НОВ БЪЛГАРСКИ УНИВЕРСИТЕТ
NEW BULGARIAN UNIVERSITY

ДЕПАРТАМЕНТ „НАЦИОНАЛНА И
МЕЖДУНАРОДНА СИГУРНОСТ“

АВТОРЕФЕРАТ

на дисертация на тема

КИБЕРСИГУРНОСТ В МРЕЖОВИ СИСТЕМИ ЗА УПРАВЛЕНИЕ

за присъждане на образователна и научна степен „доктор“,
професионално направление 9.1. „Национална сигурност“,
докторска програма „Стратегии и политики на сигурност“

Дипломант:
Николай Хранов

Научен ръководител:
доц. д-р. Юлияна Каракънева

СОФИЯ
2023

Дисертационният труд е обсъден и приет на заседание на департамент „Национална и международна сигурност“, проведено на 19.04.2023г. и със заповед № 3-РК-233/13.06.2023 г. е предложен за защита пред научно жури.

Авторът на дисертационният труд е докторант на самостоятелна подготовка, отчислен с правото на защита в докторска програма „Стратегии и политики на сигурност“, НБУ, професионално направление 9.1. Национална Сигурност.

Защитата ще се състои на 11.09.2023 г. в сградата на НБУ.

Дисертационният труд се състои от 129 страници

От които Приложение №1 се състои от 7 страници

От които Приложение №3 се състои от 13 страници

Брой на таблиците: 5

Брой на фигурите: 57

Брой на литературните източници: 31

Брой на публикациите, свързани с дисертацията: 4

Съдържание

1. ОБЩИ ОСОБЕНОСТИ И ХАРАКТЕРИСТИКИ НА ДИСЕРТАЦИЯТА

Актуалност на темата

Съвременното общество в глобален мащаб се характеризира с качествено ново отношение към информацията и използваните технологии, свързани с нея. Това се дължи на големите технологични постижения маркирали XX век – създаването и развитието на комуникационните и компютърните технологии. Развитието на Интернет показва най-добре синергетичният ефект от тяхното съчетаване и илюстрира огромното значение на комуникационните и компютърните технологии за съвременното общество, което днес определяме като информационно. Само за малко повече от двадесет години, от масовото навлизане на Интернет в обществената практика, тази технология, този истински феномен на съвременната цивилизация е намерил място във всяка страна и във всяка социална система; променил по радикален начин общуването между хората; направил общо и лесно достъпни огромни информационни ресурси; осигурил глобализирането не

само на икономиката, но и на всички области на социалната практика.

Цели и задачи на работата

Настоящият дисертационен труд е посветен на сигурността на операциите в мрежова система за управление. В свят, в който хората са напълно зависими от компютърните технологии и информационните системи, защитата на информацията е от решаващо значение. В представения труд е изследвана киберсигурността в рискова "чувствителна" среда, а именно мрежовите информационни системи.

Целта на настоящата дисертация е да се разработи теоретичен и приложен модел на сигурна система за миграция на данни в рискова среда като се приложат методи за непрекъснатост на информационния поток при миграционния процес.

За постигането на тази цели трябва да се изпълнят следните дефинирани научноизследователски задачи:

1. Разработване на процес за миграция на хибридна цифрова екосистема, съобразен с изискванията за киберсигурност.
2. Изграждане на концептуален модел за превенция на атаките и защита на информацията чрез система за управление на киберсигурността.
3. Разработване на приложен модел за превенция, защита и управление на киберсигурността в мрежова екосистема.
4. Създаване на прототип на сигурна система за миграция на информационната база.

Ограниченията, при които се решават задачите са определени от предварително зададената конфигурация на информационния масив, в съответствие с наличната информационна инфраструктура и използването на наличния хардуерен ресурс на сървърите.

2. ОБЕКТИ И ПРЕДМЕТ НА ИЗСЛЕДВАНЕТО

Обект на изследване в дисертационния труд е процесът на миграцията на съществуваща мрежова система за управление към нова информационна среда при изпълнение на изисквания на сигурност и защита на информацията.

Предмет на изследване е миграционната система на информационен масив, съдържащ “чувствителна” (рискова) информация и постигането на киберсигурност чрез внедряване на приложни техники и процедури.

