



ВОЕННА АКАДЕМИЯ „ГЕОРГИ СТОЙКОВ РАКОВСКИ”

ФАКУЛТЕТ „КОМАНДНО-ЩАБЕН“

КАТЕДРА „КОМУНИКАЦИОННИ И ИНФОРМАЦИОННИ СИСТЕМИ“

ЙОАНА АТАНАСОВА ИВАНОВА

**ИЗСЛЕДВАНЕ НА ВЪЗДЕЙСТВИЕТО НА КИБЕРАТАКИ
ВЪРХУ СИСТЕМА ЗА УПРАВЛЕНИЕ НА ТРАНСПОРТА**

АВТОРЕФЕРАТ

на дисертационен труд

за придобиване на образователната и научна степен „доктор“,
професионално направление 5.3. „Комуникационна и компютърна техника“,
научна специалност „Автоматизирани системи
за обработка на информация и управление“

НАУЧЕН РЪКОВОДИТЕЛ:

ПОЛКОВНИК ДОЦЕНТ ДОКТОР ИВАН СТЕФАНОВ ХРИСТОЗОВ

СОФИЯ, 2020

Дисертационният труд е обсъден на разширен съвет на Катедра „Комуникационни и информационни системи”, първично звено във Факултет „Командно-щабен“ на Военна академия „Г. С. Раковски” – София на 17.01.2020 г. и е насрочен за защита пред Научно жури по научната специалност „Автоматизирани системи за обработка на информация и управление”.

Авторът на дисертационния труд е докторант чрез самостоятелна подготовка в Катедра „Комуникационни и информационни системи“. Докторантът заема длъжност „асистент“ в Департамент „Телекомуникации“ на Нов български университет.

Основните изследвания по дисертационния труд са проведени в Катедра „Комуникационни и информационни системи“ на Военна академия „Г. С. Раковски”.

ДАННИ ЗА ДИСЕРТАЦИОННИЯ ТРУД:

- дисертационния труд се състои от 274 страници;
- основен текст – 217 страници;
- литературни източници – 108;
- фигури – 55;
- таблици – 41;
- брой на публикациите по дисертацията – 3;
- брой на приложенията към дисертацията - 8 с обем от 57 страници;
- номерирането на дефинициите, твърденията, фигурите и таблиците в автореферата съответства на това в дисертационния труд.

Защитата на дисертационния труд ще се състои на 27.03.2020 г. от 14:00 ч. в Академична зала А -3 на Военна академия „Г. С. Раковски”.

Материалите по защитата са на разположение на интересувашите се в стая № 206, преподавателски корпус на Военна академия „Г. С. Раковски”.

РЕЦЕНЗЕНТИ:

1.

2.

Автор: Ас. Йоана Атанасова Иванова

Тема: „Изследване на въздействието на кибератаки върху система за управление на транспорта“

Отпечатан: 2020 г.

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Вид на дисертационния труд

Дисертацията има характер на научноизследователски труд с формулирани работна хипотеза, цел и задачи. Обхваща: увод; основна част, включваща три глави; общи изводи; заключение; библиография/списък с използваната литература.

ОБЕКТ НА ИЗСЛЕДВАНЕТО

Обект на дисертационния труд са методите за моделиране на въздействието на кибератаки върху система за управление на транспорта чрез използване на специализиран симулационен софтуер.

ПРЕДМЕТ НА ИЗСЛЕДВАНЕТО

Предмет на дисертационния труд е моделиране на въздействието на кибератака върху ЦКТ на автомобилна транспортна система.

АКТУАЛНОСТ НА ТЕМАТА

Актуалността на темата се обуславя от приложението на съвременните симулационни технологии за изследване на сложни системи и визуализация на процесите, които се извършват в тях, чрез метода на агентно-базираното моделиране.

ЦЕЛ НА ДИСЕРТАЦИОННИЯ ТРУД

Целта на дисертационния труд е разработване на методика за оценка на уязвимостта и планиране на мерки за повишаване на устойчивостта на системата за управление на транспорта и транспортната система като цяло на база на предложения метод за моделиране и анализ на въздействието на кибератаки върху изградения симулационен модел на ЦКТ.

ОСНОВНИ ЗАДАЧИ НА ДИСЕРТАЦИОННИЯ ТРУД

Основните задачи на дисертационния труд са формулирани, както следва:

1. Разработка на адаптивна архитектура на система за кибернетична защита и топологичен модел на уязвимостите от кибернетични въздействия, който да представя взаимовръзките между съществуващ концептуален модел на кибер заплахата и използвания в дисертацията метод за оценка на системната уязвимост.
2. Изграждане на симулационни модели на ЦКТ, на база на които да се направи оценка и анализ на въздействието на кибератака върху системата за управление на транспорта.
3. Разработване на методика за оценка на уязвимостта на транспортната система към кибератаки.

РАБОТНА ХИПОТЕЗА НА ДИСЕРТАЦИОННИЯ ТРУД

Работната хипотеза на дисертационния труд е, че реализирането на кибератаки върху системата за управление на транспорта може да има сериозни нежелани последици върху транспортната система като сектор от критичната инфраструктура и респективно върху националната сигурност.

МЕТОДИКА НА ИЗСЛЕДВАНЕТО

Методиката на изследването включва следните стъпки за изпълнение на поставените задачи:

1. На база на информационни източници по темата да се направят сравнителни анализи, класификации, обобщения и да се изведат сигурни твърдения.
2. Да се анализират политиките за киберсигурност и добрите практики на силно развитите в икономическо отношение държави за превенция от рискове.
3. Да бъдат разгледани методи за моделиране на сложни системи.
4. Да се направи обосновка на избора на градска автомобилна транспортна система за провеждане на емпирично изследване.
5. Да се направи подбор на подходящи софтуерни продукти за реализация на емпиричното изследване.
6. Да се разработят алгоритми за изпълнение в използваните симулационни среди.
7. Да се обобщи опитът от експериментите и да се разработи методика за оценка на уязвимостта на транспортната система към кибератаки чрез моделиране на сложни системи.

ОГРАНИЧЕНИЯ

В дисертационния труд са приети следните ограничения:

1. Ограничения, свързани с контрол на средата и изследване на уязвимости на конкретни мрежови устройства предвид, че експериментите са проведени изцяло в симулационна среда и не са използвани хардуерни прототипи.
2. Подробното описание на предоставения за изследването модел на участък от градска автомобилна транспортна система се съдържа в цитираните източници, тъй като самото му изграждане не е обект на дисертационния труд.
3. За цялостното изследване на въздействието на кибератака върху ЦКТ на градска автомобилна транспортна система се налага комбинирането на два отделни продукта за симулационно моделиране, поради което преходът между двата етапа на изследването представлява логическа връзка, подкрепена с информация от цитираните литературни източници относно симптоматиката на различни кибератаки.
4. ЦКТ на автомобилна транспортна система е моделиран на ниво мрежова конфигурация без да се разглежда неговата софтуерна реализация поради конфиденциалността на информацията, невъзможността за практическа проверка на достоверността на публично достъпната информация относно, както и липсата на пряка връзка между инсталираните в ЦКТ софтуерни продукти и изпълнението на симулацията.
5. С оглед на еднозначен анализ на въздействието на кибератаката основните настройки в симулационния продукт са приети по подразбиране.
6. В модела на участъка от градска автомобилна транспортна система е въведен броят само на леките автомобили, които влизат в него.
7. Направените сравнителни анализи между метода на симулационното моделиране и други методи за изследване въздействието на кибератаки върху системата са теоретично-изследователски поради конфиденциалността на експерименталните резултати.
8. При изследване на екологичните ефекти под въздействие на кибератака върху участък от градска автомобилна транспортна система (Приложение IV), в симулационния софтуер могат да се въведат данни за броя на автомобилите с бензинов, дизелов и газов двигател спрямо общия брой на всички регистрирани автомобили, като екологичните не участват. Хибридните автомобили са

причислени към една от трите големи групи двигатели (бензинов, дизелов и газов) според един от начините си на задвижване.

9. Статистическите данни за процентните съотношения на регистрираните автомобили с дизелов, бензинов и газов двигател спрямо общия брой на регистрираните автомобили на територията на Република България са приети и за разглеждания участък поради невъзможност да бъдат определени с точност.

10. Предвид, че симулационният софтуер не дава информация в какъв обем въздух са измерени генерираните стойности на отделените емисии над участъка, в разработката се прави изчисление за обем от 1 до 1 000 000 [m³].

II. СТРУКТУРА И СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

СТРУКТУРА НА ДИСЕРТАЦИОННИЯ ТРУД

Дисертационния труд е структуриран в съответствие с поставените цел, научноизследователски задачи, работна хипотеза, обект и предмет на изследването и отразява възприетия от автора подход към проблематиката.

Състои се от увод, 3 глави с изводи към всяка от тях, заключение с насоки за бъдеща работа, 8 приложения, 41 таблици и 55 фигури с обем 274 страници. Цитираната литература включва общо 108 източника на български, английски и руски език.

СЪДЪРЖАНИЕ НА ДИСЕРТАЦИЯТА

В увода е дефинирана актуалността на разглеждания проблем, като е обоснована необходимостта от разработването на дисертационния труд. Формулирани са целта, основните задачи, ограниченията, работната хипотеза и методите, прилагани в хода на изследването.

ПЪРВА ГЛАВА. АНАЛИЗ НА УЯЗВИМОСТИТЕ И ВЪЗДЕЙСТВИЕТО НА КИБЕР ЗАПЛАХИ ВЪРХУ СИСТЕМА ЗА УПРАВЛЕНИЕ НА ТРАНСПОРТА

В Първа глава се акцентира върху логиката на функциониране на системата за управление на транспорта и в частност на Центъра на контрол на трафика (ЦКТ), както и върху адаптивното управление на кибер защитата на системата за управление на транспорта. Разглеждат се методи за оценка на риска от кибер заплахи и ефективни стратегии за неговото минимизиране предвид, че темата на дисертационния труд е основно ориентирана към сферата на киберсигурността, докато методът на симулационното моделиране е избраното от автора средство за доказване на формулираната работна хипотеза.

Разгледани са видове системи за управление на транспорта, ролята на транспортните системи във военната логистика и прилагането на метода за моделиране на сложни системи при изследването им. На база на анализ на основните типове транспорт и структурните и функционални характеристики на Интелигентните транспортни системи е направена обосновка на избора на автомобилен транспорт за провеждане на симулационните експерименти.

ВТОРА ГЛАВА. МОДЕЛИРАНЕ НА ВЪЗДЕЙСТВИЕТО НА КИБЕР ЗАПЛАХИ ВЪРХУ СИСТЕМА ЗА УПРАВЛЕНИЕ НА ТРАНСПОРТА

Във Втора глава се определят предимствата от използването на симулационните методи за решаване на сложни проблеми и задачи в случаите, когато е нецелесъобразно това да бъде направено във физическа среда.

В експерименталната част на дисертационния труд е симулирано въздействието на DoS - атака върху изграден типичен симулационен модел на ЦКТ и системата за сигнализация на светофарите на градска автомобилна транспортна система. На база на получените резултати от проведените симулации са разгледани възможни ефективни средства за защита от кибератаки.

Описанието на всеки проведен експеримент завършва с обобщени оценки и анализи, базирани на генерираните симулационни резултати, които показват в какво се изразява потенциалното въздействие на кибератаки върху реален участък от градска автомобилна транспортна система.

ТРЕТА ГЛАВА. МЕТОДИКА ЗА ОЦЕНКА НА УЯЗВИМОСТТА НА СИСТЕМАТА ЗА УПРАВЛЕНИЕ НА ТРАНСПОРТА КЪМ КИБЕР ЗАПЛАХИ

В Трета глава е разработена методика за оценка на уязвимостта на транспортната система към кибератаки чрез моделиране на сложни системи на база на направеното емпирично изследване и сравнителни анализи. В подкрепа на методиката е направена оценка на риска по два различни метода с използване на симулационните резултати. Планират се мерки за повишаване на устойчивостта на системата.

Ключови думи: киберсигурност, кибер заплаха, кибератака, транспортна система, транспорт, система за управление на транспорта, център за контрол на трафика, критична инфраструктура, симулационно моделиране, компютърни вируси, автомобилен транспорт, градски транспорт, контрол на движението, оценка на въздействието, замърсяване на въздуха, вредни емисии

УВОД

Системите за управление на транспорта и в частност Центърът за контрол на трафика (ЦКТ) са едни от най-важните компоненти на всяка транспортна система, която като сектор от критичната инфраструктура, е потенциален обект на различни по сила и характер физически и кибер заплахи. Това обуславя необходимостта от мерки за укрепване и поддържане на сигурна, функционираща и устойчива транспортна система чрез ефективни средства за защита, за да може практическата реализация на политиките за сигурност да отговори на очакванията, заложи в хода на процесите по прогнозиране и планиране. От голямо значение е правилният подход при оценка на риска от кибер заплахи и предвиждане на вероятните нежелани последици.

Критичната инфраструктура и в частност нейните сектори представляват гръбнакът на държавата и обществото. По своята същност те са съвкупност от материални и нематериални активи и управляващи ги организации, от които зависи пълноценното и правилно функциониране на държавните и частните организации, добрият жизнен стандарт на населението и националната сигурност като цяло.

Терминът „инфраструктура“ (от лат. „инфра“ - фундамент, „структура“ - строеж, разположение, взаимодействие) добива гражданственост по време на Втората световна война, когато се употребява предимно в логистиката за обозначаване на всички фиксирани и недвижими инсталации и средства за осигуряване и контрол на въоръжените сили [17].

Опитът на развитите страни показва, че за укрепване на киберсигурността е необходимо да бъдат предприети ефективни мерки, както на високо управленско ниво, така и в частния сектор. За постигане на удовлетворителни резултати са необходими финансови инвестиции, което е трудно дори за силно развитите в икономическо отношение държави. От друга страна, решението на проблема се изразява в широкото използване на симулационното моделиране и визуализацията като средства за предотвратяване на кибератаки чрез предварителното им пресъздаване във виртуална среда. В този случай финансовата инвестиция е напълно оправдана, защото е минимална в сравнение с разходите, до които би довел пробив в системите за сигурност.

