигурността и противодействието на кибербиоатаки. Като краен резултат проведените изследвания потвърждават необходимостта от разработването на **модел за прилагане** на методологии за синхронизиране на физическата сигурност, киберсигурността и биосигурността като елемент от националната сигурност.

Проведените емпирични изследвания са важна част от разработването на концепцията за кибербиосигурност и внедряването ѝ в практиката. При анализ на получените данни се постигна:

1. **Проучване** нивото на информираност на специалистите от структурите за бедствия и аварии и защита на населението в областта на киберсигурността и биосигурността.

2. **Изследване** на наличните към момента протоколи за реакция при кибер- и биоинцидент.

3. **Изследване** нивото на информираност на институциите, имащи отношение към проблема за синхронизиране на физическата, кибербиосигурността.

4. **Изследване** нивото на безопасност на данните през призмата на кибербиосигурността, получени при осъществяване на проучване на здравословния статус на човешкия микробиом с анализиране на биологичен материал – майчина кърма и фецес на дете на възраст до една година.

5. **Изследване** нивото на безопасност на данните през призмата на кибербиосигурността, получени като косвен резултат при анализ на генетичен материал от майчина кърма и фецес на дете на възраст до една година.

6. Изработване на конкретни изисквания към методологията за взаимодействие на физическата и кибербиосигурността във връзка с динамиката на взаимоотношенията между държавни и частни структури с различен предмет на дейност.

Към момента на провеждането на изследванията, свързани с младите експерти и специалистите от структурите за противодействие на заплахи в областта на киберсигурността и биосигурността, става ясно, че полето е недоразработено и с изключение на дисертацията на д-р Петър Цветанов от 2021г. на тема *„Готовност на болниците за активно лечение за медицинско осигуряване на пострадали при радиологичен тероризъм“*, защитена в МУ-София, до този момент не са правени сходни изследвания. За целите на проведеното анкетно проучване са конструирани две отделни анкетни карти, с оглед спецификата на профила на респондентите, като за отделни въпроси използваме вече разработеният модел в дисертацията на д-р Цветанов. (вж. ПРИЛОЖЕНИЕ 1 Анкета **Млади Специалисти** и ПРИЛОЖЕНИЕ 2 Анкета **Специалисти**).

Методологични ограничения на изследването

Настоящото изследване е проведено чрез онлайн анкетна форма, създадена и разпространена посредством платформата **LimeSurvey** в периода април-май 2024г. Въпреки предимствата на този метод – бързина на регистрация на данните, достъп до по-широка аудитория и автоматизирана обработка – съществуват и редица методологични ограничения, които следва да бъдат отчетени при интерпретация на резултатите:

1. **Проблеми с представителността:** Използването на онлайн анкета води до само селекция на участниците, като се допуска участие основно на лица с достъп до интернет и дигитална грамотност. Това създава риск от изкривяване на извадката спрямо генералната съвкупност. В конкретното изследване това може да бъде отбелязано през начина, по който анкетите бяха разпространени през т.нар. gatekeepers с оглед на чувствителността на регистрираните данни и спецификата на двата въпросника. Така проведеното изследване може да бъде мислено не толкова откъм неговата **представителност, а откъм неговата прецедентност.** При подбора на респонденти сме се водили не толкова от спазването на принципните за формиране на представителна извадка, в която участниците биха взели участие на базата на случаен подбор, колкото от принципите, стоящи в основата на формирането на **удобна извадка**, имаща за цел да фокусира изследването сред една определена група с конкретен професионален и социално-демографски профил. Част от недостатъците на изследването са свързани и с това, че **то географски ограничено е до територията на гр. Пловдив, като от своя страна ограничава възможността за обобщаване на данните и получените резултати.**
2. **Качество на данните:** В условията на дистанционно попълване на такъв тип изследваният винаги е налице риск от ниска ангажираност на респондентите, което може да се прояви в прибързано попълване, пропуски или произволни отговори, особено при по-дълги въпросници. В конкретният случай това се прояви под формата на възвръщаемост на данните – при анкета № 1 Млади специалистите са получени общо 216 анкети, от които частично попълнени бяха 152, а цялостно попълнени 64. При анкета №2 Специалисти общ получени анкети е 124, от които частично попълнени бяха 72, а цялостно попълнени 52. В хода на анализа на анкетите статистически са обработени само цялостно попълнените анкети, чиито резултати ще бъдат представени в изложението.
3. **Ограничен контрол върху процеса на попълване:** Изследователят няма възможност да контролира средата, в която се попълва анкетата, нито да гарантира, че респондентът я е попълнил сам и обективно. В конкретният случай разчитахме основно на gatekeepers, през чийто вътрешни канали бяха разпространени анкетите, съответно и мотивацията за тяхното

попълване от страна на участниците с оглед на вътрешната институционална динамика между ръководителите на отдели и експертите в тези отдели, както в системата на национална сигурност, така и в сферата на здравеопазването.

4. **Технически ограничения:** Макар LimeSurvey да предлага различни опции за контрол и филтриране на отговорите, при липса на регистрация или еднократни линкове, не може напълно да се изключи възможността за дублирани или фалшиви отговори.
5. **Ограничения при отворени въпроси:** Отворените въпроси често остават непопълнени или съдържат твърде кратки и неинформативни отговори, което затруднява последващия качествен анализ. В конкретният случай и при двете анкети в рамките на отворените въпроси след първоначалният анализ на данните и тяхното кодиране в SPSS ver. 27, се наложи допълнителна обработка на отворените въпроси и тяхното типологизиране така че да могат да бъдат графично обобщени и анализирани по-лесно.

Въпреки тези ограничения, онлайн анкетата чрез LimeSurvey бе предпочетена с оглед на лесната ѝ достъпност и възможността за достигане до по-широк кръг респонденти в кратък период от време.

5.1. Резултати от Анкета № 1 Млади Специалисти (Анкетна карта за проучването на информираността и подготовката на млади специалисти и студенти при действие в случай на кибератака, биотерористична атака и кибербиоатака (ID 448767)

Основни изводи

На базата на обобщените данни, могат да се формулират следните обобщаващи изводи:

1. Работа с биологични токсини: Повечето респонденти не са работили в сфера, в която може да се получат биологични токсини. Основните биологични опасности, с които се срещат, са бактерии и вируси.
2. Знания за биотероризъм и кибербиотероризъм: Повечето респонденти знаят какво е биотероризъм и кибербиотероризъм. Въпреки това, значителна част от тях не се чувстват подготвени за даване на първа помощ при биотерористична атака.
3. Подготовка и инструкции: Голяма част от респондентите нямат инструкции за действие в случай на биотерористична атака или кибератака в институциите, където работят. Лични предпазни средства също липсват в много от институциите.
4. Обучения и периодичност: Повечето респонденти смятат, че е необходимо да се провеждат периодични обучения за реагиране при бедствени ситуации и биотерористични атаки. Предпочитаният период за такива обучения е една година.
5. Кибератаки: Много малко респонденти са провеждали обучение за действие в случай на кибератаки. Повечето не разполагат с инструкции за действие при кибератаки и не могат да боравят с апаратура за оценка на кибератака.
6. Демографски данни: Повечето респонденти са жени, най-голям е относителният дял на младите специалисти под 25 години, като повечето респонденти имат трудов стаж по специалността една година, което съответства на изведения демографски профил.