Хипотеза на изследването. При прилагане на подходящи решения за киберсигурност е възможно да се постигне защита на критичната, по отношение на сигурността информация при използване на изградената мрежова (Интернет) свързаност и сигурен миграционен процес.

Методи за провеждане на изследването

При избора на методи за провеждане на изследването е отчетен характера на поставената цел, като се спазват принципите на прецизност, обективност, единство на анализа и синтеза, и дискретност. Предвид спецификата на разглеждания проблем и областта на изследване, е приложен качествен подход на изследване, които се концентрира върху цялост, обективност и точност на информацията. Избрани са научно – изследователски методи на концептуално и функционално моделиране, както и теоретичен и съпоставителен анализ с критичен аспект, причинно-следствен анализ, систематизиране, документиране и синтез.

3. СЪДЪРЖАНИЕ И СТРУКТУРА НА ДИСЕРТАЦИОННИЯТ ТРУД

За решаване на научноизследователските задачи и постигане на поставените цели дисертационният труд е структуриран във въведение, 4 глави, заключение, приложения и използвана литература.

В първа глава е направен обзор на използваните похвати и софтуерни процедури за миграция / асимилация на хибридна корпоративна мрежова система с възможност за внедрена идентификация. Описани са процедури и необходими сертификати за реализирането на информационната мрежова система на управление.

Разглежда се състоянието на проблемите и известни решения за сигурност, които се прилагат. Представена е класификация на известните инциденти и събития в киберсигурността.

Във втора глава се представя формален модел на идеалната среда на графичен и схематичен език. Проследено е тестването, очаквани резултати, интеграция на инфраструктура по вече изграден първичен мрежов управленски модел. Представена е детайлна текуща и непрекъсната диагностика на целия процес по миграция, като са съобразени всички параметри на работещият модел – идеална среда.

Изпълнени са следните задачи:

– Дизайн на базата от данни; модел на БД;

– Дизайн на информационната система, включващ хардуерната и комуникационната инфраструктура; модели на мрежовите системи на управление на инфраструктурата.

– План за миграция;

– Протоколи на трансфер на данните.

В трета глава разглежда основните похвати за активиране, разширяване и оптимизиране на функционалността, интегриране възможности за динамиката и непрекъсваемостта на информационният поток, въвеждане на дистанционен подход при обучение на персонал. Решения за сигурност.

Включени са следните етапи на процеса за сигурност:

– Откриване на вътрешни заплахи, чрез софтуер притежаващ изкуствен интелект;

– Изготвяне на функция за самооценка на информационните активи с участието на ръководните лица в мрежовите системи за управление;

– Наблюдение и контрол на достъпа от всички отдалечени точки, включително мобилни устройства;

– Програма за превенция на вътрешни заплахи;

– Предлагане на решения за киберсигурност на облачните услуги от хибриден и корпоративен тип. Контрол на жизнения цикъл.

– Предложение за концептуален модел на системата (интелигентен интерфейс) – хибриден модел №2 на киберсигурност в мрежовите системи за управление, предложен от настоящият дисертационен труд, използва като решение установяване на потенциални заплахи на системата за управление самообучаващи се алгоритми, разполагащи с изкуствен интелект. Като процеса на самообучение е непрекъснато развиваща се база за установяване на слабости и заплахи в системата, автоматично предприемане на решения, съобразени с вече установената конфигурация на системата за управление на мрежата.

В четвърта глава са представени резултатите, чрез сравнителен метод: Очаквани и изпълнени резултати, установени предимства на новата информационна система и установени параметри на киберсигурността.

Постигнати цели:

Резултати и решения за киберсигурност, като основен фактор за успешно извършване на миграционният процес на системата, с прилагането на самообучаващ се алгоритъм с елементи на изкуствен интелект, целящо постигането на максимална защита от атака тип “нулев ден”.

4. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД ПО СТРУКТУРНИ ЕЛЕМЕНТИ

4.1. ПЪРВА ГЛАВА – ИНТЕЛИГЕНТЕН ИНТЕРФЕЙС ЗА ПРЕНОС/МИГРАЦИЯ НА КРИТИЧНА ИНФРАСТРУКТУРА

В главата е направен обзор на използваните похвати и софтуерни процедури. Обзор и анализ на прилаганите ресурси за киберсигурност в корпоративните мрежи. Внедряване на интелигентен интерфейс за пренос/миграция на критична инфраструктура и данни към технологично нова кибернетична екосистема.