Компютърните симулации правят възможно провеждането на експерименти във виртуална среда с използване на математически модели на реални системи. По този начин може да се направи реалистична оценка на риска и да се решат редица изследователски проблеми, свързани с изработването на стратегии за превенция, избор на мерки за защита и подобряване сигурността и устойчивостта на системата.

ПЪРВА ГЛАВА.

АНАЛИЗ НА УЯЗВИМОСТИТЕ И ВЪЗДЕЙСТВИЕТО НА КИБЕР ЗАПЛАХИ ВЪРХУ СИСТЕМАТА ЗА УПРАВЛЕНИЕ НА ТРАНСПОРТА

1.1. Анализ на уязвимостите в киберпространството

1.1.1. Идентификация и класификация на заплахите в кибернетичното пространство

Киберсигурност представлява основно направление в националната и международната сигурност и аспект на информационната сигурност. Тя се изразява в мерки, процедури и политики за предотвратяване на различни по вид и сила кибер заплахи, както и в преодоляване на нежеланите последици при евентуално реализиране на кибератака. Реализацията на една кибератака зависи от системната уязвимост, която представлява слабост, позволяваща на атакуващия да проникне в системата.

Понятието „кибернетична война“ обикновено се разглежда като съчетание от:

- кибертероризъм;
- семантично хакерство;
- симулационна война.

Задачите, които трябва да бъдат изпълнени в този случай, са:

- 1) **На ниво данни:** посредством контрол на достъпа;
- 2) **На ниво система:** чрез правилна конфигурация;
- 3) **На ниво потребители:** постъпване на информация за нарушаване на политиката за сигурност.

1.1.2. Задачи за оценяване и планиране на защитата от кибер заплахи

За изграждане на съгласувана и цялостна политика за сигурност в киберпространството е от голямо значение да бъдат поставени конкретни задачи за оценяване и планиране на критичната инфраструктура и да се работи последователно и организирано за тяхното изпълнение.

Задачите за вземане на решения по въпросите на киберсигурността могат да бъдат обединени в групи:

- **класификация на заплахите според типа и механизмите им на реализация;**
- **оценка на системната уязвимост на база на уязвимостите на елементите на системата;**
- **оценка на последиците при реализиране на нежелано събитие;**
- **създаване на политики за защита;**
- **обсъждане на инвестиции в изследвания за укрепване на киберсигурността;**
- **анализ и повишаване на ефективността на управленските процеси.**

Националният подход за справяне със заплахи има за цел да бъде изготвена стратегия за реагиране на база на вече направените предварителни анализи и оценки. Това изисква разработване и въвеждане в експлоатация на нови високи технологии, което от своя страна е свързано с големи финансови инвестиции.

1.2. Адаптивно управление на защитата на система за управление на транспорта от кибер заплахи

Логиката на функциониране на системите за управление на транспорта е в пряка зависимост от структурата и принципа на работа на централите за контрол на трафика.

В процесите на планиране и управление на сложни системи се прилага *архитектурният подход*, който се характеризира с някои основни предимства.

От гледна точка на физическата архитектура системите за управление на транспорта представляват подсистеми на транспортните системи, които се състоят от отделни *модули* и комуникират помежду си чрез *физически потоци от данни*. Връзката между архитектурната рамка и външната среда най-често се реализира чрез устройства или системи за набавяне на данни.

Основните логически части или функционалности на класически ЦКТ на интелигентна транспортна система са:

- **събиране и обработка на данни за трафика** – извършва се от пътни станции, а самите данни се съхраняват в хранилища;
- **разпространение на информация** – това е текстова или графична информация за водачите на превозни средства, която те получават посредством указателни табели (дисплеи);
- **предприемане на мерки за управление на трафика.**

В контролната зала са разположени:

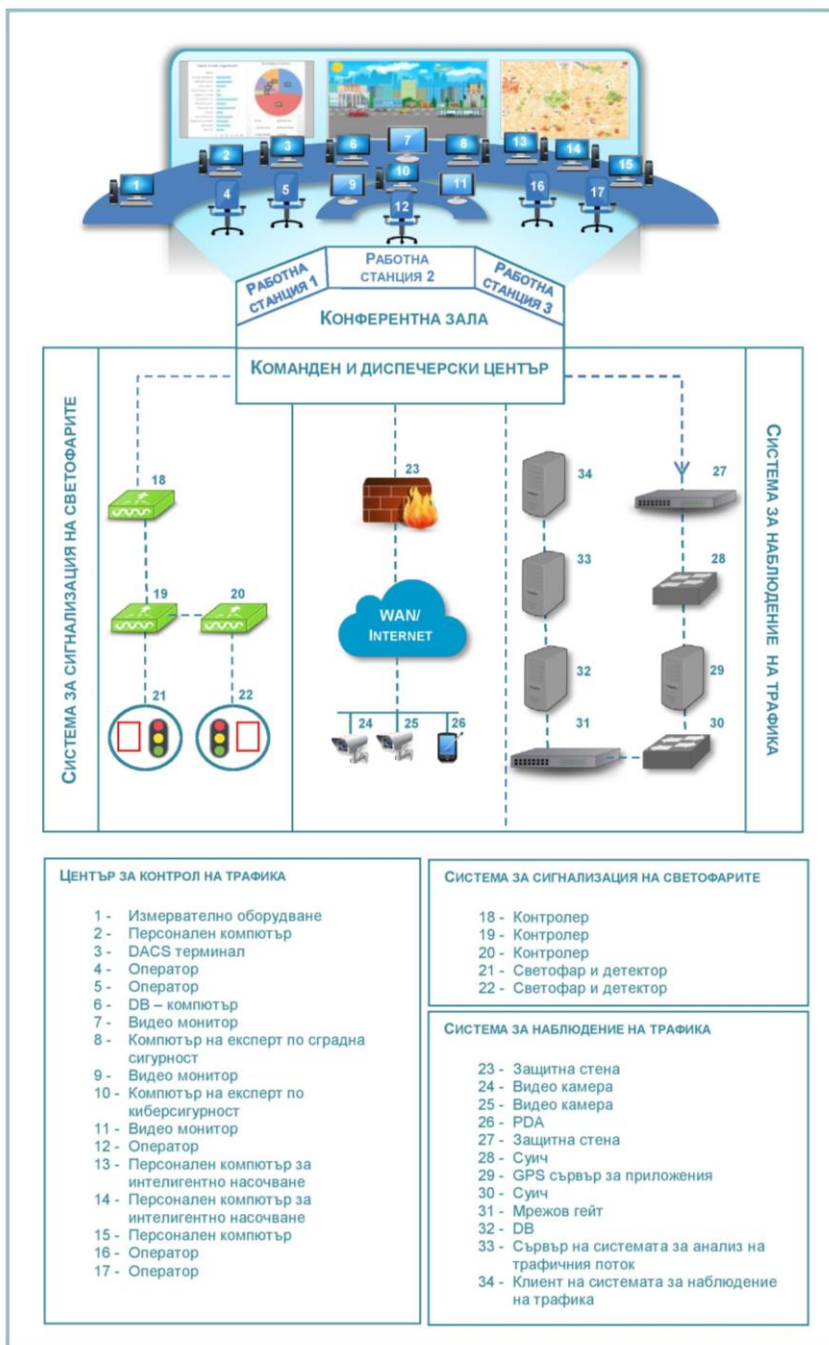
- *работни станции* - показват състоянието на сигналните контролери и детекторите на превозни средства, регулират параметрите за сигналните контролери и осъществяват достъп до правителствени база данни.
- *DB - компютър* – използва се за планиране на събития и управление на инциденти;
- *видео стена с големи размери* – за наблюдение в реално време.

Процесът на контрол се реализира чрез приложения за:

- **графична визуализация на работата и състоянието на всеки сигнал за контрол на трафика.**
- **управление на информацията за трафика** – за графично представяне на актуалната пътна обстановка.

Системите за управление на информация за трафика изчисляват трафичния поток през кръстовищата на база на данните, събирани от пътната инфраструктура. Възможностите за обмен на данни между центрове за контрол на трафика на различни транспортни системи спомагат за подобряване на стратегическото планиране и подпомагат процесите на вземане на решения, свързани с управление на трафика.

Фиг. 1 представлява схема на актуализирана функционална архитектура (част от оперативната архитектура) на класически Център за управление на транспорта, разработен от Министерството на транспорта в Мичиган. В конкретното изследване на градска автомобилна транспортна система е необходимо да бъде представена връзката между ЦКТ и Системата за сигнализация на светофарите, както и между ЦКТ и Системата за наблюдение на трафика. За по-голяма яснота схемата включва както функционална (компоненти от 23 до 26), така и техническа архитектура (компоненти от 27 до 34) на Системата за наблюдение на трафика.



Фигура 1. Функционална архитектура на класически център за управление на транспорта и в частност на трафика на градска автомобилна транспортна система.

Неговите основни компоненти са:

- **видео стена с големи размери** - за наблюдение в реално време.
- **конферентна зала** – тя представлява част от контролната зала.
- **команден и диспечерски център** – той представлява тази част от контролната зала, която отговаря за управлението на транспортни средства и за доставката на стоките и пратките до клиента, след като напуснат склада. Пакетираните пратки се разпределят на транспортните средства и след това се изпращат. Интегрираната

софтуерна информационна система ERP (Enterprise Resource Planning) получава обратна връзка под формата на доклад с цялата необходима информация [74].

Модулите в една подсистема могат да се обединят в две групи:

- **модули в централна подсистема за управление на трафика** - Централно управление на трафика и Централно управление на поддръжката;
- **модули в крайпътна подсистема за управление на трафика** - Крайпътен модул за събиране на данни за трафика, Крайпътен модул за управление на трафика, Крайпътен модул за събиране на данни за пътна настилка и околна среда.

По аналогичен начин физическите потоци с данни се разделят на:

- **физически потоци с данни в централна подсистема за управление на трафика;**
- **физически потоци с данни в крайпътна подсистема за управление на трафика .**

Необходимо е да бъдат изпълнени определени технически изисквания, чрез които:

- **да се осигури защитено предаване на данни** - крайпътните съоръжения и ЦКТ са двете крайни точки, между които се извършва пренос на данни от трафика.

Затова е необходимо данните да се криптират с технология SSL/TLS или друга аналогична на нея.

- **да се предотврати загуба на данни** – при необходимост информацията трябва да може да бъде изтеглена локално чрез компютър, като за целта пътната станция трябва да разполага с локален комуникационен интерфейс.
- **да се провери физическата свързаност** – чрез тестове.
- **да се осигури комуникационна съвместимост** – в случая интерфейсите на пътната станция за видеонаблюдение трябва да са съвместими с общата система за управление.
- **да се избегне платформена зависимост** – за целта софтуерът на системата се изгражда на модулен принцип.
- **да бъде възможен обмен на данни с външни системи и устройства** – това се взема предвид при разработка на софтуера.

На **Фиг. 2** е показана адаптивна архитектура на система за кибернетична защита, базирана на адаптивна архитектура за сигурност [46], въз основа на която следва да бъдат направени изводи за етапите при изграждане на цялостна и ефективна защита от кибер заплахи.

I. Прогнозиране

На този предварителен етап от планирането на киберсигурността основна задача е предвиждането на вероятните рискове, за да бъде постигнато впоследствие ефективно управление на риска чрез непрекъснат мониторинг и анализ на текущото състояние на процесите и системите. В практиката е необходимо да се прави ясно разграничение между понятията *риск* и *неопределеност*. За риск се говори в случаите, когато е възможно да бъдат количествено определени вероятностите за различни събития или изходи и самите събития са предсказуеми. В противен случай се прави оценка на неопределеността. *Информационната неопределеност*, произтичаща от недостатъчна или недостоверна информация, както и от погрешни допускания, е характерна за планирането на бъдещи събития. Прогнозираните неопределености могат да бъдат редуцирани чрез допълнително изследване, събиране на данни и анализ.



Фигура 2. Адаптивна архитектура на система за кибернетична защита.

Съществуват множество методи за анализ и количествена оценка на риска. На различните нива на вземане на решения се използват различни методи за анализ на риска в зависимост от конкретните цели.

- **Метод „дърво на решенията“;**
- **Метод за анализ чрез „дърво на събитията“;**
- **Метод за анализ чрез „дърво на грешките“;**
- **Метод, базиран на теорията на размитите множества;**
- **Метод Монте – Карло;**
- **Метод на общата вероятност.**
- **Метод на трите фактора (3F)**

Това е общоприет и широко използван метод за анализ и количествена оценка на риска, според който *рискът R* се дефинира като величина, съставена от произведението на три параметъра. Съществуват различни варианти на метода в зависимост от подбора на параметрите за оценка на риска.

Във формулата

$$R = P * E * C \quad (1)$$

P е вероятността да се случи инцидент; *E* е експозицията или продължителността на вредното въздействие върху даден обект, система или лице, която може да се обясни и като степен на застрашеност; *C* е потенциал за възникване на щети, който е показател за тежестта на последиците от инцидента (вид и размер на щетата), които от своя страна също са с вероятностен характер.

- **Експертен подход**

При този метод обобщената оценка на риска се основава на метода на трите фактора, като в конкретния случай стойностите на риска могат да бъдат изчислени на база на вероятността от нежелано събитие *P* и потенциала за възникване на щети *C* (степен на опасност *H*):

$$R = P * C \quad (2)$$

Управлението на риска във връзка с киберсигурността се изразява в:

- **предвиждане на възможните кибер заплахи, насочени към информационните системи в командните центрове на секторите от критичната инфраструктура.**
- **приемане на съответните мерки за превенция и минимизиране на нежелани последици в случай на детектирани кибератаки.**

Моделът на дейностите по управление на риска включва:

- А. Инициране на процеса;**
- Б. Дефиниране на средата (контекста);**
- В. Идентифициране на рисковете;**
- Г. Анализ на риска;**
- Д. Оценка на риска;**
- Е. Противодействие на риска;**
- Ж. Мониторинг и проследяване на процеса на управление на риска [15].**

II. Превенция

На този етап специално внимание се обръща на топологичния анализ на уязвимостите *TVA (Topological Vulnerability Analysis)*, чието редуциране е право пропорционално на минимизирането на риска от нежелани последици вследствие на инцидент. TVA идентифицира критичните уязвимости и осигурява стратегии за сигурност на активите чрез поддържане на ефективни мрежови защити в целия жизнен цикъл „защита – детектиране – реагиране“ (*protect – detect – react*).