На базата на данните от анкетата, най-големите рискове, които се открояват могат да бъдат типологизирани в няколко категории и под категории:

1. Биологични токсини:
   - Бактерии и вируси: Най-често срещаните биологични опасности на работното място.
   - Киселини, химикали и химични вещества: Също представляват значителен риск.
2. Липса на подготовка и инструкции:
   - Недостатъчна подготовка за биотерористични атаки: Много респонденти не се чувстват подготвени за даване на първа помощ при биотерористична атака.
   - Липса на инструкции и лични предпазни средства: В много институции липсват инструкции за действие и лични предпазни средства.
3. Кибератаки:
   - Недостатъчна подготовка за кибератаки: Много малко респонденти са провеждали обучение за действие в случай на кибератаки.

- Липса на инструкции и апаратура за оценка на кибератака: Повечето респонденти не разполагат с инструкции за действие при кибератаки и не могат да боравят с апаратура за оценка на кибератака.

4. Вредите от кибератака:
   - Изтичане на лични данни: Най-често посочваната вреда при компрометиране на чувствителни данни.
   - Психологически травми и финансови злоупотреби: Също представляват значителен риск.

Тези рискове показват необходимостта от подобряване на подготовката и инструкциите за действие при биотерористични атаки и кибератаки, както и от провеждане на периодични обучения за реагиране при бедствени ситуации. На базата на откритите с рискове с цел превенция могат да бъдат направени и няколко предложения:

За да намалим рисковете, свързани с биотероризъм, кибербиотероризъм и биологични токсини, можем да предприемем следните мерки:

1. Подобряване на знанията и подготовката
   - Обучения и семинари: Провеждане на редовни обучения и семинари за персонала относно биотероризъм и кибербиотероризъм. Това включва теоретични и практически занятия.
   - Информационни материали: Разпространение на информационни материали, които обясняват рисковете и начините за реагиране при биотерористични атаки и кибератаки.
2. Разработване и внедряване на инструкции
   - Инструкции за действие: Разработване на подробни инструкции за действие при биотерористични атаки и кибератаки. Тези инструкции трябва да бъдат достъпни за всички служители.
   - Симулации и упражнения: Провеждане на симулации и упражнения, които разиграват хипотетични сценарии на биотерористични атаки и кибератаки. Това ще помогне на персонала да се подготви за реални ситуации.
3. Осигуряване на лични предпазни средства
   - Лични предпазни средства: Осигуряване на лични предпазни средства за всички служители, които могат да бъдат изложени на биологични токсини. Това включва маски, ръкавици, защитни облекла и др.
   - Инструкции за използване: Обучение на персонала как правилно да използва личните предпазни средства.
4. Подобряване на инфраструктурата и технологиите
   - Оценка на биологичното замърсяване: Осигуряване на апаратура и методология за оценка на биологичното замърсяване. Обучение на персонала как да борави с тази апаратура.
   - Киберсигурност: Внедряване на системи за киберсигурност, които защитават чувствителните данни на институцията. Обучение на персонала как да реагира при кибератака.
5. Периодични проверки и актуализации
   - Периодични проверки: Провеждане на периодични проверки на готовността на институцията за реагиране при биотерористични атаки и кибератаки.
   - Актуализации на инструкциите: Редовно актуализиране на инструкциите за действие и обучителните материали, за да се отразят новите заплахи и технологии.
6. Създаване на специализирани екипи
   - Специализирани екипи: Създаване на специализирани екипи от обучени специалисти, които да реагират при биотерористични атаки и кибератаки. Тези екипи трябва да бъдат на разположение 24/7.
7. Повишаване на осведомеността
   - Кампании за осведоменост: Провеждане на кампании за повишаване на осведомеността сред служителите и обществеността относно рисковете от биотероризъм и кибератаки.

Тези мерки ще помогнат за значително намаляване на рисковете и ще повишат готовността на институциите и персонала за реагиране при бедствени ситуации.

5.2. Резултати от Анкета № 2 Специалисти (Анкетна карта за проучването на информираността и подготовката на специалисти в областта на киберсигурността, биосигурността и кибербиосигурността (ID 427823)

Основни изводи

На базата на проведеното анкетно проучване и представените данни могат да бъдат направени няколко обобщения:

1. Липса на знания и подготовка за биотероризъм и кибербиотероризъм
   - Знания за увреждания на здравето: 73.08% от респондентите не знаят какви увреждания на здравето може да се предизвикат при злоупотреба с чувствителни данни.
   - Подготовка за първа помощ: 87.50% от респондентите не се чувстват подготвени за даване на първа помощ при биотерористична атака или инцидент с биологични токсини.
2. Липса на инструкции и лични предпазни средства в институциите
   - Инструкции за действие при биотероризъм: 78.85% от респондентите нямат инструкции за действие в институцията, в която работят, в случай на биотерористичен акт.
   - Лични предпазни средства: 71.15% от респондентите нямат лични предпазни средства във институцията, с които да се предпазят при биотерористична атака или случаен инцидент.
3. Липса на обучение за кибератаки
   - Обучение за кибератаки: 65.38% от респондентите не са провеждали обучение за действие в случай на кибератаки.
   - Инструкции за действие при кибератаки: 61.54% от респондентите нямат инструкции за действие в институцията, в която работят, в случай на кибератаки.
4. Вредите от кибератака
   - Изтичане на лични данни: 34.62% от респондентите посочват изтичането на лични данни като основна вреда при кибератака.
   - Психологически травми: 13.46% от респондентите посочват психологическите травми като основна вреда.
   - Финансови злоупотреби и загуби: 21.15% от респондентите посочват финансовите злоупотреби и загуби като основна вреда.

Тези рискове подчертават необходимостта от подобряване на знанията и подготовката на персонала, разработване и внедряване на инструкции за действие при биотерористични атаки и кибератаки, осигуряване на лични предпазни средства и провеждане на редовни обучения и семинари. Това ще помогне за значително намаляване на рисковете и повишаване на готовността за реагиране при бедствени ситуации.

Резултатите от проведеното изследване сред експертите също разкрива значителни пропуски в знанията и подготовката за биотероризъм и кибератаки. Повечето респонденти не са работили в среда с биологична опасност, като основните инциденти, които познават, включват инциденти в изследователски лаборатории, ядрени аварии и нерегламентирано изхвърляне на биологични отпадъци. Въпреки това, значителна част от респондентите не знаят какви увреждания на здравето може да се предизвикат при злоупотреба с чувствителни данни, като основните увреждания включват психологически травми и промяна на диагноза и лечение.