Обзор на специализирана система за миграция/асимилация на хибридна корпоративна мрежова система с възможност за внедрена идентификация, чрез дистанционна криптирана връзка към нова кибернетична екосистема, без активния процес да преустанови функционирането си, докато първата система не бъде окончателно асимилирана в новата такава, без да бъде нарушаван баланса на нейната киберсигурност.

Автоматизирането на дейностите на корпоративната мрежа, като правило, започва с внедряване на различни системи, по-специално съхранение, обработване и менажиране на критична работна информация, счетоводни и кадрови системи, изграждане на електронна система за управление на документи, създаване на системи за подкрепа и договорни дейности. В случая се визира наличието на няколко информационни системи в предприятието, които могат да работят автономно и са компоненти на „пачуърк[1]“ автоматизацията. В основата на изграждането на мрежовите системи за управление е концепцията за единично информационно пространство, с което трябва да работят всички подсистеми в единна база данни.

Пачуърк автоматизация на мрежовите системи за управление се формира, като правило, на базата на собствени разработки с добавяне на определено количество готов софтуер, който може да поддържа различни операционна система. В мрежовите системи за

[1] Цялостно решение на автоматизацията???? Напротив – на парче е

управление се създава базата на единни интегрирани платформи. Създаването на мрежовите системи за управление в рамките на една инструментална среда, значително подобрява ефективността на системата.

Днес широко се използва процесният подход към управлението дейностите на мрежовата система на управление. Той определя степента на автоматизация на основните и поддържащи бизнес процеси в корпоративните мрежи. В основата на работата на ИС на предприятието е функционалният подход, докато при мрежовите системи за управление е интегрираният набор от програми или информационни системи, които поддържат основните процеси на информационната екосистема.

Корпоративната информационна система не е само съвкупност от програми за автоматизиране на информационни процесите: управление производство, ресурси, финансови и икономически дейности.

Характерна особеност на мрежовите системи за управление е интегрирането от край до край, в чиято основа е системният модул, отговорен за бизнес процеса на цялата мрежова система на управление.

Аналогично избраната хибридна информационна система е насочена към решаване на частни задачи, докато мрежовите системи за управление е инструмент за повишаване на ефективността от всички гледни точки. Хибридната информационна мрежа е отворена интегрирана система в реално време, която автоматизира информационните процеси на всички нива и области на дейност, включително бизнес процеси за вземане на управленски решения.

Основната цел на мрежовите системи за управление е да се повиши ефективността и съхранението на информацията, т.е. задачите, които трябва да бъдат решени за постигане на тази цел са следните:

- свързване на информационните потоци на отделни единици и услуги в единно информационно пространство;

- повишаване на ефективността на получаването на информация, както и подобряване на нейните качества;

- увеличаване на скоростта на вземане на управленски решения и намаляване на рисковете,

дължащи се на обработката на надеждна висококачествена входна информация.

Функционалността на информационната система се определя от естеството и вида дейност, организационната и правна структура, географско разположение, характера на информационен обмен;

В мрежовите системи за управление следва да включва компоненти, които гарантират промяна на информационното пространство в корпоративните мрежи:

- редактиране на базата данни, промяна на структурата, полетата на таблици, връзки, индекси и др.;

- модификация на интерфейсите за въвеждане, преглед и корекция на информация;

- управление на структурата и функциите на бизнес процесите;

- промяна в организационното и функционално съдържание на потребителските места;

- генериране на отчети, сложни бизнес сделки и форми;

- разрешение на информация (за целите на информационната сигурност), регистрация на часа на

въвеждане и промяна на данни, водене на записи промени / изтривания на данни;

- инструменти за анализ на състоянието на системата по време на работа.

Анализът на състоянието на системата включва изследвания относно:

- оптималност на архитектурата на базата данни;
- ефективността на алгоритмите и програмите;
- статистика: броят на записите, документите, транзакциите, транзакциите;
- дневници на извършените операции;
- използваната дискова и оперативна памет.