Това включва:

- **идентифициране на критичните уязвимости;**
- **показатели за сигурност;**
- **редуциране на фалшивите тревоги за заплахи;**
- **планиране на мерките за реагиране в случай на атака.**

На *Фиг. 3* е проследен цялостният поток на TVA. Първоначално е построен концептуален модел на кибер заплахата („Триъгълник на кибер заплахата“ - The Cyber Threat Triangle), който показва взаимовръзките между данните за входната кибер заплаха, потенциалните уязвимости и мотивацията на атакуващия [70].



Фигура 3. Поток на TVA.

III. Детектиране

CTI е абревиатура за означаване на *Cyber Threats Intelligence*, което се характеризира със способността за разпознаване индикаторите на действията по време на всяка фаза от кибератаката и се отличава със следните основни предимства:

- *възможността атаката да бъде видяна в контекст;*
- *точност на детектиране и реагиране;*
- *по-бързо детектиране.*

IV. Реагиране

Съгласно материала „Концепция и стратегия за разработване на система за ранно реагиране на киберпрестъпления“, изготвен от Международната академия за обучение по кибер разследвания [37], *Системата за ранно реагиране* включва следните основни компоненти:

- *входни данни за кибер заплахи;*
- *платформа за споделяне на кибер заплахите;*
- *консултации за инцидентите, управление на инцидентите и анализ на данните.*

Основният бизнес процес по координиране на инциденти се състои от две части:

А. Процес за ранно предупреждение.

Б. Процес за конкурентно осигуряване на сигурност.

1.3. Системи за управление на транспорта

1.3.1. Същност и значение на транспортната система.

Като сектор от критичната инфраструктура, *транспортната система* представлява съвкупност от всички видове транспорт, транспортни средства, пътища, транспортни възли, складови бази и ремонтни предприятия.

В практиката понятията транспорт, спедиция и логистика често се употребяват съвместно поради тяхната взаимосвързаност. Ако транспортната система се разглежда като средство или елемент на логистиката, в описанието следва да бъдат включени и услуги по снабдяване, дистрибуция, приемане, съхранение, контрол на придвижването, ремонтни дейности и сервизно обслужване.

Логистиката на сигурността и отбраната е едно от направленията, в което намират широко приложение т. нар. *логистични транспортни системи*. Съществуването на това понятие се обуславя от факта, че процесът на транспортиране е част от цялостното функциониране на всяка логистична система.

Според Бялата книга за отбраната [2] за поддържане и развитие на отбранителните способности на страната е необходимо да се инвестира в изследвания, свързани с внедряване и използване на иновативни и високотехнологични решения, сред които и такива за подобряване на логистичното осигуряване.

Наред с логистичното осигуряване, транспортирането осигурява мобилността на формированията, тъй като според Доктрината за логистиката на БА то е средство за придвижване на сили, екипировка, оборудване, хора и запаси, включително и необходимото оборудване за товаро-разтоварни дейности, докато отговорността за изпълнението на военните превози и транспортирането при провеждане на операции на територията и акваторията на страната, е на изпълнителната власт, управленските и командни органи на въоръжените сили.

Ролята на транспортната система в този процес отново е свързана с осигуряване на средства (съоръжения, оборудване, транспортни средства от всякакъв тип) за извършване на специфични транспортни дейности по време на самата операция.

1.3.2. Видове транспорт и категории пътища

Видовете транспорт според Министерство на транспорта, информационните технологии и съобщенията на РБ са:

- **автомобилен транспорт** - според предназначението си автомобилите биват: *леки автомобили; товарни автомобили; автобуси; тролейбуси; специални.*
- **железопътен транспорт** - съвременните влакове могат да се класифицират по следния начин: *пътнически влакове; монорелс; товарни влакове; високоскоростни влакове; електрически мотрисни влакове (ЕМВ).*
- **въздушен транспорт** – в зависимост от предназначението си конвенционалните и висококапацитетните самолети се класифицират по следния начин: *пътнически; товарни (за превоз на товари и поща); комбинирани.*
- **воден транспорт** - водният транспорт се разделя на *морски и речен транспорт.*
- **комбиниран транспорт** - представлява интермодален транспорт, както е прието да се нарича превозът на товари, при които една транспортна единица или пътно превозно средство се използват без да се обработва товарът, с минимум два вида транспорт.

Пътищата попадат в следните три категории в зависимост от предназначението си: *автомагистрала; автомобилни пътища; „международна мрежа Е“ [1].*

1.3.3. Основни предимства и недостатъци на автомобилния транспорт

Автомобилният транспорт е избран да бъде обект на изследване в дисертационния труд поради това, че е основен вид транспорт, което се обуславя от следните му характеристики:

- *най-голям обхват на мрежата от автомобилни пътища;*
- *предлага най-голямо разнообразие от превозни средства в сравнение с останалите видове транспорт;*
- *отличава се с маневреност и сравнителна независимост от условията на околната среда (градска или извънградска);*
- *липсва забавяне поради голям обем начално-крайни операции.*

Освен, че е най-широко разпространен, автомобилният транспорт фигурира в статистиките като основен причинител на замърсяването на околната среда наред с енергетиката и индустрията, което се дължи на:

- *вида на използваното течно гориво и наличието на примеси в него;*
- *тип двигател (дизелов, бензинов и газов);*
- *конструкционни особености на автомобила;*
- *голяма продължителност на експлоатация;*
- *неизправно техническо състояние на автомобила;*
- *лоша пътна настилка;*
- *неблагоприятни метеорологични условия.*

Автомобилният трафик става причина за приблизително 25% от емисиите на въглероден диоксид (CO₂) в света. Авиацията допринася с 12% към замърсяванията причинени от транспорта като цяло (или 2.5% от общите емисии), а пътният транспорт - със 77%.

1.3.4. Развитие и въвеждане на Интелигентни транспортни системи

Стратегическата визия за ITS е като един интегратор на транспортни средства, комуникации и интермодалност в регионален мащаб. Основите на транспорта включват концепцията на транспортирането като комплексна система и рамка за нейния анализ [84]. Автоматизацията, комуникациите и вградената електроника допринасят за усъвършенстването на съвременните транспортни системи и осигуряват значителни предимства, като същевременно ги правят уязвими към въздействия, упражнявани посредством киберпространството.

Като основни компоненти на ITS, системите за контрол на сигнализацията и контролните центрове са изложени на потенциален риск да станат мишена на хакери, които могат да използват киберпространството като проводник на злонамерен софтуер [88].

1.3.5. Интегрирани компоненти на Автомобилна транспортна система

По отношение на градската транспортна среда съществува необходимост от системи за управление и контрол на градския трафик (*UTMC - Urban Traffic Management and Control System*), които представляват усъвършенствани системи за контрол на градския трафик (*UTC - Urban Traffic Control System*) и на практика са едни от най-важните компоненти на съвременните ITSs.

Рамката за UTMCS добавя актуализирани основни функции към съществуващите UTCS, както следва:

- *Система за адаптивен контрол на сигнализацията (ATSCS - Adaptive Traffic Signal Control System);*
- *Система за автоматично детектиране на инциденти (AIDS - Automatic Incident Detection System);*
- *Информация за трафика в реално време.*

Освен изброените компоненти има тенденция за добавяне на допълнителни функционалности, като например:

- *мониторинг и контрол на замърсяването на въздуха;*
- *приоритизация на публичния транспорт;*
- *използване на данни on-line с осигуряване високо ниво на киберсигурност.*

На база на всички изброени дотук предимства UTMCS може да бъде дефинирана като градска транспортна система от следващо поколение.

Структурата на една конвенционална съвременна ATS включва следните компоненти:

- *Системи за контрол на сигнализацията (TSCS - Traffic Signal Control Systems)* – координират сигнализацията на светофарите. Тези системи се състоят от: *светофари; комуникационна мрежа; централен компютър или компютърна мрежа.*
- *Системи за управление на магистралите (FMS - Freeway Management Systems)* - управлението на магистралите включва:
 - *Център за управление (FMC - Freeway Management Center);*
 - *връзки към други ITS – компоненти в градския район [85].*
- *Системи за управление на транзита (TMSs - Transit Management Systems)* – включват технологии за автоматична локация на превозното средство (AVL) и компютърно-базиран диспечерски системи в помощ на автобусите при спазване на графика и цялостно подобряване на обслужването [50].
- *Софтуер за управление на транзита (TMS - Transit-management Software)* – оптимизира използването на всички приложени технологии и представлява част от

интегрирана система за управление, която се намира в Центъра за управление на транспорта/ транзита [72].

- **GPS (Global Positioning System) – базирани системи** – използват GPS-проследяване и GPRS-пренос на данни чрез мобилен оператор. Наблюдението и контрола на всяко превозно средство се извършва от компактно GPS-устройство, съставено от GPS-приемник и GPRS-модул. Всеки автомобил може да бъде наблюдаван от компютър с достъп до Интернет.

- **Системи за видеонаблюдение (VSS - Video Surveillance System)** – извършват безжичен пренос на видео сигнали от превозните средства в реално време. Основните им компоненти са видео камери и GPS-модул за навигация, свързан към цифров видеорекодер, чийто изход на свой ред е свързан към радио-модем. Системата за наблюдение и мониторинг използва глобалните мобилни мрежи, като трансферът на видео чрез криптирана връзка се извършва чрез GPRS – 3D.

Подсистемите на физическата архитектура на ITS се обединяват в следните класове: центрове, области, превозни средства, пътници [76]. Схемата на **Фиг. 5** съдържа основните подсистеми, разпределени по класове.

1.3.6. Външни въздействия върху функционирането на ITS

ITSs функционират в среда, която се характеризира с различни опасности, като в настоящото изследване обект на анализ са **физическите заплахи и кибер заплахи (вируси; зловреден софтуер и уеб атака)**.

Най-честата форма на кибератака е DoS (Denial-of-Service), в която нападателят претоварва сървъра, изпращайки толкова интензивен трафик (flooding), че потребителски заявки не могат да бъдат обработени. По своята същност DoS - атаката представлява изпращане на множество пингове към целеви компютър.

Друга форма на DoS - атака е свръх експлоатацията на системни ресурси (централен процесор, памет или структури от данни, съхранявани в паметта), което води до повреда или пълен отказ на системата. Повредата на мрежово устройство (защитна стена, рутер, суич) също причинява претоварване на мрежата поради усилен трафик, което на свой ред води до преустановяване работата на системата. Още по-сериозна е заплахата от DDoS - атаките, защото нападателят използва не само един, а множество компютри [43].

По отношение на транспортните системи светофарите са особено уязвими за DDoS - атаките. Най-често срещаната заплаха към транспортните центрове за управление е зловреден софтуер, който е в състояние да причини щети на системата дори в случаите, когато нейният център не е свързан към Интернет. Портативни мултимедийни плейъри, мобилни телефони, както и компакт дискове могат да бъдат проводници на зловреден софтуер [48].

Специфичен тип атака в голяма степен наподобява семантично хакерство. Първоначално нападателят получава достъп до транспортния център за управление, комуникационната връзка за предаване на сигнала или контролера на светофара. След това той манипулира управляващите сигнали по начин, който не е твърде очевиден, например чрез намаляване или увеличаване на продължителността на сигнала на зелената светлина в сравнение със сигнала при референтния модел, който в известен смисъл е оптимизиран.

Това е форма на ATP (Advanced Persistent Threat) - сравнително нов клас кибер заплахи, които имат някои определени характеристики, отличаващи ги от традиционните заплахи, като например: специфични и ясно дефинирани цели; високо

организиран и добре обезпечен от гледна точка на ресурси нападатели; дълъг латентен период; трудни за детектиране



Фигура 5. Физическа архитектура на ITS.

1.3.7. Характеристики на основни видове системи за управление на транспорта

Логистичното осигуряване на видовете товари при транспортирането им е свързано с изпълнение на дейности по планиране, организация, управление и контрол. По своята същност системите за управление на транспорта представляват софтуерна платформа, чието предназначение е да предостави инструменти за наблюдение и контрол на веригите за доставки.

Веригата за доставки включва **компоненти** (транспорт, превозвачи, търговци, доставчици, ръководен екип, материални и нематериални ресурси) и **услуги** (складиране, закупуване, обслужване на клиенти и реализиране на продажби).

В зависимост от методите за доставка се различават два вида системи за управление на транспорта:

- **местен софтуер** – спедиторите извършват инсталиране и поддръжка на софтуера на сървърите в помещения;
- **облачно базиран софтуер като услуга (SaaS – Software as a Service)** – проектиран е да работи на един сървър (облака на доставчика) и да се използва от спедиторите.

Основните критерии за оценка на системите за управление на транспорта са:

- **осигуряване на по-голяма функционалност на транспорта;**
- **редуциране на финансовите разходи;**
- **минимизиране на риска;**
- **по-бързо и лесно персонализиране.**

Допълнителни критерии за оценка, които осигуряват предимство на системите за управление на транспорта от гледна точка на потребителите, са:

- **възможност за интегриране с ERP платформи** – позволява пълно свързване на веригите за доставка, удовлетворява потребностите, свързани с интегриране и цялостно планиране, управление, контрол и анализ. Това са мултифункционални продукти, които гарантират сигурност и надеждност, както и достъпност на информационните ресурси независимо от локацията.
- **използване на интерфейсен портал за сътрудничество** – дава възможност за входящо и изходящо управление на графици за назначаване, както и за бързо и сигурно проследяване на транспортните движения до клиентите.
- **динамично SQL SSRS (Server Reporting Services) - отчитане** – услугите за отчет дават възможност за създаване и споделяне на интерактивни карти, таблична и графична информация и др.