Подготовката и инструкциите за действие при биотероризъм са недостатъчни. Повечето респонденти не са провеждали обучение за действие в случай на биотероризъм и нямат инструкции за действие в институциите, където работят. Лични предпазни средства също липсват в много от институциите. Освен това, повечето респонденти смятат, че оказването на медицинска помощ на хора, претърпели биотерористична атака, носи риск за тяхното здраве, и много от тях не се чувстват подготвени за даване на първа помощ при такива инциденти.

Кибератаките също представляват значителен риск, като много малко респонденти са провеждали обучение за действие в случай на кибератаки. Повечето не разполагат с инструкции за действие при кибератаки и не могат да боравят с апаратура за оценка на кибератака. Основните вреди от кибератака включват изтичане на лични данни, психологически травми и финансови злоупотреби.

Препоръки за намаляване на рисковете

За да се намалят рисковете, свързани с биотероризъм и кибератаки, е необходимо да се подобрят знанията и подготовката на персонала чрез редовни обучения и семинари. Разработването и внедряването на подробни инструкции за действие при биотерористични атаки и кибератаки е от съществено значение. Осигуряването на лични предпазни средства за всички служители и подобряването на инфраструктурата и технологиите за оценка на биологичното замърсяване и киберсигурност също са важни мерки. Провеждането на периодични проверки и актуализации на инструкциите, създаването на специализирани екипи от обучени специалисти и повишаването на осведомеността сред служителите и обществеността ще помогнат за значително намаляване на рисковете и повишаване на готовността за реагиране при бедствени ситуации.

5.3. Резултати от Анкета № 3: Изследването на микробиома на кърмата като пример за анализ на чувствителни данни с медицинско значение

Споделянето и използването на чувствителни данни от живи хора представлява значителни предизвикателства при разглеждането на етични, правни и обществени въпроси. В ЕС Общият регламент за защита на данните (GDPR) има за цел да защити гражданите на ЕС от нарушения на неприкосновеността на личния живот и данни в днешното общество, управлявано от данни, чрез установяване на правила за обработката и движението на лични данни. GDPR обаче оставя място за национални дерогации и това позволи да се запази известна последователност в правния пейзаж в рамките на Европейското икономическо пространство (ЕИП), оказващи неблагоприятно въздействие върху практиката на клинични и научни изследвания

Изследванията, включващи здравна информация, са изправени пред съществени предизвикателства, рискове и ограничения по отношение на поверителността на пациентите. Проучвания в последните години показват, че много пациенти не се чувстват удобно, когато всичките им здравни данни се споделят, дори ако основните идентификатори са премахнати. Един чувствителен елемент от здравната информация е свързана с данни за новородените. Кърменето на новородените в първите месеци след раждането е природосъобразния начин за тяхното оцеляване и приспособяване към начина на живот. Данните, които са получени от научни изследвания в различен аспект за кърмата, кърменето и здравословния статус на детето и майката, са важен елемент от концепцията за жизнен просперитет на човешката популация като цяло. Все повече се прилага модела на персонализирани данни съотнесени към социалната и екологичната среда, което изисква много внимателно събиране, обработка, съхранение и ползване на тези персонални данни. За да проверим нивото на информираност от една страна и от друга нивото на потенциална заплаха от злонамерено използване на събраните персонални данни ние проведохме анкети сред кърмещи майки, като част от научно изследване върху профила на микробиома на кърмата съотнесен към здравето на детето.

В нашето изследване поради ограничеността на времето и финансирането ние проведохме анкета и анализирахме данните от лабораторното проучване на един от ключовите параметри на кърмата, наличието на полезни микроорганизми в микробиома на изследваните проби кърма. Проектирането на подходящо проучване е ключов момент в биомедицинските изследвания. Анкетата, която проведохме, ни даде възможност да оценим нагласите и възможността за участие на много от участниците като донори на кърма за изследването, което проведохме паралелно. В резултат на изследването на микробиома на кърмата и получените резултати, които свързахме с информацията от изготвеното проучване, ни даде убедеността от защита на интелектуалната собственост в лицето на разработения протокол за изследване на кърмата за установяване на състояние на дисбиоза. Разработеният протокол се отнася до разработването на специфичен метод за in vitro количествено определяне на бързо предсказване на дисбиоза при бебета до 1-годишна възраст, при което се постига способността да се контролира човешкия микробиом, като в метода, според описанието, се вземат предвид от една страна общи показатели като възраст и пол, а от друга страна специфичните показатели за човешкото здраве. Предложеният метод се основава на обработката на данни от анализи на разнообразието и съотношението на микроорганизми в чревния тракт и други телесни течности (слюнка, кърма, изпражнения), количеството на метаболитите, използвани като биомаркери и отчитане нивото на ензимната активност на ензими, използвани като биомаркери, позволяващи да се вземат предвид индивидуалните характеристики на хората. Методът се основава на in vitro анализ на баланса на чревната микробиота при деца от един до дванадесет месечна възраст и прогноза

за възстановяването му при установена дисбиоза чрез изчисляване на коефициенти на корелация между ключови показатели, разделени в три основни групи:

1. Съотношение между състава и количеството на микроорганизмите в кърмата и в изпражненията на детето;

2. Корелация между ензимния профил и активността на ензимите, отговорни за усвояването и метаболизма на компонентите на млякото (лактоза, липиди, олигозахариди, протеини) в проби от кърма и изпражнения на детето;

3. Корелация между количеството на метаболитите, получени от метаболизма на основните компоненти на кърмата от микробиотата в кърмата и във фекалиите на детето.

Има три ключови аспекта, които трябва да се имат предвид по отношение на публикуване на чувствителни здравни данни в режим на анонимност. Първо, точното дефиниране на термина е доста трудно. Терминологията се различава в държавите-членки на ЕС. Например в Обединеното кралство данни, които са „свързани-анонимизирани“ или „псевдонимизирани“, могат да се считат за „анонимни“, ако администраторът на данни няма достъп до ключа за свързване. Второ, когато става въпрос за данни или биопроби, свързани с пациенти, не е сигурно колко ефективно могат да бъдат анонимизирани. Освен това, ако са анонимизирани, съществува опасение, че част от тяхната изследователска стойност може да бъде намалена. Трето, пълната (несвързана) анонимност не позволява на донора да упражни правото си да оттегли съгласието си и прави невъзможно връщането на резултати от изследвания или случайни открития към тях.