4.2. ВТОРА ГЛАВА – КОНЦЕПТУАЛЕН МОДЕЛ

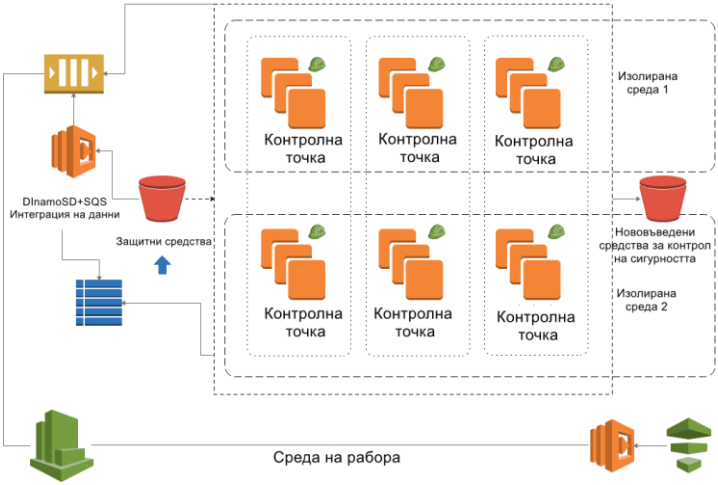
В тази глава се разглежда концептуален модел за преодоляване на заплахи, превенция и повишаване нивото на защита в мрежова система за управление, чрез прилагане на иновативни методи и най-добрите практики за управление на Киберсигурността, в дисертационният труд е извършеният анализ на мрежова система за управление и предложените от нея услуги, с цел да се определят основните ѝ характеристики:

• Предложение за система на самообслужване при поискване: Предоставя се източник на ресурси за самообслужване при поискване. Това е важна характеристика на изчислителните облаци, тъй като това позволява на процесите да променят използваните услуги като пространство и компютинг за изчисления, според необходимостта на системната и нейното натоварване без да се нарушават операциите на хоста.

• Предложение за широк достъп до мрежата: Да се използват ресурси тип cloud computing (Облачна изчислителна мощност), които могат да бъдат достъпни и осигурени, чрез основни мрежова връзка и за няколко вида устройства.

• Предложение за събиране на ресурси: Да бъдат обединени ресурсите на системата за повече ефективно и ефикасно използване. Чрез multitenancy (архитектура на софтуерно мултинаемане) и виртуализация, много потребители могат да се обслужват от един и същ физически хардуер.

В главата се определя модел на мрежовите системи за управление: Предложени са три функционални модела, ведно с тяхното описание, предимства и недостатъци, анализ на CVSS v4.1 резултати от оценка на нивата на сигурност. Предложение за функционален модел (Модел №1: идеална среда) на мрежова система за управление, както следва:



Фиг. 13: Принципна схема общ целеви модел №1 – идеална среда [2]

[2] Номерацията на фигурите е взета от Дисертацията

Проведен експеримент: Показания на процесите при неутрализиране на атаката (табличен вид – експорт от системата):

CVSS Base Risk Matrix - Access Vector (AV), Authentication (Au), AccessComplexity(AC) Risk Analysis

Access Vector (AV)	Local (L)	Adjacent Network (A)	Network (N)
Vulnerabilities	8084	164	119278
Exploitable	59%	26%	44%
Access Complexity (AC)	**High (H)**	**Medium (M)**	**Low (L)**
Vulnerabilities	17333	70847	39346
Exploitable	49%	56%	25%
Authentication(Au)	**Multiple (M)**	**Single (S)**	**None (N)**
Vulnerabilities	0	2292	125234
Exploitable	0%	55%	45%

Фиг. 22: Процесите при неутрализиране на атаката[3]

Базова матрица на риска с включени Вектор на достъпа (AV), Автентификация (Au), Сложност на достъпа, Рисков анализатор /съдържа съотношението на установените уязвимости към тези подлежащи на въздействие/

CVSS Base Risk Matrices - Confidentiality (C), Availability (A), Integrity (I) Impact Risk Analysis

	None (N)	Partial (P)	Complete (C)
Confidentiality Vulns	9044	37476	81006
Confidentiality Exploit	16%	31%	55%
Integrity Vulns	24805	22496	80225
Integrity Exploit	27%	29%	56%
Availability Vulns	40135	6243	81148
Availability Exploit	21%	65%	56%