Диаграмата на **Фиг. 6** представя обобщена статистическа информация за потреблението на конкретни системи за управление на транспорта, събрана чрез проучване на мненията на потребителите [96].

ИЗВОДИ ОТ ПЪРВА ГЛАВА

1. За своевременно идентифициране на кибер заплахите с цел предотвратяването им е целесъобразно да се прилага методът на сценариите (т. 1.1.).
2. Правилното функциониране на системите за управление на транспорта и на транспортните системи като цяло зависи основно от устойчивостта на центровете за контрол на трафика и степента им на защитеност към кибератаки (т. 1.2.).
3. За оценката на риска от кибер заплахи и определяне на устойчивостта на ЦКТ, респективно на системата за управление на транспорта е удачно да се прилага метода на трите фактора (т. 1.2.), тъй като дава възможност за отчитане на системната уязвимост.
4. След анализ на всички видове транспорт автомобилният транспорт е избран като най-подходящ за провеждане на експерименталните изследвания поради своите предимства и недостатъци (т. 1.3.3.).

ВТОРА ГЛАВА.

МОДЕЛИРАНЕ НА ВЪЗДЕЙСТВИЕТО НА КИБЕР ЗАПЛАХИ ВЪРХУ СИСТЕМА ЗА УПРАВЛЕНИЕ НА ТРАНСПОРТА

2.1. Моделиране на сложни системи

2.1.1. Възможности и ограничения на моделирането на сложни системи

Сложните или комплексни системи по своята същност са съставни и включват множество подсистеми, които взаимодействат помежду си, като по този начин добавят нови свойства към цялостната система. Това съвместно действие или взаимоотношение се нарича синергизъм и се изразява в това, че крайният ефект или отговор е различен или по-голям от сумата на ефектите, предизвикани поотделно от всеки агент.

В общия случай процесът на моделиране се изразява в създаване на *модел* на реален обект (система), извършването на експерименти с него и анализ на получените резултати в случаите, когато реалният обект не може да бъде подложен на непосредствено изучаване. Моделът представлява достоверно изображение на реален обект, система или понятие във форма, различна от реалното му съществуване, на база на което се извършват наблюдения и изследвания с познавателна цел.

Процесът на моделиране се подчинява на следните основни принципи:

- **Принцип на информационната достатъчност;**
- **Принцип на осъществимостта;**
- **Принцип на множеството от модели;**
- **Принцип на агрегирането;**
- **Принцип на параметризацията.**

Съществуват различни класификации на моделите според подхода за създаването им, структурата и предназначението им. Най-общо те се обединяват в два големи класа:

- **веществени;**
- **символни.**

Според друга базова класификация моделите се разделят на:

- **механични** – те трябва да притежават колкото е възможно повече съществени характеристики на реалната система в резултат от наблюдението ѝ, за да бъдат в състояние да предвидят нейното бъдещо поведение при нормално функциониране, както и да предскажат как тя би работила под въздействие на нежелани външни въздействия.
- **емпирични** – представляват математически функции, които се използват, когато информацията за структурната свързаност и функционалните механизми на системата не е достатъчна поради нейната сложност. Необходимо е да се създадат хипотези въз основа на външни системни характеристики. Структурата се определя от наблюдаваните взаимовръзки между експерименталните данни.

Математическите модели се причисляват към т. нар. символни модели, които пресъздават реалния обект с помощта на символи (схеми, чертежи, системи уравнения) и се разделят на следните две групи:

- **детерминирани** – зависимостите в обекта, които са предмет на изследването, имат строго определен и неизменен във времето характер.
- **статистически** – зависимостите в обекта са под влияние на случайни фактори.

За целите на съвременните научни изследвания широко се използва **компютърното моделиране**, чиято основна разновидност е **симуляционното**

моделиране. *Симулационният модел* представлява сложен математически алгоритъм, който може да се дефинира като точно и еднозначно описана крайна последователност от действия над определени входни данни, която винаги води до резултат, намиращ се във функционална зависимост от данните, постъпили на входа на системата.

Симулационните модели могат да се класифицират по следния начин:

- **непрекъснато изменящи се модели** - модели, чиито изменения се осъществяват по непрекъснат начин.
- **дискретно изменящи се модели** - модели, чиито изменения стават дискретно във времето. Измененията в състоянието на системата се разглеждат като последователно настъпващи състояния, които могат да се разграничат едно от друго.
- **смесени** - комбинация от първите два. Подходящи са, когато анализаторът изучава система, която може да се опише като група от непрекъснати потоци от информация, ресурси и т.н.

Симулационните модели предоставят големи възможности за:

- Извличане на изводи за нова система без да се налага да се построи реално, или да се направят промени в съществуваща без да се разстройва работата ѝ.
- Визуализиране операциите на нова или съществуваща система при различни условия.
- Изследване на начина за осъществяване на взаимодействие между отделните компоненти на системата и как това влияе върху общата системна производителност.
- Диагностика на изследваната система и регистриране на неизправности и проблеми.
- Разработване на специфични политики.
- Повишаване ефективността на системата като цяло.

Поради гореизброените предимства на симулационните модели, те намират приложения при:

- Усъвършенстване и модифициране на системи.
- Оптимизация на функционирането на сложни системи и процеси.
- Подпомагане процеса на проектиране.
- Намиране на алтернативни решения.
- Прогнозиране.
- Изучаване на околната среда.
- Изследване и възпроизвеждане на процеси, които са невидими за човешкото око.

Компютърно подпомагано учение (КПУ) за укрепване на гражданската сигурност е едно от най-актуалните приложения на симулационното моделиране в съвременните условия.

Прилагането на компютърните симулационни модели е свързано с въвеждане на следните ограничения:

- Симулационните модели не могат да оперират с неточни входни данни – на практика в модела могат да бъдат въведени и некоректни входни данни, но това би довело до генерирани на изходни данни, които не са удовлетворителни. Това е начин да се установи как системата функционира в ситуации, в каквито не е желателно реалната система да работи.
- Симулационните модели не могат да бъдат използвани за описание на системни характеристики, които не са изначално заложили в модела.
- Симулационните модели не генерират решения на проблеми, а само подпомагат процеса на вземане на решение с информацията, която предоставят.

2.1.2. Методи за моделиране

Под *метод* в симулационното моделиране се има предвид основната рамка за свеждане на една реална система до нейния модел на база на правила и условия за построяване на модела (програмен език). Изборът на метод зависи от системата, която ще бъде моделирана и от целта на моделирането.

Аналогично на основните видове математически модели, методите за моделиране най-общо се разделят на две големи групи:

- **детерминирани** – създава се базов модел, чрез който реалните процеси в обекта се изследват и описват аналитично.
- **статистически** – дават възможност характеристиките на обекта да се оценяват от две позиции: от позицията на средните (номинални) стойности на параметрите и от позицията на статистическите им характеристики. Базира се на методи от теория на вероятностите, статистиката и корелационно-регресионния анализ. Методът Монте-Карло е основен метод за статистически изпитания. Той се изразява в многократни изпитвания на обекта - варианти на анализа му, при което се задават случайни стойности на работните характеристики на процесите в обекта и се отчитат съответните реакции.

Конкретно по отношение на симулационното моделиране, първата стъпка е създаване на материален програмен модел на базата на начален *концептуален модел*, който представлява абстрактен модел, определящ структурата на моделираната система, свойствата на нейните елементи и причинно-следствените връзки, присъщи на системата и съществени за постигане на целите на моделирането.

Построяването на концептуалния модел се извършва на няколко етапа:

1) *Определяне типа на системата*

- **статична или динамична** - според признака мощност на множеството от състояния;
- **динамични системи с дискретни състояния** (множеството от състояния е крайно или изброимо) и **системи с непрекъснато множество от състояния** [52], [53].
- **детерминирана или стохастична** - в зависимост от движението на системата (смяната на състоянията).

2) *Описание на работното натоварване* - представлява съвкупност от външни въздействия, оказващи влияние върху ефективността от използването на дадена система в рамките на провеждана операция.

3) *Декомпозиране на системата* - извършва се в съответствие с избраното ниво за детайлизация на модела, което се определя от: *поставените цели, информационния обем, изискванията към точността и достоверността на изходните резултати*.

Най-иновативният и ефективен метод за създаване на интерактивни симулации е агентно-базираното моделиране. За целта са необходими мощни компютри. В зависимост от степента на човешко участие се различават два вида симулации: *отворена (интерактивна)* и *затворена симулация*. При отворената симулация потребителят може да влияе върху алгоритъма в реално време. Интерактивни компютърни симулации могат да бъдат създадени посредством езици за програмиране (Java, C++), специализирани езици за симулации, софтуерни продукти за компютърни анимации (Flash) и т.н. При затворената симулация потребителят не може да оказва влияние върху симулационния алгоритъм в реално време.

2.1.3. Симулационни методи и инструментални средства за подпомагане моделирането на сложни системи

Формулировката на темата на дисертационния труд предполага да бъде направено цялостно теоретично и експериментално изследване на въздействието на кибератака върху система за управление на транспорта, което освен моделиране на ЦКТ и симулиране на въздействието на определен тип атака върху него, трябва да включва и оценка на риска от кибератаки.

Независимо от вече направената в предходната т. 2.2.2 класификация на съвременните симулационни методи, с най-широко приложение в практиката са следните симулационни методи:

- **емпиричен метод** – прилага се при научни изследвания, които имат за цел събиране на знание чрез директно или индиректно наблюдение, опит или експеримент.
- **експериментален метод** – представлява вид емпиричен метод, при който данните се добиват чрез задаване на различни стойности на променливи и наблюдаване на настъпващите изменения.
- **стохастичен метод** – при този метод времето е основният параметър, от който зависят случайно избраните числени резултати от вероятностни разпределения.
- **аналитичен метод** – основава се на анализ (логически, математически, комплексен), който представлява разделяне на цялото на съставни части с цел опознаване или натрупване на практически опит за обект или система.
- **динамичен метод** – изразява се в представяне на динамични взаимодействия между елементите в изследваната система, като дава възможност за отчитане на вероятностния характер на определени елементи.

Настоящото изследване се характеризира с приложението на методи или отделни техни етапи и разновидности, както следва:

- **емпиричен метод** – формиране (наблюдение) и формулиране (индукция) на работна хипотеза; твърдения относно последствията от хипотезата под формата на проверяеми прогнози (дедукция); експериментално доказване на хипотезата (проверка); оценяване на резултатите от проверката (оценка).
- **експериментален метод** – изразява се в провеждане на няколко серии от експерименти с избраните софтуерни продукти за симулационно моделиране.
- **стохастичен метод** – в използваните продукти за симулационно моделиране времето и продължителността на симулацията са основни входни параметри, които се въвеждат преди стартиране на симулацията и от които генерираните резултати пряко зависят.
- **динамичен метод** – използваните симулационни продукти предоставят възможност за отчитане на взаимодействията между елементите на изследваните сложни системи.
- **логически анализ** – прилага се при формулиране на обобщени оценки на резултатите, които са поместени в края на всеки проведен експеримент с оглед на по-голяма яснота при тълкуване на предхождащите го графики и таблици.

Емпиричният и в частност експерименталният метод са основните, които авторът прилага директно в разработката предвид, че оценките и анализите в нея се базират на експериментални резултати от симулационно моделиране.

Симулационното моделиране съществено допринася за укрепване на сигурността основно на етапите прогнозиране и планиране на заплахы от различен характер. При

една симулационна война (кибервойна) самите симулационни модели могат да станат обект на семантично хакерство и да бъдат така манипулирани, че неосезаемо да генерират неверни резултати при привидно правилно функциониране. При недостатъчно ефективни мерки за сигурност обект на кибератаки могат да станат симулатори с приложение в различни области.

Симулационното моделиране на кибератаки върху критична инфраструктура е направление, което позволява да се прилагат иновативни методи и решения. Съществуват различни софтуерни продукти за симулация и визуализация на процеси (технологични, индустриални, физични, математични, биологични, химични и др.), даващи възможност да се изследва самата атака и нанесените щети в зависимост от нейния характер и продължителност.

2.1.4. Методи за оценка на чувствителността и неопределеността в процеса на моделиране

- **Анализ на чувствителността (sensitivity analysis)** - за да бъде сведено до минимум нивото на неопределеност, трябва да бъде взета предвид реакцията на модела при различни по сила и характер промени, отклонения или външни въздействия, които могат да постъпят под формата на грешки във входните данни, т.е. неговата **чувствителност**. Методите за оценка и анализ на чувствителността в процеса на моделирането могат да бъдат класифицирани, както следва: *предварителни методи; локални методи; математически методи; статистически методи; графични методи.*
- **Анализ на неопределеността** - използва вероятните описания на входовете и дава възможност да бъдат получени разпределенията на вероятностите на резултатите от моделирането и индексите на системната ефективност. Неопределеностите могат да бъдат класифицирани, както следва:
 - *неопределеност на знанията (knowledge uncertainty);*
 - *естествена изменчивост (natural variability);*
 - *неопределеност на решението (decision uncertainty) [78].*

2.1.5. Верификация и валидиране на моделите

Последователните етапи при изграждане на симулационен модел на система или процес са:

- **Формиране замисъла на модела;**
- **Формулиране на задачата;**
- **Оформяне на концепцията на модела;**
- **Реализация чрез съответен софтуер за симулационно моделиране;**
- **Верификация и валидиране** - при използване на симулационното моделиране за изследване на даден обект или система се изисква да бъде извършена проверка доколко моделът е адекватен и дали може да бъде коригиран при регистриране на неточности и грешки в процеса на симулация.
- **Използване на модела** - *еднократно* - докато се вземе решение; *текущо* - използва се постоянно за обучение.