ГЛАВА ШЕСТА:
АНАЛИЗ НА ДАННИТЕ ПРИ СИНХРОНИЗИРАНЕ НА ФИЗИЧЕСКАТА СИГУРНОСТ И КИБЕРСИГУРНОСТТА В ДИГИТАЛНИТЕ ОБЩЕСТВА

6.1. Общи положения

Преплитането на цифровите технологии и физическия свят въвежда ера, в която сигурността вече не се ограничава до кибердомейна или физическия домейн, а обхваща и двете. Това изисква преоценка на парадигмите за сигурност, подчертавайки значението на синхронизираните стратегии за защита на нашите все по-дигитални общества. Важността на този въпрос се състои в нейната актуалност за националната сигурност, икономическата стабилност и защитата на правата и свободите на личността. Размиването на границите между физическите и цифровите процеси, разбирането и прилагането на интегрирани мерки за сигурност е от първостепенно значение.

Пейзажът на заплахите в цифровите общества се характеризира със своята сложност и динамика, тъй като противниците на държавите непрекъснато експлоатират взаимовръзките между физическата и киберсферата. Киберфизическите системи, като електрически мрежи, транспортни мрежи и здравеопазване, се превръщат в основни цели за кибербиотерористични атаки, демонстрирайки потенциала на кибератаките да причинят физически последствия. Този развиващ се пейзаж подчертава необходимостта от единен подход към сигурността, който обхваща както кибернетични, така и физически уязвимости.

Синхронизирането между физическата сигурност и киберсигурността е от решаващо значение за предотвратяване, реагиране и смекчаване на инциденти, свързани със сигурността. Несъгласуваните усилия могат да доведат до пропуски в позициите за сигурност, което улеснява заплахите да проникнат през защитата. Синхронизираният подход гарантира, че мерките за сигурност са съгласувани, разузнаването се споделя между домейни и реакциите при инциденти са бързи и ефективни. Тази холистична перспектива е от съществено значение за укрепване на защитите срещу комплексни заплахи, които използват връзката между физическия и цифровия свят.

Цифровите общества се характеризират със своята зависимост от информационните и комуникационни технологии за ежедневните си функции, от управление и търговия до социално взаимодействие и забавление. Тази зависимост създава киберфизическа среда, която е неразделна част от функционирането на обществото, но също така въвежда уязвимости. Защитата на този свят изисква нюансирано разбиране за това как цифровата и физическата сигурност се пресичат и влияят една на друга, което налага стратегии, които са адаптивни и гъвкави и гледат напред.

Нововъзникващите технологии като AI, интернет на нещата (IoT) и блоковата верига играят ключова роля в оформянето на пейзажа на сигурността. Въпреки че тези технологии предлагат

иновативни решения за подобряване на сигурността, те също така въвеждат нови уязвимости и вектори на атака. Двойната цел на нововъзникващите технологии подчертава значението на включването на стратегии за сигурност, ориентирани към технологиите, които се опитват едновременно да използват тези иновации за защита и да смекчат рисковете, които те представляват.

Синхронизирането между физическата сигурност и киберсигурността също представлява предизвикателства за политиката и управлението. Разработването и прилагането на политики, които обхващат и двете области, изисква координация между широк кръг от заинтересовани страни, включително държавни агенции, частни сектори и гражданско общество. Освен това глобалният характер на киберзаплахите налага международно сътрудничество, което допълнително усложнява усилията за управление. Справянето с тези предизвикателства е от решаващо значение за създаването на ефективни и устойчиви рамки за сигурност.

Икономическите последици от синхронизираните стратегии за сигурност са значителни. Инцидентите в киберсигурността могат да имат преки финансови последици, като разходи, свързани с отговор и възстановяване, както и косвени последици, като загуба на доверие на потребителите и увреждане на репутацията на марката. Обратно, ефективната синхронизация може да подобри икономическата стабилност чрез защита на критичната инфраструктура, гарантиране на надеждността на цифровите транзакции и изграждане на доверие в цифровите екосистеми.

Интегрирането на мерки за физическа и киберсигурност повдига и социални и етични въпроси. Въпроси като опасения за поверителността, наблюдение и потенциална злоупотреба с технологии трябва да бъдат внимателно обмислени. Тук може да представим един пример от реалния живот, който на пръв поглед не касае използването и потенциалната злоупотреба с чувствтелни персонални данни. Татуировките и перманентния грим са широко разпространени в световен мащаб, но все още значително малък брой са публикуваните научни изследвания по отношение на здравния риск свързан с тях. Нарастващата им популярност доведе до увеличаване на съобщенията за последващи инфекции. Татуирането може да се разглежда като пример от една страна за здравен риск (инфекции, психологични проблеми), а от друга като иконически и социален риск (нерагламентирания внос, разпространение и употреба на мастила и други консумативи за татуиране). Въпреки че мастилата се инжектират в човешкото тяло, обикновено за тях не се изисква строгото съблюдаване на специфичните изисквания за безопасност за разлика от други вещества (напр. лекарства, импланти и др.). По своята същност този процес представлява нараняване на кожата, вследствие на което могат да се развият повърхностни и вътрешни инфекции, да се отключат системни възпалителни процеси, екзема, псориазис, лишеи, фотодерматит и т.н. Получените наранявания чрез нарушение на епидермалната бариера на кожата по време на татуиране представляват „врата“ за микробни патогени, които в последствие могат да причинят локална инфекция на раната. В някои случаи е възможно да възникнат нежелани реакции веднага след процедурата, но могат да се появят и продължителни инфекциозни процеси, тъй като патогените от цветните пигменти могат да проникнат в кръвта чрез кръвоносната система на дермата. Поради тези факти като основен източник за здравен риск се считат съставките на мастилото. Докато преди десетилетия са се използвали само натурални багрилни продукти (един от най-разпространените е екстракт от растението Lawsonia inermis), към настоящия момент масово се прилагат мастила с неясен произход и съдържание, тъй като все още липсват единни международни стандарти за тяхното производство. Предлаганите на пазара мастила за татуировки представляват сложни смеси, съдържащи над 100 съединения от пигменти, разтворители, сгъстители, консерванти и други примеси. Липсата на ясно описание също крие сериозни рискове за здравето, въпреки че информацията за точния списък на съставките трябва да бъде предоставена от всеки производител. Татуистите и козметиците купуват свободно мастилата най-често директно от доставчици или чрез интернет, което създава допълнителни проблеми. Сериозни притеснения предизвиква и факта, че голяма част от мастилата се транспортират и съхраняват в контейнери за многократна употреба. Този процес крие допълнителен риск от замърсяване (напр. със стафилококи, стрептококи и др.). Резултати от научни проучвания докладват за наличието както на аеробни, така и на анаеробни бактерии в търговски мастила за татуировки и перманентен грим, съхранявани при аеробни и анаеробни условия. Това означава, че дори фабрично запечатани мастила могат да съдържат анаеробни бактерии, за които е известно, че виреят в среда с ниско съдържание на кислород (каквато е дермалния слой на кожата) заедно с аеробните бактерии. Логично следва да се предполага, че замърсените мастила могат да предизвикат инфекция и от двата вида бактерии.