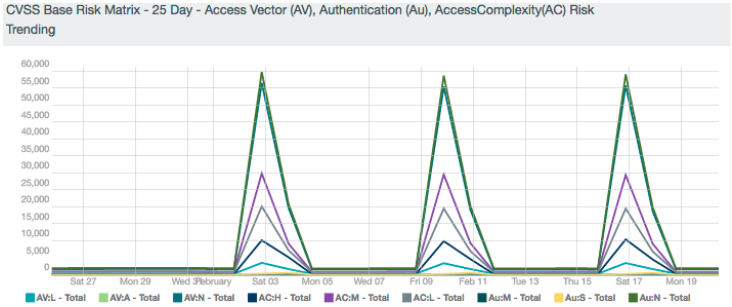
Фиг. 23: Съотношението на установените уязвимости към тези подлежащи на въздействие[3]

[3] Номерацията на фигурите е взета от Дисертацията

Базова матрица на риска с включени общата система за оценка на уязвимостите.

Съдържа конфиденциалност, наличност и интегритет на информацията, с добавяне на анализ на риска от въздействието: измерването е съгласно стойности от съотношението на установените уязвимости към тези подлежащи на въздействие.

Графично представяне на измерването:



Фиг. 24: Рискова матрица при 25 дневно замерване за инциденти[4]

[4] Номерацията на фигурите е взета от Дисертацията

4.3. ТРЕТА ГЛАВА – КОНФИГУРИРАНЕ

В главата се Конфигуриране на следните избрани параметри и решения, осигуряващи максимално ниво на превенция и защита от идентифицираните заплахи в приетата информационна инфраструктура – Модел 2 Хибридна система:

- Софтуерно дефинираните мрежи – SDN – с установени предварително и зададени комуникационни правила и нива на достъп.

- Software-defined computer: пакет от дефинирани регламенти за сигурност, в процеса по внедряване на външни приложения.

- Времетраене и преоразмеряване на виртуалните дискове. Процес на автоматичен анали от системата за необходимостта от софтуерен и хардуерен ресурс, както и спестяването на такъв – освобождаване при намалена необходимост.

- Live Migration – Мигриране в текущо време.

- SMB Transparent Failover: процеси за улесняване конфигурирането на MS Windows базирани машини в клъстеризация .

- SMB Scale Out: оптимизиране на оркестрация при споделянето на файлове с мащабиране предоставя възможност за споделяне на една и съща папка от множество възли на един и същи клъстер.

- Checkpoints: Превенция в реално време, чрез шлюзове към база данни за противодействие на известни зловредни кодове и потенциални техни мутации.

- Автоматизирано възстановяване: bootloader платформа за критично възстановяване на системата при тотален срив от текущият клъстер аз архивиране в реално време.

- Dynamic Device Association: менажиране в реално време на всички оторизирани в и свързани към системата устройства.

- Controller-Switch Trust: Контрола за предоставяне и снемане на доверие от външни програми при работа с базата данни вътрешна за системата.

- Controller-App Plane Trust: Контрола за мениджмънт на правила на външни програми при работа с базата данни вътрешна за системата.

- Security Domains: определящ фактор при класификацията на актива на мрежата, нивата на достъп и свързаността с външният свят.

- Дистанционен пряк достъп до паметта (RDMA): Мениджмънт подход с цел превенция от зловреден код тип “ransomware”, представляващ криптографска зловредна програма, която при успешно внедряване заразява цялата система и нейните данни, като ги криптира и иска откуп за тяхното отключване.

- Получаване на мащабиране на страниците (RSS): Надежден софтуерен механизъм, който не изисква висок ресурс за обмен на информация между два интернет базирани сайта от системата като поддържа, следене и функционалност.

- Опашка на виртуална машина (VMQ): Процес по оптимизация на трафика, чрез физическият мрежов адаптер, който прехвърля данните, директно към паралелна опашка за изпълнение.

- Обединяване на мрежовия адаптер: възможност за сливане на няколко входно / изходни комуникационни устройства в едно с цел по – лесна конфигурация, повишаване на капацитета на обработените данни, ниско

ниво на отказ – ако откаже един намалява скоростта, не спира свързаността.