2.2. Моделиране на въздействието на кибер заплахи върху система за управление на транспорта с използване на специализиран симулационен софтуер

2.2.1. Моделиране и оценка на въздействието на DoS - атака върху Център за контрол на трафика на градска автомобилна транспортна система

Центърът за контрол на трафика (ЦКТ) е „сърцето“ на Системата за управление на трафика, където управлението на трафика се изпълнява чрез вземане на решения, както и допълнителни услуги и операции. ЦКТ отговаря за получаването, наблюдението и анализа на информацията за пътните условия.

Основните услуги, свързани с управлението на трафика, са: *планиране, функциониране, анализ* [87].

Моделът на Център за контрол на трафика е изграден от автора в симулационната среда Riverbed Modeler Academic Edition 17.5 след подробно проучване на функционалната организация и мрежовите конфигурации на съществуващи контролни центрове. Създаден е модел на типичен ЦКТ според концептуалната архитектура на един от лидерите в областта – Huawei [59].

Авторът е избрал да симулира DoS - атака към ЦКТ на градска автомобилна транспортна система, защото според статистиките този тип атаки върху компютърните системи, които са свързани с Интернет, са най-широко разпространени.

Едно от основните предимства на модела е, че дава възможност за успешно стартиране и изпълнение на симулацията без регистриране на софтуерни грешки и проблеми, тъй като направените експериментални тестове показват, че това не би се получило при неправилен подбор на устройствата, несъвместимост между тях или некоректното им свързване в мрежа. В допълнение избраната от автора топология тип „шина“ е много често използвана при изграждане на контролни центрове в реални условия според предварително проучените източници.

2.2.1.1. Същност и характеристики на използваните в симулационния модел мрежови устройства и компоненти

Версията на симулационния софтуер, предназначена за изследователски цели (Riverbed Modeler Academic Edition 17.5) дава на моделиращия възможност да избира измежду множество реални типове и модели мрежови устройства и компоненти, които се представят като „възли и връзки“ и могат да бъдат конфигурирани чрез задаване на съответни технически параметри [90].

Авторът е избрал този симулационен софтуер за изследването, защото генерираните резултати са достоверни и не се налага непременно да бъдат сравнявани с резултати, измерени при провеждане на експерименти с реален хардуерен прототип.

Проектираната от автора мрежова конфигурация в симулационната среда Riverbed Modeler Academic Edition 17.5 се базира на проучване на практически реализирани Центрове за контрол на трафика и включва:

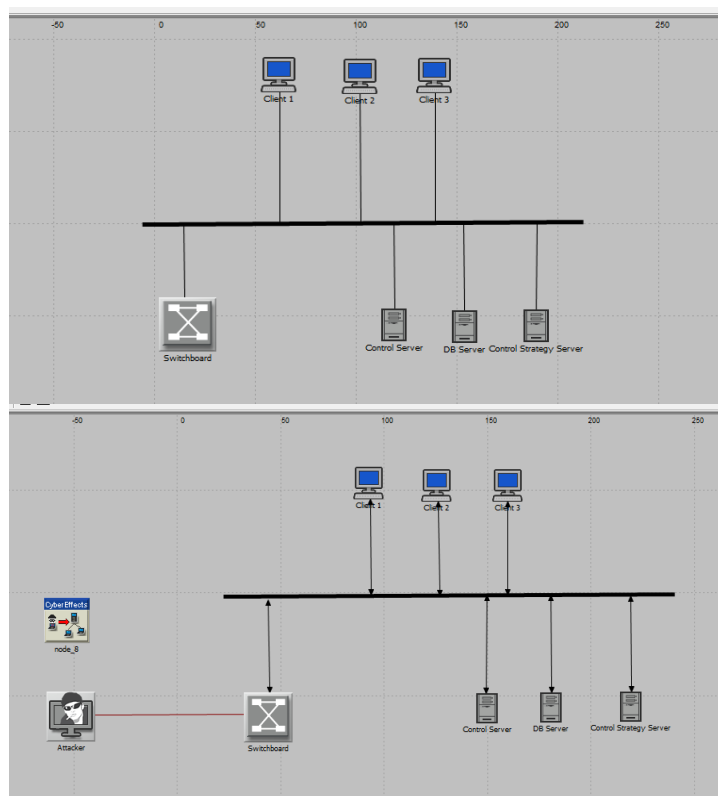
- **Работни станции** - в симулационния модел авторът е избрал да свърже три работни станции от типа **ethcoax_station** към шина **eth_coax_adv** с кабел **eth_tap** съгласно изискванията за съвместимост на физическите компоненти в линейна шинна мрежа.
- **Сървъри** - в симулационния модел свързаните сървъри са три от типа **ethernet_server_adv**: контролен сървър, сървър за съхранение на БД и сървър за стратегически контрол в смисъл на оперативен контрол, който се изразява във формирането и изпълнението на стратегическите планове.

- *TCP: Minimum Available Bandwidth > Auto-Calculate* – това е минималният наличен трафик (в bps).
- *IP: IP Host Parameters > Default* – това са параметри за адресиране и препращане на IP хост, тъй като IP разпознава логическите интерфейси на хостовете по техния IP адрес, който представлява уникален номер.
- *IP: IP Processing Information > Default* – този атрибут описва средата, използвана от централния процесор. Скоростта на услугата показва максималната скорост на препращане на този процесор (в packets/s или bps). От размера на паметта се определя каква част от нея е заделена за съхраняване на пакети за препращане.

• **Физически компоненти на мрежата** – при изграждане на мрежовата конфигурация е използван съвременен суич от типа **ethernet 128_switch_adv** с оглед на това, че в повечето практически реализирани конфигурации се използва суич.

При моделиране въздействието на кибер заплаха върху моделирания в симулационната среда ЦКТ са приложени кибер въздействия чрез конфигурацията **cyber_effects_attrib_definer**. Връзката между работната станция на атакуващия (**cyber_ethernet_wkstn_adv**) и суича (**ethernet 128_switch_adv**) е от типа **10BaseT_adv**, тъй като тази спецификация широко се използва в локални мрежи от всички размери.

На **Фиг. 14** са представени „screenshots” съответно на т.нар. референтен модел в нормално състояние (M_{Ref}) и на същия модел под въздействие на DoS - атака (C).



Фигура 14. Модел на ЦКТ съответно в нормално състояние и под въздействие на DoS - атака.

В симулационния модел са зададени настройки само на необходимите и оптимални за стартиране на симулацията входни параметри. Авторът е избрал да работи със съвременни, но конвенционални мрежови устройства. Настройките на параметрите на суича и сървърите са приети по подразбиране с оглед на конкретен и

еднозначен последващ анализ, базиран единствено на оценката на въздействието на кибер заплахата без отчитане на допълнителни външни и вътрешни фактори.

В **Таблица 3** се съдържат генерираните резултати от симулацията за максималните стойности на изпратения и получения трафик в зависимост от времето на пристигане при M_{Ref} и при кибератака C .

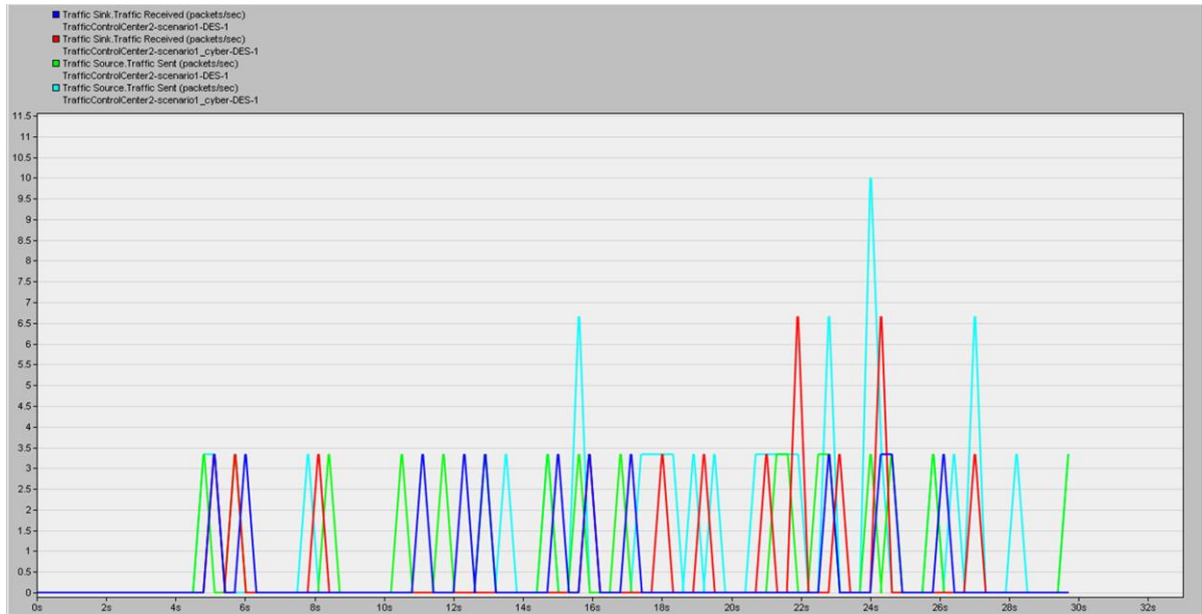
Таблица 3. Данни за пиковите стойности на изпратения и получения трафик в зависимост от времето на пристигане в случаите M_{Ref} и C .

Сценарии	T [s]	M_{Ref}		C	
		$T_{S, max}$ [packets/s]	$T_{R, max}$ [packets/s]	$T_{S, max}$ [packets/s]	$T_{R, max}$ [packets/s]
1	2	3.3	3.3	10	6.7
2	1	3.3	3.3	10	6.7
3	0.5	6.7	10	10	13.5
4	0.25	13.5	13.5	16.5	13.5
5	0.2	20	20	16.8	13.5
6	0.15	27	23	27	13.5
7	0.1	26.5	20	33.5	20
8	0.05	44	40	44	37
9	0.025	80	50	80	50
10	0.02	90	84	84	58

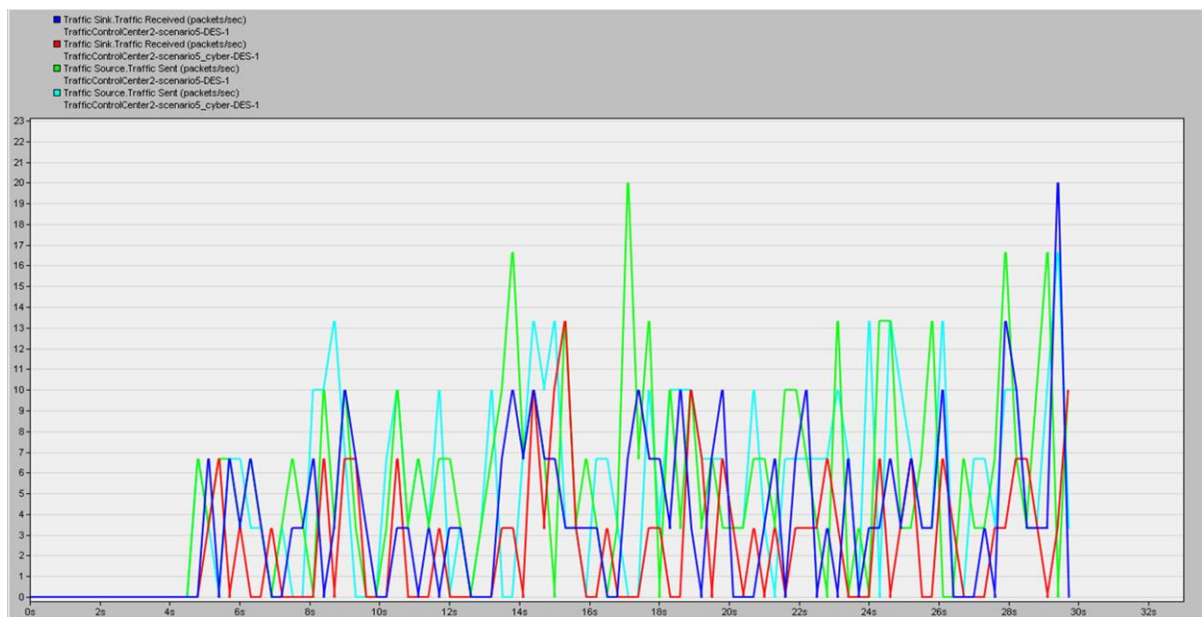
От сравнителните графики, показани на **Фиг. 15, 16 и 17** се вижда на коя секунда от изпълнение на симулацията са регистрирани пикови стойности за изпратения и получения трафик при модела в регулярен режим M_{Ref} и под въздействие на кибератаката C .

Таблица 4 съдържа обобщените резултати от трите графики, които показват в кои времеви диапазони R в [s] са регистрирани пиковете на изпратения и получения трафик, като функции на избраните три стойности на времето на пристигане ($T_1 = 2$ [s], $T_2 = 0.2$ [s] и $T_3 = 0.02$ [s]) съответно за референтния модел M_{Ref} и при кибератаката C .