От друга страна е налице социален и икономически риск през използването на студия за татуировки, които осъществяват по същество търговска дейност. При направеното съвсем бегло проучване в нашата страна липсва сериозен контрол както по отношение на вноса на мастила и консумативи, така и върху дейността на салоните за татуировка по отношение на спазване на хигиенните условия за интервенция в човешкото тяло.

Балансирането на необходимостта да се гарантира защитата на индивидуалните права и свободи е сложно предизвикателство, което изисква обмислени подходи, които зачитат етичните принципи и социалните ценности.

Изграждането на устойчивост в цифровите общества изисква ангажимент за непрекъснато проучване, иновации и сътрудничество. Това включва не само разработването на технически решения, но и създаването на култура, която признава сигурността сред хората и организациите. Образованието и осведомеността са ключови компоненти на това усилие, както и създаването на партньорства между сектори и граници.

Синхронизирането между физическата сигурност и киберсигурността в цифровите общества е не само технически проблем, но и многостранно предизвикателство, което се пресича с политиката, икономиката, обществото и етиката. Справянето с това предизвикателство изисква цялостен и интегриран подход, който признава сложността на ландшафта на заплахите и използва сътрудничеството и иновациите за изграждане на устойчиви защити. Тъй като дигиталните общества продължават да се развиват, значението на синхронизираните стратегии за сигурност само ще нараства, което подчертава необходимостта от непрекъснати изследвания, диалог и действия в тази критична област.

Предложение за нова концепция за взаимодействието между физическата и киберсигурността

Сближаването на физическата сигурност и киберсигурността в цифровите общества бележи значителна промяна на парадигмата в подхода за защита на нашия взаимосвързан свят. Важността на тази тема не може да бъде надценена, тъй като тя пряко засяга националната сигурност, икономическата стабилност и неприкосновеността и безопасността на хората. Това нарастващо разчитане на цифровите технологии разми границите между физическото и киберпространството, създавайки сложен пейзаж, в който заплахите могат да преминат през тези области и да имат дълбоки последствия. Това академично изследване подчертава необходимостта от синхронизиран подход към сигурността, интегриращ физически и киберстратегии за справяне с многостранния характер на съвременните заплахи. Такъв интегриран подход е не само полезен, но и от съществено значение за намаляване на рисковете и повишаване на устойчивостта при сложни и променящи се заплахи.

Интегрирането на технологиите за AI и машинно обучение (ML) в системите за сигурност е пример за иновативните стратегии, използвани за прогнозиране и противодействие на заплахи. Тези технологии имат потенциала да революционизират практиките за сигурност, като предоставят възможности за прогнозиране, като по този начин изместват парадигмата от реактивни към проактивни механизми за сигурност. Посочените по-горе казуси, като атаката на червея Stuxnet и ботнет експлоатацията на Mirai, илюстрират конкретните последици от киберфизическите заплахи и критичната необходимост от здравословна синхронизация между мерките за физическа и кибернетична сигурност. Такива инциденти служат като напомняне за присъщите уязвимости в нашите взаимосвързани системи и потенциала за катастрофални последици, ако тези уязвимости не бъдат адресирани по подходящ начин.

Предизвикателствата, свързани със синхронизирането на физическата сигурност и киберсигурността, са многобройни и включват технологични, организационни и културни аспекти. Преодоляването на тези предизвикателства изисква съгласувани усилия за насърчаване на интердисциплинарно сътрудничество, интегриране на съвременни технологии и преодоляване на сложни регулаторни условия. Документът показва, че докато технологичните решения са незаменими, човешкият фактор играе ключова роля за ефективността на мерките за сигурност. По-специално образованието и обучението се очертават като основни компоненти в култивирането на култура, съзнателна за сигурността, която признава взаимосвързания характер на заплахите и значението на интегрираните практики за сигурност.

Регулаторният натиск и натискът за съответствие допълнително усложняват процеса на синхронизация, изисквайки гъвкавост и адаптивност в задълженията за сигурност, за да се отговори на

законовите изисквания. които в същото време ефективно защитават от заплахи. GDPR в ЕС служи като отличен пример за това как регулаторните рамки оформят практиките за сигурност, изисквайки от организациите да приемат всеобхватни подходи, които обхващат физическа и цифрова защита. Тези разпоредби подчертават значението на синхронизацията не само за защитата на данните и инфраструктурата, но и за осигуряване на съответствие с по-строги законови изисквания.

Бъдещето на сигурността в цифровите общества е неразривно свързан с усилията за предвиждане, адаптиране и смекчаване на рисковете, породени от променящия се пейзаж на заплахите. Това изисква непрекъснати изследвания, инвестиции в нововъзникващи технологии и международно сътрудничество за разработване и прилагане на ефективни стратегии за синхронизация. Проучването на тенденциите и прогнозите в облака разкрива ясен консенсус сред експертите относно нарастващото значение на синхронизирането между физическата сигурност и киберсигурността. Интегрирането на AI и IoT технологиите, фокусът върху устойчивостта и стратегиите за възстановяване и акцентът върху вътрешните заплахи подчертават динамичния характер на предизвикателствата пред сигурността и иновативните подходи, разработени в отговор.

Сливането на физическата и киберсигурността в рамките на цифровите общества бележи решителна промяна в подхода към защитата на критична инфраструктура, данни и активи. Тази интеграция се движи от нарастващата взаимовръзка между физически съоръжения и кибер мрежи, което води до появата на киберфизически системи (CPS). Както е посочено от Humaed et al. (2017), CPS са неразделна част от работата на критична инфраструктура, включително електрически мрежи, транспорт и здравеопазване, което подчертава важността на единния подход към сигурността. Авторите твърдят, че взаимосвързаният характер на тези системи ги прави уязвими на широк спектър от атаки, което налага синхронизирани стратегии за сигурност, които се справят както с кибернетични, така и с физически заплахи.

Сложността на пейзажа на заплахите в цифровите общества е допълнително разработена от Kitchin and Dodge (2014), които обсъждат как цифровизацията на физически транзакции създава нови уязвимости. Те подчертават, че традиционните мерки за сигурност, предназначени да се справят изолирано с физически или киберзаплахи, вече не са достатъчни. Необходимостта от интегрирани подходи към сигурността се подчертава от Alcaraz и Zeadally (2015), които представят задълбочен анализ на предизвикателствата и решенията за защита на индустриалните системи за контрол от киберфизически атаки. Изследването им подчертава критичността на синхронизирането на физическата сигурност и киберсигурността за защита срещу сложни атаки, които могат да имат катастрофални физически последици.

Предизвикателството за синхронизиране на стратегиите за физическа сигурност и киберсигурност е изследвано от Collier et al. (2016), които предлагат стратегическа рамка за постигане на ефективна интеграция. Тази рамка подчертава важността на организационната координация, споделянето на разузнавателна информация и ефективните стратегии за реагиране. По подобен начин Zhu и Basar (2011a; 2011b) разглеждат оперативните предизвикателства на синхронизацията, включително необходимостта от съвместими технологични платформи и комуникационни протоколи между домейни. Тези проучвания подчертават трудността за постигане на синхронизация, но също така и потенциалните ползи от една позиция за сигурност.