- Внедряване на Distributed Firewalls: Цялостна разпределена защитна стена с множество потребители, която се предлага като услуга от доставчика на интернет свързаност. Администратора на мрежовата системата за управление конфигурира правила на защитната стена, за да защити своите виртуални мрежи от нежелан трафик, идващ от интернет и интранет мрежи.

5. ЗАКЛЮЧЕНИТЕЛНА ЧАСТ

Общи изводи и заключение

В резултат на извършените изследвания в дисертационния труд, са получени решения на актуални задачи, свързани с киберсигурността в мрежовите системи за управление. Постигнати са следните основни резултати:

В първа глава е направен Обзор на използваните иновативни похвати и софтуерни процедури. Анализ на основните подходи за оценка и управление на рисковете

за киберсигурността в корпоративните мрежи, в следните етапи:

1. Обзор на информационната система и основни рискове за сигурността на мрежовите системи за управление. Информационни мрежи и ключови активи;

2. Дефиниране на детайлни изисквания и бизнес процеси, които трябва да се реализират в системата. Концепцията за сигурност на корпоративните мрежи;

3. Основни методи за оценка на сигурността в мрежовите системи за управление и тяхното приложение.

Във втора глава:

Са проследени:

Основните параметри и свързаност на системата, за която се предлагат моделите на дисертационният труд-

Самообслужване при поискване: опростено планиране на капацитет с ресурсите на компютърните услуги;

Концептуален модел за преодоляване на заплахи, превенция и високо надеждна защита на мрежова система за управление, чрез прилагане на иновативни

методи и най-добрите практики за управление на Киберсигурността;

Приноси на предлаганата мрежова система за управление методологии за защита на корпоративните мрежи. Теоретични основи, очаквани резултати, интеграция на инфраструктура и решения по вече изграден първичен мрежов управленски модел – идеална среда.

Предложени са три функционални модела на мрежова система на управление;

Като методика за пресмятане на уязвимост е използвана Common Vulnerability Scoring System (CVSS) - Общата система за оценка на уязвимостите на CVSS v4.1, резултати от оценка на нивата на сигурност.

В трета глава са подробно изложени спецификите на Активиране, разширяване и оптимизиране на функционално интегрираните възможности за динамиката и адекватност на поточни нововъведения, въвеждане иновативен подход при обучение на

персонал. Вътрешни заплахи за сигурността на корпоративните мрежи, в следните етапи:

1. Откриване на вътрешни заплахи, чрез софтуер притежаващ изкуствен интелект;

2. Определяне на модел на системата;

3. Изготвяне на прогресираща функция на общата система за оценка на уязвимостите, предоставя начин за улавяне и установяване на основните характеристики на уязвимостта и изготвяне на числена оценка, отразяваща нейната сериозност. След това числовата оценка бива преведена в качествено представяне (като ниско, средно, високо и критично) чрез алгоритмично представяне, с цел правилно управление на процесите в киберсигурността на мрежовата система на управление

4. Наблюдение и контрол на отдалечения достъп от всички отдалечени точки, включително мобилни устройства;

5. Иновативна програма за защита от вътрешна заплаха;

6. Киберсигурност на облачните услуги от хибриден и корпоративен тип. Контрол на жизнения цикъл.

В четвърта глава /ПРИЛОЖНА ЧАСТ/ са посочени предимства на новоинтегрираната информационна система, с установени параметри. Посочване на хардуернаи софтуерна интеграция за извършване на миграционният процес, с участието на самообучаващ се алгоритъм притежаващ изкуствен интелект, целящ постигането на максимална защита от нападение тип “нулев ден”.

а) Дизайн на информационната система, хардуерната и комуникационната инфраструктура;

б) Определяне на потребителския интерфейс / проверка на крайното състояние;

в) План за миграция;

г) Проверка на крайното състояние;

д) Процедура за верификация;

е) Проверка на FourWay Handshake;

ж) Дискретизация на протокола.

6. НАУЧНИ И ПРАКТИКО - ПРИЛОЖНИ ПРИНОСИ

Научни приноси

1. Създадена е авторска и иновативна методика за инкорпориране на данните по делокализираната инфраструктура.