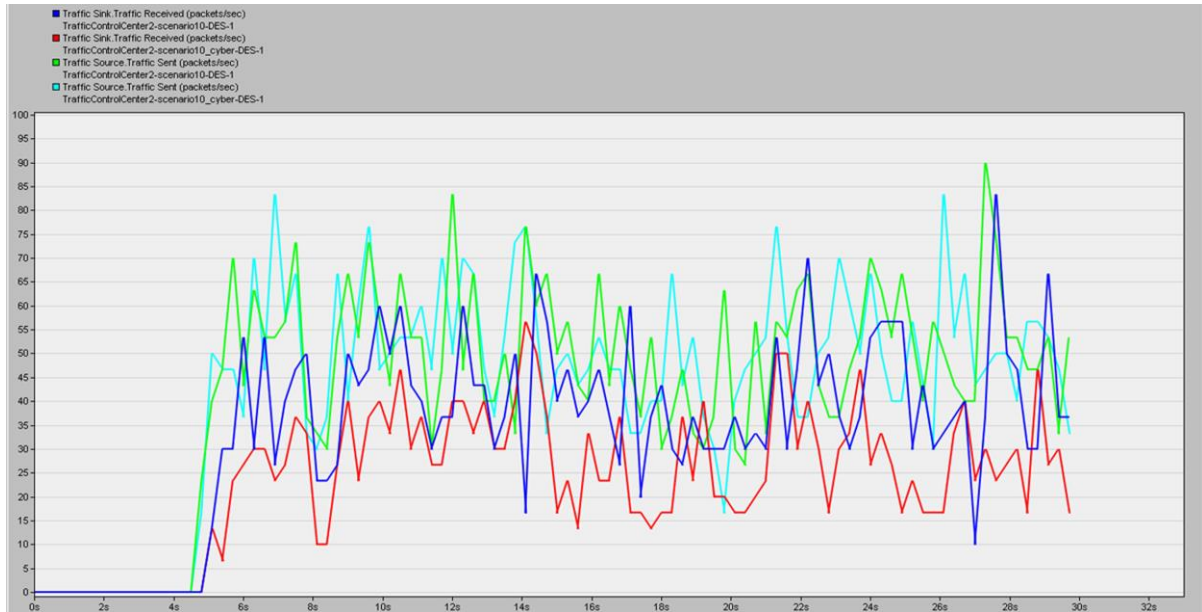
Продължителността на симулацията $D = 30$ [s] е разделена на шест времеви диапазона R , всеки от които е с продължителност 5 [s].



Фигура 15. $T_S = f(T)$ и $T_R = f(T)$ при $T = 2$ [s].



Фигура 16. $T_S = f(T)$ и $T_R = f(T)$ при $T = 0.2$ [s].



Фигура 17. $T_S = f(T)$ и $T_R = f(T)$ при $T = 0.02$ [s].

Таблица 4. Стойности на изпратения и получения трафик, като функции на T , регистрирани във времеви диапазони R , съответно за M_{Ref} и C .

R [s]	T ₁				T ₂				T ₃			
	M _{Ref}		C		M _{Ref}		C		M _{Ref}		C	
	T _{S, max}	T _{R, max}	T _{S, max}	T _{R, max}	T _{S, max}	T _{R, max}	T _{S, max}	T _{R, max}	T _{S, max}	T _{R, max}	T _{S, max}	T _{R, max}
[1, 5]	3.3	3.3	3.3	0	3.3	3.3	3	3	45	10	50	13
[5, 10]	3.3	3.3	3.3	3.3	10	10	13.5	6.7	73	60	84	37
[10,15]	3.3	3.3	3.3	0	16.7	10	13.5	10	84	66	76	56
[15, 20]	3.3	3.3	6.7	3.3	20	10	13.5	13.5	66	60	66	40
[20, 25]	3.3	3.3	10	6.7	13.5	6.7	13.5	6.7	70	70	76	50
[25, 30]	3.3	3.3	6.7	3.3	16.7	20	16.7	10	90	84	85	47

Обобщена оценка на резултатите

На база на табличните и графичните резултати може да се направят следните изводи. Под въздействие на кибератаката в интервала [25, 30] при зададено време на пристигане $T_3 = 0.02$ [s] се вижда, че броят на получените в сравнение с изпратените пакети ($T_{R, max}/T_{S, max}$) намалява с около 45 %, докато при M_{Ref} получените пакети са само със 7 % по-малко от изпратените. Може да се направи извод, че под въздействие на кибератаката се наблюдава проблем при получаване на изпратените пакети.

При $T_2 = 0.2$ [s] в същия времеви диапазон под въздействие на кибератаката броят на получените към изпратените пакети ($T_{R, max}/T_{S, max}$) намалява с 40 %, докато при M_{Ref} се наблюдава по-голям брой на получените пакети в сравнение с изпратените. Но пиковите стойности при $T_2 = 0.2$ [s] за M_{Ref} са регистрирани във времевия диапазон [15, 20], като в този случай броят на получените в сравнение с изпратените пакети ($T_{R, max}/T_{S, max}$) намалява с 50 %. Следователно, авторът прави допускането, че пакетите са

пристигнали със закъснение в интервала от 20-та до 30 - та секунда без това да свидетелства за неправилно функциониране на мрежата.

При $T_1 = 2$ [s] в същия времеви диапазон под въздействие на кибератаката броят на получените към изпратените пакети ($T_{R, \max}/T_{S, \max}$) намалява с близо 50 %, докато при M_{Ref} броят на получените пакети е равен на изпратените. Пиковите стойности в този случай са във времеви диапазон [20, 25], когато броят на получените пакети намалява с 36 % в сравнение с изпратените. Считано от 15 – та до 30 – та секунда, броят на получените пакети намалява с около 43 % в сравнение с изпратените. Следователно, в този случай пакетите не са получени дори с известно закъснение и е очевидно въздействието на кибератаката.

2.2.2. Моделиране и оценка на въздействието на DoS – атака върху системата за сигнализация на градска автомобилна транспортна система

Получените резултати от симулацията с Riverbed Modeler Academic Edition 17.5 създават предпоставки за разширен анализ на въздействието на DoS – атаката. Необходимо е да се направи разглеждане за случай, при който наводняването на сървъра със заявки води до възпрепятстване и спиране на работата му, което причинява нарушения в нормалната сигнализация на светофарите и пълното спиране на работата им.

Преходът между двете изследвания представлява логическа връзка от тип логическо следване (импликация), което се налага от обстоятелството, че за цялостното изследване на системата за управление на транспорта са комбинирани два различни софтуерни продукта за симулационно моделиране. Riverbed Modeler Academic Edition 17.5 показва въздействието на DoS – атаката върху ЦКТ на мрежово ниво, докато Aimsun 8.0 дава възможност да се направят логически допускания за начина, по който нейното деструктивно действие продължава върху системата за сигнализация на светофарите, след като сървърът вече е преустановил работа.

В подкрепа на твърденията за хода и последиците от DoS – атаката върху ATS авторът е избрал да се позове на изследванията на Prof. J. Alex Halderman от Мичиганския университет в областта на компютърната сигурност, извършени със съдействието на пътна агенция в Мичиган [51].

Концепцията на експерименталното изследване има за цел да покаже сравнителна характеристика между генерираните изходни данни от използването на референтен модел в регулярен режим и съответно под въздействието на кибер заплаха. Обмислен е частен случай на потенциални нарушения на светлинната сигнализация вследствие на кибер заплаха върху конкретна транспортна система. Използваният референтен симулационен модел е резултат от ефективната работа на група учени, изследващи автомобилния трафик в градска среда и оптимизацията му [38], [102].

Софтуерът Aimsun 8.0 има три компонента, които позволяват динамични симулации - Microscopic Simulator, Mesoscopic Simulator и Hybrid Simulator. Те дават възможност за симулация на различни трафични мрежи (градски мрежи, магистрали, околоръстни пътища, пътни артерии и комбинации от тях).

Следващите **Таблицы 5, 6, 7, 8 и 9** представят изходните данни от симулацията за някои от основните параметри на модела на градски автомобилен транспорт: *поток (Flow)*; *скорост (Speed)*; *закъснение (Delay)*; *опашка (Mean Queue)*; *брой спирания (Number of Stops)*. Изследваните параметри са основните характеристики на трафика според цитираните специализирани източници.

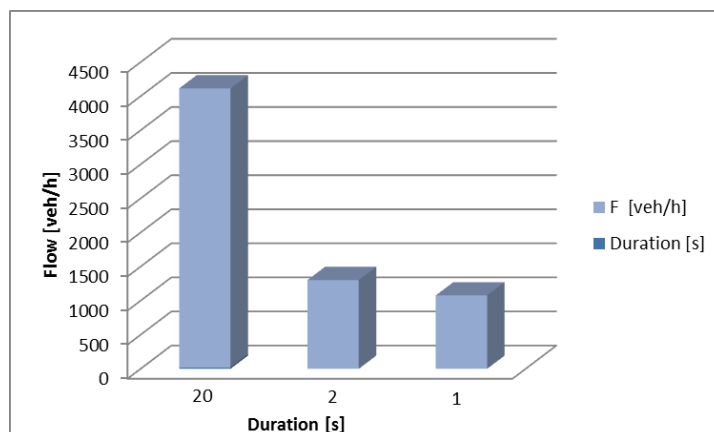
Средната стойност на *продължителността на сигнализация D* за изследваното кръстовище в референтния модел е приблизително 20 s. Източникът на DoS – атаката

има за цел пълното преустановяване на работата на светофарите. Авторът е симулирал това въздействие чрез неравномерно намаляване на продължителността на сигнализация D за зелената светлина. Условно се приема, че светофарите преустановяват работа при средна продължителност на сигнализация 1 [s], тъй като симулацията не може да бъде изпълнена при задаване на нулеви стойности.

Резултатите от симулацията на DoS - атака (C_{DoS}) върху референтния модел (M_{Ref}) на участък от градска автомобилна транспортна система за основните параметри, които характеризират трафика (F, T_D , V, Q и N), са представени в **Таблицы 5, 6, 7, 8** и **9**. Сравнителните диаграми на **Фиг. 18, 19, 20, 21** и **22** показват по какъв начин се променят стойностите на избраните параметри спрямо измерените за M_{Ref} под въздействие на кибератаката, т.е. в зависимост от продължителността на сигнализация D.

Таблица 5. Данни за потока (F) като функция на продължителността на сигнализация (D).

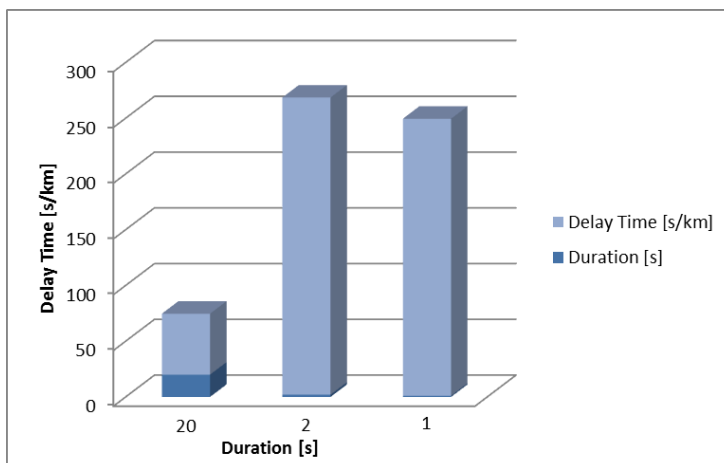
Въздействие	D [s]				F [veh/h]	F/ F _{max} [%]	F/ F _{Ref} [%]
M_{Ref}	20				4094	100.00	100.00
C_{DoS}	1	3	2	1	1300	31.75	31.75
	1	1	1	1	1076	26.28	26.28



Фигура 18. $F = f(D)$

Таблица 6. Данни за закъснението (T_D) като функция на продължителността на сигнализация (D).

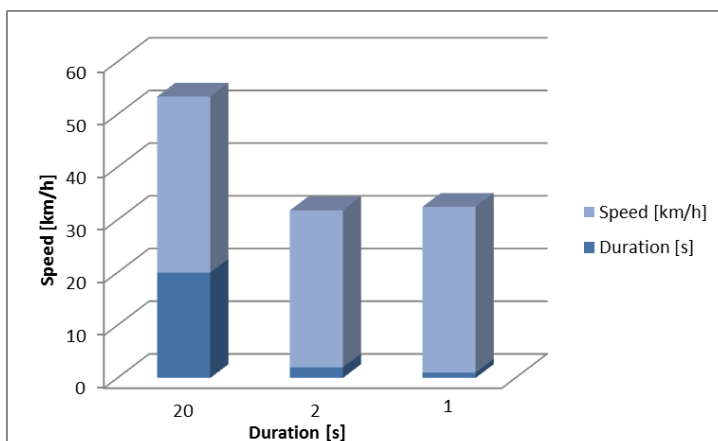
Въздействие	D [s]				T_D [s/km]	$T_D/ T_{D, max}$ [%]	$T_D/ T_{D, Ref}$ [%]
M_{Ref}	20				54.63	20.50	100.00
C_{DoS}	1	3	2	1	266.53	100.00	487.88
	1	1	1	1	248.46	93.22	454.81



Фигура 19. $T_D = f(D)$

Таблица 7. Данни за скоростта (V) като функция на продължителността на сигнализация (D).

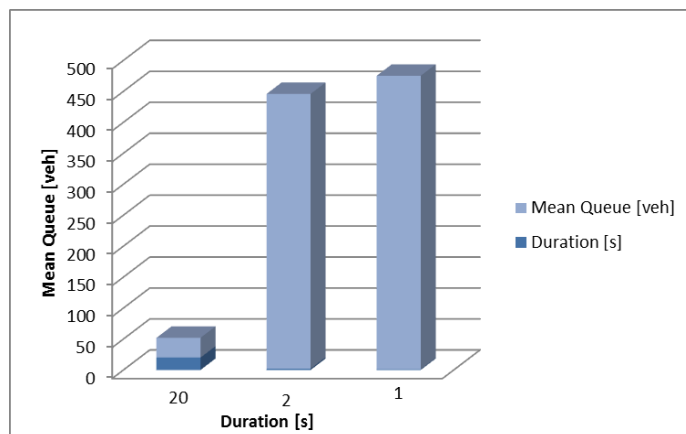
Въздействие	D [s]	V [km/h]	V/ V _{max} [%]	V/ V _{Ref} [%]
M _{Ref}	20	33.41	100.00	100.00
C _{DoS}	1 3 2 1	29.80	89.19	89.19
	1 1 1 1	31.47	94.19	94.19



Фигура 20. $V = f(D)$

Таблица 8. Данни за опашката (Q) като функция на продължителността на сигнализация (D).