Измеренията на политиката и управлението на синхронизирането на физическата и киберсигурността са изследвани от Dunn-Cavelty и Suter (2009), които анализират последиците за националната политика и политиките за сигурност. Те твърдят, че ефективната синхронизация изисква не само технически решения, но и политически рамки, които улесняват сътрудничеството между правителствени агенции, частни сектори и международни партньори.

От икономическа гледна точка Anderson and Moore (2006) представят общ анализ на разходите и ползите, свързани с прилагането на синхронизирани мерки за сигурност. Те подчертават потенциала за значително икономическо въздействие, включително предотвратяване на вредни пробиви, защита на критична инфраструктура и подобряване на доверието на потребителите в цифровите системи. Тази икономическа перспектива е от съществено значение за разбирането на по-широките последици от стратегиите за сигурност и оправдаването на инвестициите в синхронизирани мерки за сигурност.

Ролята на технологичните иновации за улесняване на синхронизирането на физическата и киберсигурността е ключова тема в литературата. Demirkan et al. (2020) обсъждат потенциала на блокчейн технологията за подобряване на сигурността в кибер-физическите системи чрез осигуря-

ване на сигурен и прозрачен механизъм за управление на достъпа и контрола. Mitchell and Chen (2014) изследват използването на AI за откриване и реагиране на заплахи за сигурността във физическите и кибер домейни, илюстрирайки как технологията може да преодолее пропастта между традиционно отделни домейни.

Практическите приложения на синхронизираните стратегии за сигурност са подчертани чрез казуси. Krotofil et al. (2015) представят казус за сигурността на системите за промишлен контрол, демонстрирайки как мерките за физическа сигурност могат да бъдат интегрирани в защитата на киберсигурността за защита срещу саботаж и шпионаж. Тези примери от реалния свят предоставят ценна представа за предизвикателствата и успехите на прилагането на синхронизирани подходи към сигурността.

Обществените последици от синхронизираните мерки за сигурност са обсъдени от Dunn-Cavelty и Leese (2018), които разглеждат въздействието върху неприкосновеността на личния живот и гражданските свободи. Те предупреждават, че интегрирането на физически и кибер технологии за наблюдение може да доведе до инвазивен мониторинг, който поражда етични опасения. Въпреки това те също така отбелязват, че внимателно разработените мерки за сигурност могат да подобрят обществената сигурност, без да застрашават индивидуалните права, като подчертават използването на балансиран подход.

Значението на международното сътрудничество за постигане на ефективна синхронизация между физическата сигурност и киберсигурността е подчертано от Nye (2016). Той твърди, че киберзаплахите пресичат националните граници, което изисква съгласувани усилия за разработване и прилагане на стратегии за сигурност, които са ефективни на глобално ниво. Тази перспектива подчертава необходимостта от международни норми и споразумения, които улесняват сътрудничеството в защитата на киберфизическите системи.

Гледайки напред, литературата предлага няколко области за бъдещи изследвания, включително разработването на усъвършенствани алгоритми за откриване на заплахи, изследване на нови модели на управление и оценка на дългосрочните икономически въздействия на синхронизираните стратегии за сигурност. Изследователи като Radanliev et al. (2020a; 2020b) предлагат акцент върху интегрирането на нововъзникващи технологии, като IoT и интелигентна инфраструктура в рамките на сигурността. Тези бъдещи насоки подчертават непрекъснатото развитие на полето и необходимостта от непрекъснати иновации и сътрудничество.

Прегледът на литературата подчертава критичното значение на синхронизирането на физическата сигурност и киберсигурността в цифровите общества. Нарастващата взаимосвързаност между физическата и цифровата сфера представлява уникални предизвикателства, но също така и възможности за разработване на цялостни стратегии за сигурност. Прегледаните произведения колективно подчертават необходимостта от интегрирани подходи, които се занимават със сложността на ландшафта на заплахите, който предизвиква организацията и технологичната интеграция и последиците за политиката, управлението и обществото.

Синхронизирането между физическата сигурност и киберсигурността в цифровите общества е критично и сложно начинание, което изисква интердисциплинарен подход, използващ най-новите технологични резултати и насърчаване на култура на осъзнаване на сигурността. Важността на тази тема произтича от нейното пряко въздействие върху защитата на критичната инфраструктура, икономическите интереси и благосъстоянието на хората в един все по-дигитален свят. Тъй като цифровите общества продължават да се развиват, интегрирането на физическата и киберсигурността ще стане още по-важно за справяне със сложните и взаимосвързани заплахи на бъдещето. Това академично изследване не само подчертава настоящите реалности и предизвикателства на синхронизацията, но също така подчертава необходимостта от новаторски, интегрирани стратегии за навигация, работещи в сложността на дигиталната ера. Пътят напред изисква сътрудничество, иновации и твърд ангажимент за подобряване на сигурността във всички нейни измерения, осигурявайки по-безопасно и по-устойчиво цифрово общество за бъдещето.

ЗАКЛЮЧЕНИЕ

В съвременния свят, където технологиите и интернет играят все по-голяма роля в ежедневието ни, кибербиосигурността се утвърждава като критичен аспект от националната сигурност. Тази дисертация разгледа различните измерения на кибербиосигурността, включително заплахите, уязвимостите и необходимите мерки за защита. Анализът показа, че биологичните системи и данни са подложени на нарастващи рискове от кибератаки, които могат да имат сериозни последици за общественото здраве, икономиката и социалната стабилност.

Основните изводи от изследването подчертават необходимостта от интегриран подход към кибербиосигурността, който включва както технически, така и организационни мерки. Важно е държавите да разработят и прилагат стратегии за защита на критичната инфраструктура, да инвестират в обучение и повишаване на осведомеността сред населението, както и да насърчават международното сътрудничество в борбата срещу киберзаплахите.

Проведената анкета сред специалисти в различни области като сигурност, киберсигурност и клинични лаборатории също показа тревожни резултати. Резултатите от анкетата разкриха ниска степен на готовност за опазване на чувствителни биомедицински данни и липса на подготвеност за реакция при биотерористични заплахи. Това подчертава необходимостта от незабавни действия за подобряване на капацитета и подготовката на тези ключови сектори.