2. Направен е анализ на основните подходи в областта, като са взети техните предимства и недостатъци за градивни сегменти в настоящият дисертационен труд.

3. Постигнато е ново знание чрез въвеждане на едно адекватно и интуитивно информационно решение за миграция в иновативно подобрена облачна среда с цел оптимизиране и повишаване на всички критерии по кибербезопасност и гъвкавост към нововъведения.

4. Направен е авторски анализ на основните подходи в областта, като са взети техните предимства и недостатъци за градивни сегменти в настоящият дисертационен труд.

5. Обогатени са приетите добри практики при миграционен процес в затворена информационна система.

6. Анализирани всички тенденции в сектора към настоящият момент, като е предложено високо производително и кибернадежно информационно решение.

Практико-приложни приноси

1. Въз основа на проведените изследвания и анализи на специфичната инфорационна среда от затворен тип, са направени информационно приложими решения с научно-практическо приложение за създаване на нов подход при управление и Киберсигурност на мрежовите системи за управление марка.

2. Реализиран е мащабен проект по практическото създаване, виртуализиране, миграция на морално и софтуерно остаряла мрежова система на управление в корпорация, работеща изключително със значително чувствителна информация – финансови операции, към строго адекватна и динамична облачна среда със иновативни защитни механизми и надеждност при отказ

и огледално архивиране на три нива. Като оценката на решението е на значително ниска стойност и бързо изпълнение – определящи фактори за всяка система от високо ниво.

3. Създадена е авторска и иновативна методика за инкорпориране на данните по делокализираната инфраструктура.

4. Посочени са предимства на новоинтегрираната информационна система, с установени параметри на хардуерна и софтуерна интеграция за извършване на миграционният процес, с участието на самообучаващ се алгоритъм притежаващ изкуствен интелект, целящ постигането на максимална защита от нападение тип “нулев ден”.

5. Конфигуриране на иновативна програма за защита от вътрешна заплаха - софтуерен тип.

6. Разработен и асемблиран дизайн на информационната система, хардуерната и комуникационната инфраструктура.

7. НАУЧНИ ПУБЛИКАЦИИ ПО ТЕМАТА НА ДИСЕРТАЦИОННИЯТ ТРУД

1. ХРАНОВ, Н, 2017. Киберсигурност при облачните услуги. Сборник на участници в младежки дискусионен форум „Младите хора и Сигурността“. Магистърски факултет. Департамент „Национална и международна сигурност (НБУ), София: Издателство Авангард Прима, ISBN: 978-619-160-767-9.

2. ХРАНОВ, Н, 2023. Киберсигурност в мрежови системи за управление. IT4SEC Доклади - IT4SEC Reports, издавано от секция "Информационни технологии в сигурността" - ИТС, ИИКТ-БАН, ISSN (online) 1314-5614. DOI: https://it4sec.org/bg

3. ХРАНОВ, Н, 2023. Техники за оценяване на киберзаплахи в мрежова система за управление. IT4SEC Доклади - IT4SEC Reports, издавано от секция "Информационни технологии в сигурността" - ИТС, ИИКТ-БАН, ISSN (online) 1314-5614. DOI: https://it4sec.org/bg

4. ХРАНОВ, Н, 2023. Using Cloud Transforming for Big Network Management Procedure (Обратно Облачна

трансформация в корпоративни мрежи на управление). Електронен журнал: „Образование, научни изследвания и иновации“ (Education, Scientific Research and Innovation), година I, книжка 3, септември 2023, ISSN (online) 2815-4630. DOI: https://e-journal.unibit.bg

ДЕКЛАРАЦИЯ ЗА ОРИГИНАЛНОСТ

Долуподписаният Николай Найденов Хранов

- Декларирам, че настоящата работа е мое лично дело и че добросъвестно съм посочил всички използвани източници.
- Декларирам също така, че съм спазил/а изискванията за авторско право по отношение на използваните източници и не съм използвал неправомерно чужди текстове, без да посоча техния автор и източник.
- Уведомен съм, че в случай на констатиране на плагиатство в настоящата работа, комисията по защитата е в правото си да я отхвърли.

Заглавие на дисертационният труд:
КИБЕРСИГУРНОСТ В МРЕЖОВИ СИСТЕМИ ЗА УПРАВЛЕНИЕ

Подпис:.....