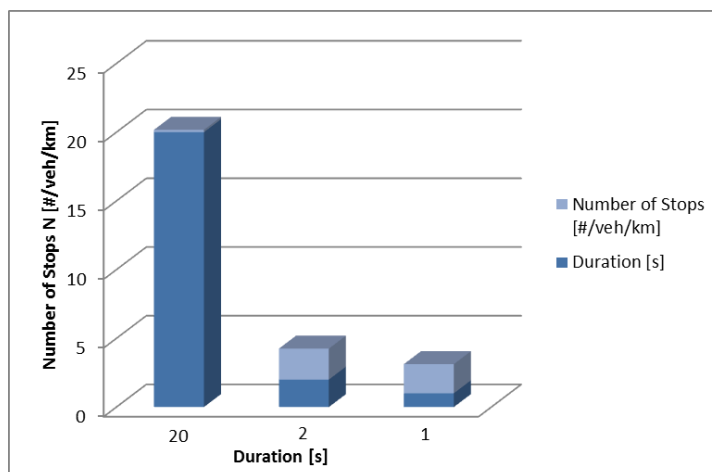
Въздействие	D [s]	Q [veh]	Q/ Q _{max} [%]	Q/ Q _{Ref} [%]
M _{Ref}	20	31.92	6.73	100.00
C _{DoS}	1 3 2 1	443.82	93.61	1390.41
	1 1 1 1	474.13	100.00	1485.37



Фигура 21. $Q = f(D)$

Таблица 9. Данни за броя на спиранията (N) като функция на продължителността на сигнализация (D).

Въздействие	D [s]	N [#veh/km]	N/ N _{max} [%]	N/ N _{Ref} [%]
M _{Ref}	20	0.17	7.56	100.00
C _{DoS}	1 3 2 1	2.25	100.00	1323.53
	1 1 1 1	2.12	94.22	1247.06



Фигура 22. $N = f(D)$

Обобщена оценка на резултатите

От табличните данни и сравнителните диаграми се вижда, че когато средната продължителност на сигнализация е приблизително равна на 2 секунди (за зелена светлина), съотношението F / F_{Ref} е равно на 31.75 %. Това означава, че под въздействието на DoS - атаката потокът F намалява с приблизително 68 % в сравнение с M_{Ref} . В този случай времето на закъснение T_D се увеличава приблизително 5 пъти в сравнение с $T_{D, Ref}$ и скоростта намалява с приблизително 11 % в сравнение с V_{Ref} . Опашката Q нараства близо 14 пъти спрямо Q_{Ref} . Броят на спиранията N е близо 13 пъти повече в сравнение с N_{Ref} .

В случая, когато се симулира преустановяване работата на светофарите и се приема, че средната продължителност на сигнализация е равна на 1 секунда за зелена

светлина (равносилно на 0 [s]), времето на закъснение T_D се увеличава 4,5 пъти, а броят на спиранията N – 12,5 пъти. Вижда се, че опашката Q нараства неимоверно (15 пъти) спрямо M_{Ref} , като същевременно потокът F намалява с близо 74 % в сравнение с измерения при M_{Ref} .

Въз основа на получените симулационни резултати може да се заключи, че под въздействие на DoS - атаката се наблюдават големи натрупвания, водещи до пълно спиране на движението в разглеждания участък.

2.2.3. Моделиране и оценка на въздействието на АРТ върху системата за сигнализация на градска автомобилна транспортна система

Втората серия експерименти със софтуер Aimsun 8.0 имат за цел да покажат потенциалното въздействие на семантична атака върху системата за сигнализация чрез равномерни дискретни изменения в продължителността на сигнализация D , които могат да останат незабелязани за неопределен период от време. За целите на настоящото изследване условно се приема, че кибератаки C_1 и C_2 променят продължителността на сигнализация съответно с -10 и +10 [s] в сравнение с референтния модел (M_{Ref}). Представените симулации са направени за времеви интервал от 10:00:00 до 11:00:00 ч. **Таблицы 10, 11, 12, 13 и 14** съдържат максималните и референтните стойности на измерените параметри, както и съответните съотношения. Зависимостите на избраните параметри от продължителността на сигнализация са графично визуализирани посредством 3D стълбовидни диаграми на **Фиг. 24, 25, 26, 27 и 28**.

Обобщена оценка на резултатите

Когато средната продължителност на сигнализация е намалена с 10 [s] (за зелена светлина) в сравнение със средната продължителност на сигнализация в референтния модел, съотношението F / F_{Ref} е равно на 77,45 %. Това означава, че под въздействието на кибератака C_1 потокът F намалява с приблизително 23 %. В този случай времето на закъснение T_D се увеличава повече от 3 пъти в сравнение с $T_{D, Ref}$ и скоростта намалява с приблизително 16 % в сравнение с V_{Ref} . Опашката Q нараства близо 5 пъти спрямо Q_{Ref} . Броят на спиранията N е 1,5 пъти повече в сравнение с N_{Ref} .

При увеличаване на средната продължителност на сигнализация с 10 [s] (за зелена светлина) в сравнение със средната продължителност на сигнализация в референтния модел времето на закъснение T_D , скоростта V и броя на спиранията N не се променят чувствително за разлика от опашката Q , която нараства над 4 пъти и потокът F , който намалява с 35 %.

Изводът е, че потоците F и опашките Q се променят значително под влияние на двете кибератаки, което означава, че под въздействие на потенциални АРТs или някакъв вид семантична атака, може да се наблюдават натрупвания, които да доведат до пътнотранспортни произшествия.

Изследването може да се разшири като се направят оценка и анализ на екологичните ефекти под въздействие на кибер заплаха върху градска автомобилна транспортна система (**Приложение IV**).

2.2.4. Сравнение на генерираните симулационни резултати в Aimsun 8.0 с резултати от аналогично изследване със симулатор, изграден с Microsoft Visual C++ 6.0 и MatLab 7.0

2.3. Методи и средства за защита на физическите и кибер аспекти на критичната инфраструктура

2.3.1. Средства за наблюдение, мониторинг и физическа сигурност

- *Наблюдение, мониторинг и защита от фактори на околната среда;*
- *Контрол на достъпа;*
- *Защита от радиочестотни смущения;*
- *Защита от външни електромагнитни полета;*
- *Защита от смесване на сигнали;*
- *Защита от затихване на сигнала;*
- *Защита при проблеми с пропускателната способност (честотната лента) на преносната среда.*

2.3.2. Средства за повишаване на киберсигурността въз основа на потенциалните уязвимости.

- *Рутер (маршрутизатор);*
- *Виртуални частни мрежи (VPN);*
- *Защитна стена (Firewall);*
- *Honeypots компютърни системи и Honeynets компютърни мрежи;*
- *Комплексни решения за защита от кибер заплахи (UTM - Unified Threat Management).*

2.3.3. Моделиране и оценка на въздействието на DoS - атака върху оптимизиран модел на Център за контрол на трафика на градска автомобилна транспортна система

В тази част от разработката авторът предлага модел на ЦКТ, който в същината си е базиран на вече описания типичен модел на ЦКТ.

За разлика от базовия модел на ЦКТ, в този случай кибер защитата се постига чрез използване на защитна стена от тип *ethernet2_slip8_firewall_adv*, която представлява специално програмиран рутер, поставен между източника на кибер заплахата и суича (*Фиг. 30*). Първоначалните настройки на защитната стена (TCP и IP: Processing Information) са приети по подразбиране:

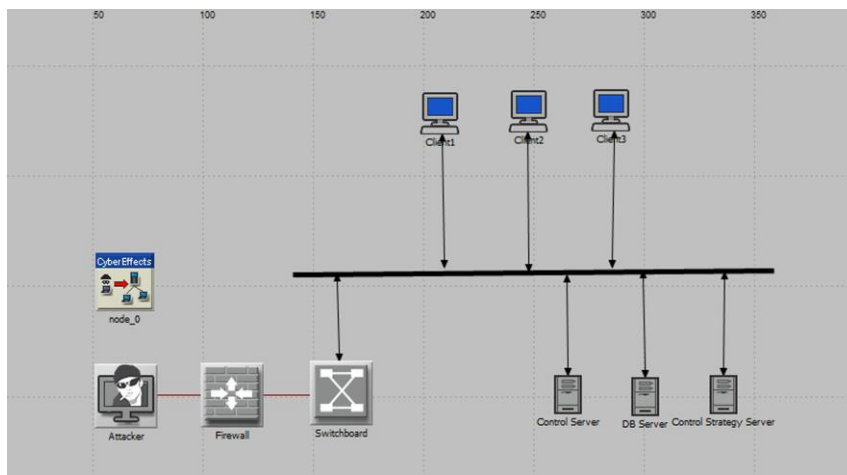
Целта на автора е на база на резултатите от проведената серия експерименти да докаже, че методът на симулационното моделиране е високо професионален за оценка на риска от кибер заплахи и изследване на различни възможности за надеждна кибер защита.

В *Таблица 17* са представени данните от проведените симулации на кибератака от тип DoS върху модела на ЦКТ на градска автомобилна транспортна система. Съпоставени са резултатите в двата изследвани случая. В първия случай защитна стена липсва и изграждането на кибер защитата се постига чрез специфични настройки на устройствата от гледна точка на техните уязвимости. Във втория случай защитната стена присъства като отделен елемент.

Таблица 18 съдържа обобщените резултати въз основа на трите графики, които показват в кои времеви диапазони R в [s] са регистрирани пиковете на изпратения и получения трафик, като функции на избраните три стойности на времето на пристигане

($T_1 = 2$ [s], $T_2 = 0.2$ [s] и $T_3 = 0.02$ [s]) при кибер въздействие без използване на защитна стена (БЗС) и със защитна стена (ЗС).

Продължителността на симулацията отново е $D = 30$ [s], разделена на шест времеви диапазона R , всеки от които е с продължителност 5 [s].



Фигура 30. Модел на ЦКТ с включена защитна стена под въздействие на DoS - атака.

Обобщена оценка на резултатите

Методологията на анализ е подобна на предходния случай, при който сравнението се прави между резултатите под въздействие на кибератаката и при референтния модел. От табличните и графичните данни в този случай може да се направи извод, че при използване на защитна стена броят на изпратените пакети $T_{s, \max}$ като цяло е по-нисък в сравнение с броя на изпратените пакети при използване вградени защити на мрежовите устройства.

До времевия интервал [25,30], когато броят на изпратените пакети е по-малък от 80, се наблюдава по-добра филтрация на изпратените пакети вследствие използването на защитна стена, отколкото при използване само на вградените защити на устройствата. В последния времеви интервал, когато броят на изпратените пакети надвишава 80, се наблюдава „насищане“, което може да бъде отгадено на ограниченост на конкретния вид защитна стена. Необходимо е да се установи също дали самите пакети представляват заплаха или не. В случай, че определени пакети застрашават системата, избраният модел защитна стена трябва да бъде подобрен, заменен или интегриран с други средства за защита.

В допълнение може да се каже, че когато е използвана защитна стена, случаите на наводняване със заявки са редуцирани до само един в последния времеви интервал от всички общо десет сценария, докато без средства за усилен киберзащита наводняването започва във времеви интервал [20, 25] и се задълбочава в последния времеви интервал [25, 30]. Това означава, че отказ на системата може да се наблюдава в поне два от всички десет сценария. Ако това трябва да бъде представено с вероятност от нежелано събитие, то следва, че при използване на защитна стена тази вероятност е 10 % и е поне два пъти по-висока, когато защитна стена не е поставена [66].

Преконфигуриране на защитната стена

В този случай процесът на оптимизация може да продължи с реконфигуриране на защитната стена с оглед на подобряване на функционалността ѝ. Експериментът е

проведен отново след въвеждане на следните настройки:

- *L2TP: Control Channel Parameters* – L2TP е протокол за тунелиране, който се използва за подпомагане на VPN или като част от доставка на услуги чрез ISPs. Комбинацията от двата протокола (L2TP/IPSec) осигурява конфиденциалност, автентификация и цялост на пакетите. L2TP определя типа на криптиране чрез задаване на стойност от 0 (няма криптиране) до 7 (криптиране с помощта на алгоритъм, определен от Cisco). Направените настройки са показани на **Фиг. 34**.
- *Security: IPSec* – атрибутът IPSec се използва за конфигуриране на параметри, свързани със сигурността на възела. Протоколът IPSec се реализира директно върху протоколния стек TCP/IP, който работи на 3-ти слой от OSI модела. На **Фиг. 35** се вижда какви настройки на глобалните свойства (*Global Properties*) са избрани за провеждане на симулацията.
- *AH (Authentication Header)* е удостоверяващо начало, а продължителността на сесията (*Lifetime*) е 28800 [s]. Използваният алгоритъм за автентификация по време на установената IPSec сесия е *HMAC-SHA1*.

Симулационните резултати от експериментите със защитната стена в първоначалния вариант (ЗС₁) и след нейното преконфигуриране (ЗС₂) са представени в **Таблицы 19 и 20**.

Обобщена оценка на резултатите

На база на получените симулационни резултати може да се направи извод, че преконфигурирането на защитната стена с използване на специфични настройки за повишаване на сигурността на ЦКТ, води до намаляване на забавянето на предаването на пакетите в два от сценариите съответно при време T₁ и T₂.

При T₁ в интервал [5, 10] се наблюдава, че при един и същ брой на изпратените пакети, броят на получените пакети е различен от 0, когато е използвана ЗС₂. Аналогичен е резултатът при T₂ в интервал [20, 25], тъй като при един и същ брой на изпратените пакети броят на получените при използване на ЗС₂ е по-голям в сравнение с този при използване на ЗС₁.

Предвид, че симулационните резултати не се различават чувствително при използване на ЗС₁ и ЗС₂, може да се направи заключение, че основно предимство на изградения симулационен модел на ЦКТ е неговата универсалност, т.е. от способността му да не се влияе съществено от различни промени в настройките на отделните устройства.

От друга страна, липсата на резки изменения в генерираните данни от симулацията в двата случая показват, че при задаване на настройки по подразбиране използваната защитна стена е достатъчно надеждна. В случай, че при използването ѝ степента на защита не е удовлетворителна, следва да бъдат предприети други мерки за усиление на защитата на ЦКТ.