На базата на анализа и констатациите от изследването, предлагам следните конкретни мерки за подобряване на кибербиосигурността:

1. Законодателни инициативи: Разработване и приемане на нови закони и регулации, които да обхващат специфичните нужди на кибербиосигурността. Тези нормативни актове трябва да включват строги изисквания за защита на биомедицинските данни и процедури за реагиране при инциденти. Особено внимание трябва да се обърне на регламента МИС 2, който въвежда задължителни стандарти за сигурност и поверителност на медицинската информация.
2. Обучение и повишаване на осведомеността: Провеждане на редовни обучения и семинари за служителите в здравните институции и лаборатории относно най-добрите практики за киберсигурност. Обученията трябва да включват теми като разпознаване на фишинг атаки, управление на пароли и използване на криптиране.
3. Инвестиции в технологии: Инвестиране в модерни технологии за киберсигурност, включително системи за откриване на проникванията (IDS), системи за предотвратяване на проникванията (IPS) и инструменти за мониторинг на мрежовия трафик. Тези технологии трябва да бъдат внедрени в критичните инфраструктури и постоянно обновявани.
4. Международно сътрудничество: Участие в международни форуми и инициативи за обмен на информация и добри практики в областта на кибербиосигурността. Създаване на партньорства с други държави и организации за съвместни проекти и изследвания.
5. Симулации и упражнения: Организиране на регулярни симулации и упражнения за реакция при кибератаки и биотерористични заплахи. Тези упражнения ще помогнат на институциите да идентифицират слабостите в своите системи и да разработят ефективни планове за действие.
6. Публично-частни партньорства: Насърчаване на публично-частни партньорства между правителствени агенции, академични институции и частния сектор за разработване на иновативни решения и технологии за кибербиосигурност.
7. Мониторинг и одит: Въвеждане на редовен мониторинг и одит на системите за киберсигурност в здравните институции и лаборатории. Това ще помогне за ранното откриване на уязвимости и своевременното им отстраняване.
8. Специализирана защита за изследователски центрове с генетично модифицираи организми (ГМО): Специално внимание трябва да се обърне на изследователските центрове, работещи с ГМО. Тези центрове трябва да бъдат оборудвани със специфични мерки за защита на техните бази данни и експериментални резултати, тъй като потенциалните последствия от компрометиране на тази информация могат да бъдат особено сериозни.

Тенденциите в развитието на съвременните заплахи ясно очертават необходимостта от стратегически и интегриран подход към кибербиосигурността като неразделен компонент на националната сигурност. На основата на проведените изследвания и направения анализ предлагам следните препоръки за усъвършенстване на политиките и практиките в тази област:

1. **Разширено участие на частния сектор и ИТ компаниите в кибербиосигурността:**

Частният сектор, включително биотехнологични компании, ИТ фирми и доставчици на облачни услуги, притежава значителна част от критичната инфраструктура и бази от биологични данни. Затова е необходимо:

- Приемане на законодателни изисквания за съвместимост със стандарти за кибербиосигурност (напр. ISO/IEC 27001 с разширения за работа с биоданни).
- Насърчаване на публично-частни партньорства между държавни институции, академични среди и частни компании с цел развитие на иновативни биосензори, криптографски алгоритми и други технологични решения в сферата на биосигурността.
- Създаване на сигурни механизми и протоколи за докладване и обмен на информация между държавата и частния сектор при инциденти.

2. **Регионално сътрудничество в Югоизточна Европа:**

Кибер и биозаплахите често са трансгранични по своя характер. Това изисква координирани усилия между държавите от региона чрез:

- Създаване на регионална координационна платформа (например балканска група по кибербиосигурност под егидата на ENISA или друга международна организация).
- Организиране на съвместни учения и симулации с участието на здравни, военни и ИТ структури.
- Обмяна на добри практики и експерти, създаване на регионална база данни с компетентни специалисти в областта.
- Разработване на хармонизирана нормативна рамка за защита на биологичните данни, контрол и унифицирани стандарти за частния сектор.

В заключение, устойчивото развитие на националната сигурност в условията на цифровизация и биотехнологичен прогрес е немислимо без адекватни мерки за кибербиосигурност. Реализирането на горепосочените препоръки ще съдейства за изграждането на по-ефективна, адаптивна и устойчива система за национална и регионална защита срещу съвременните хибридни заплахи. Кибербиосигурността не може да бъде пренебрегвана като част от националната сигурност. Тя изисква постоянни усилия и адаптивност, за да се справи с новите предизвикателства и да гарантира защитата на жизненоважни биологични системи и данни. Само чрез координирани действия и устойчиви политики можем да осигурим безопасността и благосъстоянието на нашето общество в цифровата ера.

ИЗВОДИ

На базата на анализа и констатациите от изследването, предлагам следните конкретни мерки за подобряване на кибербиосигурността:

1. Законодателни инициативи: Разработване и приемане на нови закони и регулации, които да обхващат специфичните нужди на кибербиосигурността. Тези нормативни актове трябва да включват строги изисквания за защита на биомедицинските данни и процедури за реагиране при инциденти. Особено внимание трябва да се обърне на регламента МИС 2, който въвежда задължителни стандарти за сигурност и поверителност на медицинската информация.
2. Обучение и повишаване на осведомеността: Провеждане на редовни обучения и семинари за служителите в здравните институции и лаборатории относно най-добрите практики за киберсигурност. Обученията трябва да включват теми като разпознаване на фишинг атаки, управление на пароли и използване на криптиране.
3. Инвестиции в технологии: Инвестиране в модерни технологии за киберсигурност, включително системи за откриване на проникванията (IDS), системи за предотвратяване на проникванията (IPS) и инструменти за мониторинг на мрежовия трафик. Тези технологии трябва да бъдат внедрени в критичните инфраструктури и постоянно обновявани.
4. Международно сътрудничество: Участие в международни форуми и инициативи за обмен на информация и добри практики в областта на кибербиосигурността. Създаване на партньорства с други държави и организации за съвместни проекти и изследвания.
5. Симулации и упражнения: Организиране на регулярни симулации и упражнения за реакция при кибератаки и биотерористични заплахи. Тези упражнения ще помогнат на институциите да идентифицират слабостите в своите системи и да разработят ефективни планове за действие.

6. Публично-частни партньорства: Насърчаване на публично-частни партньорства между правителствени агенции, академични институции и частния сектор за разработване на иновативни решения и технологии за кибербиосигурност.

7. Мониторинг и одит: Въвеждане на редовен мониторинг и одит на системите за киберсигурност в здравните институции и лаборатории. Това ще помогне за ранното откриване на уязвимости и своевременното им отстраняване.

8. Специализирана защита за изследователски центрове с ГМО: Специално внимание трябва да се обърне на изследователските центрове, работещи с генетично модифицирани организми (ГМО). Тези центрове трябва да бъдат оборудвани със специфични мерки за защита на техните бази данни и експериментални резултати, тъй като потенциалните последствия от компрометиране на тази информация могат да бъдат особено сериозни.

НАУЧНИ ПРИНОСИ

На базата на разработения дисертационен труд могат да се изведат следните научни и научно-приложни приноси:

1. Предложен е модел за съчетаване на физическата сигурност с киберсигурност и биосигурност при осъществяване на перманентен контрол на институции и фирми, работещи с чувствителни данни.
2. Предложен е модел за интердисциплинарен подход при надграждане на дейностите при осигуряване на кибербиосигурност при вектора чувствителни персонални данни – обработване на големи масиви от данни с чувствителна информация – регламент за съхранение и достъп до чувствителните големи бази данни.
3. Предложена е концепция за интердисциплинарен подход при разработване на протокол от мероприятия, които да осигурят нужната кибербиосигурност при работа с чувствителни данни на хората, касаещи здравния им статус.

Кибербиосигурността не може да бъде пренебрегвана като част от националната сигурност. Тя изисква постоянни усилия и адаптивност, за да се справи с новите предизвикателства и да гарантира защитата на жизненоважни биологични системи и данни. Само чрез координирани действия и устойчиви политики можем да осигурим безопасността и благосъстоянието на нашето общество в цифровата ера.

ПУБЛИКАЦИИ ВЪВ ВРЪЗКА С ДИСЕРТАЦИОННИЯ ТРУД

1. Bakov,K.,THE NEW REALITIES IN SYNCHRONIZING PHYSICAL SECURITY AND CYBERSECURITY IN DIGITALSOCIETIES , научно списание „Сигурност и отбрана“ – НВУ „Васил Левски“ , Година III Брой 1, 2024 г.
2. Mollova-Doshkova, D., Bakov, K., Iliev, I., The Art of Asking and Analyzing Sensitive Questions in Breast Milk Microbiome Research, Acta Microbiol. Bulg., приета за публикуване в издание 40(2) за 2024г. (Q4).
3. Bakova, D., Yaneva, A., Harizanova, S., Shopova, D., Mihaylova, A., Kasnakova, P., ... & Iliev, I. (2025). Monitoring Health Risks Associated with Body Modifications (Tattoos and Permanent Makeup): A Systematic Review. Cosmetics, 12(1), 8. (Q2)

УЧАСТИЯ В НАУЧНИ ФОРУМИ С ДОКЛАДВАНИ РЕЗУЛТАТИ ПО ДИСЕРТАЦИЯТА

1. Баков, К., Новите реалности при синхронизиране между физическата сигурност и киберсигурността в дигиталните общества, доклад, Конференция „Революции и Еволюции“, в ПУ „Паисий Хилендарски“ – 05-07.03.2024 г., участие.
2. Илиев, И., и Баков, К., Зелената икономика – предизвикателства и примери за интердисциплинарни решения, доклад, Международна научна конференция „Интердисциплинарния подход в приложното поле на икономическите и социалните науки“.
3. Баков, К., Финансиране на терористична организация чрез криптовалути, доклад Международна научна конференция „Интердисциплинарния подход в приложното поле на икономическите и социалните науки“.

4. Баков, К., Социално-емоционалното образование в контекста на физическата сигурност в учебната среда, доклад, Национална конференция „Социално-емоционално обучение в квалификацията на учителите“ (26-29 ноември 2023г.).
5. Daniela Mollova, Kostadin Bakov, Miroslav Zhekov, Ilia Iliev, Potential for the development of biosensors for the analysis of sensitive parameters in the study of the breast milk microbiome, II National scientific conference Physics-Engineering-Technology, 27-28 November 2024, Plovdiv, Bulgaria, poster D-8, p. 71.

БИБЛИОГРАФИЯ НА ЦИТИРАНАТА В АВТОРЕФЕРАТА ЛИТЕРАТУРА

1. Денчев, С. (2019). *Информация и сигурност*, Академично издателство „За буквите“ .ISBN 978-619-185-369-4
2. Чаушев, Х. (Декември 2024). Генеративен AI и съдържание в социалните медии – комуникационни предизвикателства в сферата на сигурността. *Сигурност и отбрана*(2), 179-187. https://doi.org/10.70265/YVKC6923
3. Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8,* 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002
4. Anderson, R., & Moore, T. (2006, October 27). The economics of information security. *Science, 314* (5799), 610-613. DOI: 10.1126/science.1130992. Retrieved from: https://www.cl.cam.ac.uk/~rja14/Papers/sciecon2.pdf
5. Collier, Z. A., Panwar, M., Ganin, A. A., Kott, A., Linkov, I. (2016). Security Metrics in Industrial Control Systems. In: Colbert, E., Kott, A. (eds) *Cyber-security of SCADA and Other Industrial Control Systems*. Advances in Information Security, vol 66 (pp. 167–185). Springer, Advances in Information Security, vol 66 (pp. 167–185). Springer, Cham. https://doi.org/10.1007/978-3-319-32125-7_9
6. Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics,* 7(2), 189–208. https://doi.org/10.1080/23270012.2020.1731721
7. Dunn-Cavelty, M., & Suter, M. (2009, December). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection, 2*(4), 179-187. https://doi.org/10.1016/j.ijcip.2009.08.006
8. Kitchin, R., & Dodge, M. (2014). *Code/space: Software and everyday life*. Massachusetts: MIT Press.
9. Krotofil, M., Larsen, J., & Gollmann, D. (2015, April). The process matters: Ensuring data veracity in cyber-physical systems. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security* (pp. 133-144). https://doi.org/10.1145/2714576.2714599
10. Li, Z., Chen, H., & Wang, P. (2019). Lateral flow assay ruler for quantitative and rapid point-of-care testing. *Analyst, 144*(10), 3314-3322.
11. Liu, H.; Ge, J.; Ma, E.; Yang, L. Advanced biomaterials for biosensor and theranostics. In Biomaterials in Translational Medicine, 1st ed.; Yang, L., Bhaduri, S.,Webster, T., Eds.; Academic Press: Cambridge, MA, USA, 2019; pp. 213–255.
12. Mitchell, R., & Chen, R. (2014). Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. *IEEE Transactions on Dependable and Secure Computing, 12*(1), 16-30. DOI: 10.1109/TDSC.2014.2312327
13. Nye Jr, J. S. (2016). Deterrence and dissuasion in cyberspace. *International security, 41(3), 44-71. https://doi.org/10.1162/ISEC_a_00266*
14. Radanliev, P., De Roure, D. C., Nurse, J. R., Mantilla Montalvo, R., Cannady, S., Santos, O., ... & Maple, C. (2020a). Future developments in standardisation of cyber risk in the Internet of Things (IoT). *SN Applied Sciences, 2,* 1-16. https://doi.org/10.1007/s42452-019-1931-0
15. Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., ... & Burnap, P. (2020b). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity, 3,* 1-21. https://doi.org/10.1186/s42400-020-00052-8
16. Zhu, Q., & Basar, T. (2011a, April). Towards a unifying security framework for cyber-physical systems. In Proceedings of the workshop on the foundations of dependable and secure cyber-physical systems (FDSCPS-11) (pp. 47-50). Retrieved from: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=b860375d2d89142f9b26870411f7ec7e0b56568a
17. Zhu, Q., & Başar, T. (2011b, December). Robust and resilient control design for cyber-physical systems with an application to power systems. In *2011 50th IEEE Conference on Decision and Control and European Control Conference* (pp. 4066-4071). IEEE. DOI: 10.1109/CDC.2011.6161031