2.3.4. Допълнителна информация относно настройките за сигурност в модела на ЦКТ и логическата връзка между проведените експериментални изследвания със симулационни продукти

В **Таблица 21** се съдържа информация за това какво е заложено в модела на ЦКТ, за да се увеличи устойчивостта му към кибер атаки, както и в какво конкретно се изразява резултатът от използването на описаните специфични настройки за сигурност.

Разгледани са следните три случая:

- *DoS - атака върху модела на ЦКТ без защитна стена - M_{FWD0}*;
- *DoS - атака върху модела на ЦКТ след въвеждане на ЗС₁ с настройки по*

подразбиране - M_{FW1} ;

- *DoS - атака върху модела на ЦКТ след преконфигуриране на $3C_1$ в $3C_2 - M_{FW2}$.*

Протоколът IGMP се настройва в прозореца *Attributes* на сървърите от *IP > IP Multicasting (многократно предаване) > IGMP Parameters* с цел да се предотврати загубата на пакети, т.е. системата да се стабилизира по начин, който не позволява на кибер атаката да предизвиква вътрешни флуктуации в нея.

Негативното въздействие на кибератаката намалява с повишаване на ефективността на поставената защитна стена чрез конфигурирането ѝ с подходящи настройки за сигурност. Следователно, пътно-транспортната обстановка не се влияе от въздействието на кибер атаката, когато моделът на ЦКТ е оптимизиран чрез въвеждане на защитна стена, която е конфигурирана така, че да осигури максимално ниво на защитеност.

Таблица 22 и диаграмата на *Фиг. 36* представят зависимостта между броя на получените пакети под въздействие на DoS - атаката върху ЦКТ (БЗС, $3C_1$ и $3C_2$) и потока от превозни средства F през изследвания участък в интервал $R = [20, 30]$ от продължителността на симулацията в секунди. Предвид, че резултатите от симулацията на DoS - атака върху ЦКТ се измерват в брой изпратени и получени пакети в секунда [packets/s], по ординатата са нанесени максималните стойности на получените пакети $T_{R, \max}^*$.

2.4. Разработка на алгоритми за изпълнение в използваните симулационни среди

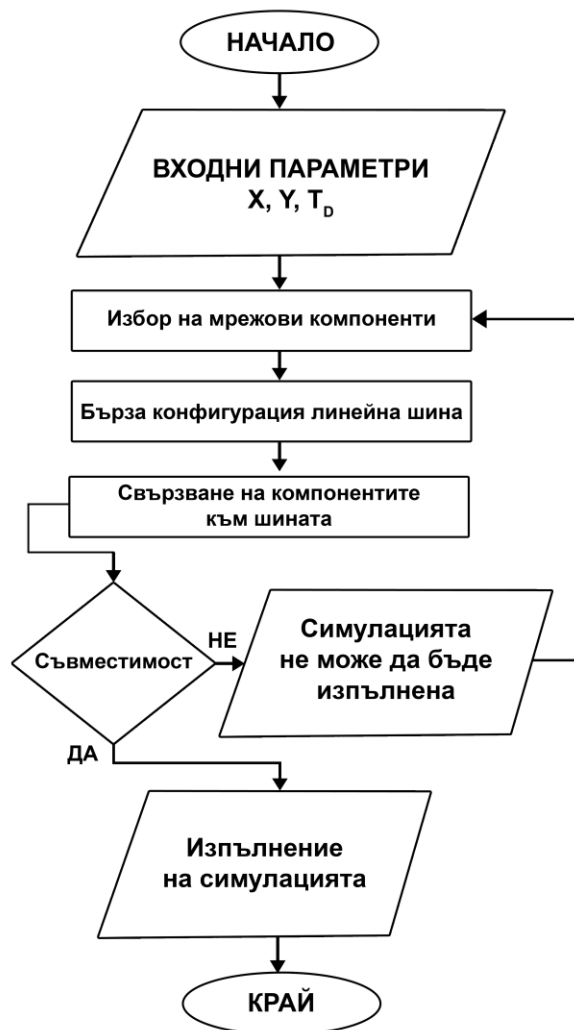
В случая алгоритмите са описани първоначално в текстова форма като последователност от етапи в процеса на моделиране и симулация, на база на която впоследствие е направено и графично представяне във вид на примерни блокови схеми (*Фиг. 37, 38 и 39*).

Предстои да бъдат представени два разклонени алгоритъма за изпълнение в симулационен софтуер Riverbed Modeler Academic Edition 17.5 и един алгоритъм за изпълнение в симулационна среда Aimsun 8.0.

Конкретната последователност от стъпки в трите алгоритъма осигурява успешното стартиране и изпълнение на симулациите, както и генерирането на надеждни резултати за оценка и анализ, които да подпомагат процеса на вземане на решения и да допринасят за научно-приложното изследване на реални проблеми на киберсигурността. Следователно всяка промяна в последователността от действия или пропускане на стъпки може да доведе до получаване на некоректни резултати и съответно до некоректни изводи.

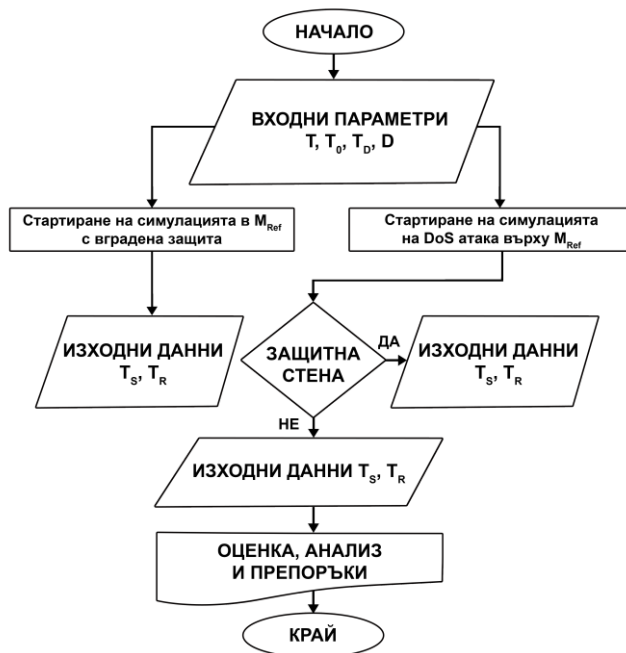
*Данните са извадени от *Таблицы 17 и 19*.

- Алгоритъм за моделиране на ЦКТ, изпълнен в симулационна среда Riverbed Modeler Academic Edition 17.5.



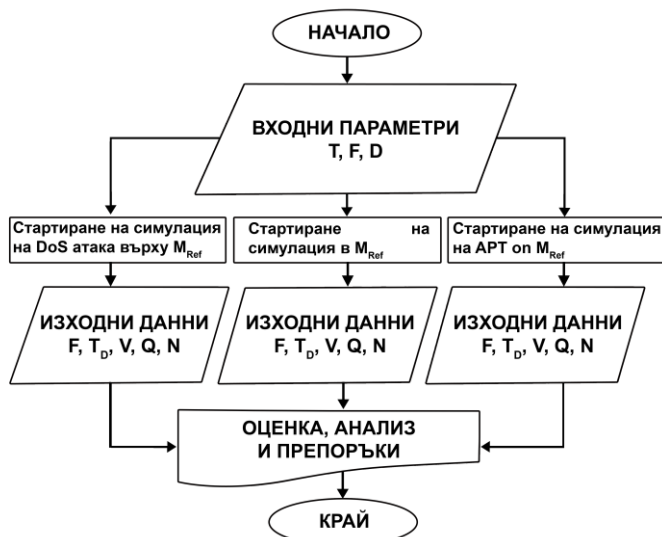
Фигура 37. Алгоритъм за моделиране на ЦКТ, изпълнен в симулационна среда Riverbed Modeler Academic Edition 17.5.

- Алгоритъм за симулиране на DoS атака, изпълнен в Riverbed Modeler Academic Edition 17.5.



Фигура 38. Алгоритъм за симулиране на DoS - атака върху ЦКТ, изпълнен в Riverbed Modeler Academic Edition 17.5.

- Алгоритъм за симулиране на въздействието на кибератака върху системата за сигнализация на светофарите, изпълнен в Aimsun 8.0.



Фигура 39. Алгоритъм за симулиране на въздействието на кибератака върху системата за сигнализация на светофарите, изпълнен в Aimsun 8.0.

ИЗВОДИ ОТ ВТОРА ГЛАВА

1. Използването на професионалния симулационен продукт Riverbed Modeler Academic Edition 17.5 за провеждане на експерименталното

изследване дава възможност за планиране на устойчивостта чрез повишаване на защитата в изградения симулационен модел и възможността за оценка на системната уязвимост (т. 2.2.1.).

2. Симулационните резултати показват, че кибератаките могат да причинят усложнена пътно-транспортна обстановка (т. 2.2.2.) и повишаване на замърсяването на въздуха с вредни вещества (Приложение IV).
3. Оптимизацията на симулационния модел на ЦКТ чрез поставяне на защитна стена редуцира въздействието на DoS - атаката върху него (т. 2.3.3.).
4. Направеният сравнителен анализ между симулационното изследване със софтуер Aimsun 8.0 и избраното аналогично изследване с Visual C++ 6.0 и MatLab 7.0 показва, че получените сходни резултати в двата случая отразяват реалистично нормална пътно-транспортна обстановка в градска среда, което доказва тяхната достоверност (2.2.4.).

ТРЕТА ГЛАВА.

МЕТОДИКА ЗА ОЦЕНКА НА УЯЗВИМОСТТА НА СИСТЕМАТА ЗА УПРАВЛЕНИЕ НА ТРАНСПОРТА КЪМ КИБЕР ЗАПЛАХИ

Настоящата глава е посветена на последващо изследване, базирано в голямата си част на обобщаване на опита от проведените експерименти и направените изследвания, описани в предходните глави, поради което се налага обособяването му в отделна глава.

3.1. Разработка на методика за оценка на уязвимостта и планиране на мерки за повишаване на устойчивостта на системата за управление на транспорта

Методиката може да бъде структурирана в следните стъпки:

- 1) Изпитване за надеждност
- 2) Дефиниране на уязвими компоненти и агенти
- 3) Избор на инструментариум за оценка на уязвимостта
- 4) Идентифициране и анализ на киберзаплахите
- 5) Анализ на симулацията
- 6) Мерки за повишаване на устойчивостта към кибер заплахи
- 7) Алгоритмизация на цялостния симулационен процес
- 8) Анализ на ползите от прилагане на симулационни методи за целите на администрацията и бизнеса.

3.2. Оценка на вероятността от кибератаки върху Центъра за контрол на трафика

Предстои да бъде представен метод за оценка на вероятността от кибератаки върху системата за управление на транспорта, чиято специфика се дължи на използването на симулационни резултати за количествена и качествена оценка на риска.

Рискът се отнася до отклонението на един или повече резултата за едно или повече бъдещи събития от тяхната очаквана стойност. Предвид, че вероятността е броят на избраните случайни събития към общия брой събития, рискът може да бъде изчислен като произведение от вероятността (P) и щетите (C) [$R = P \cdot C$] и представен като функция на P [$R = f(P)$] чрез вероятностно разпределение.

В конкретния експеримент фокусът е върху броя на нежеланите събития (m) под въздействието на DoS - атака върху ЦКТ за всеки от общо 10 последователни сценария. Използваната среда за симулация е Riverbed Modeler academic Edition 17.5.

Параметърът T („Interarrival time“) определя разпределението и аргументите да бъдат използвани за генериране на случайни резултати за времената между последователните изпращания на пакети в състояние „ON“. В случая се задават различни стойности на T в M_{Ref} и под въздействие на кибератаката, докато стойностите по подразбиране на всички останали параметри остават непроменени.

Въз основа на предходните обобщени оценки на резултатите (Глава втора) е направено допускането, че тези нежелани събития се изразяват в аномални стойности на изпратения ($T_{s, max}$) и получения трафик ($T_{R, max}$) в сравнение с референтния модел M_{Ref} . Изпратеният и получения трафик се измерват в пакети в секунда [packets /s]. Броят на всички събития за всеки отделен сценарий е 6, защото продължителността на симулацията е разделена на 6 равни интервала от 5 [s].

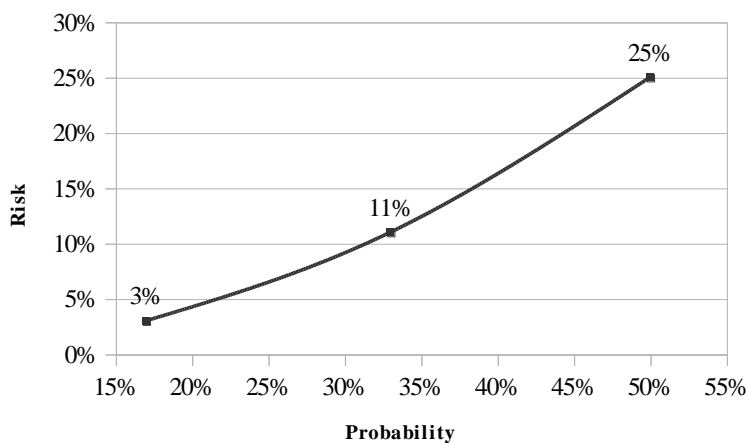
Таблица 23 съдържа изчислените вероятности за реализиране на DoS - атака (P) и възможните щети (C), както и количествена оценка на риска (R). Направено е условно експертно определяне на очакваните щети на база на броя на регистрираните нежелани събития за всеки сценарий предвид, че е логично по-големият брой нежелани събития да причини повече щети. Практически, ако $m = 0$, тогава $C = 0$ и ако $m = n = 6$, тогава

щетите C се приемат за максимални - 1 (100%). Следователно, ако $m = 1$ и $n = 6$, тогава C е съотношение на 1 към 6. Стойността му е съответно 2, 3, 4 или 5 пъти повече, ако $m = 2, 3, 4, 5$.

Разпределението на вероятностите е представено графично на **Фиг. 41**, като стойностите на вероятността (probability) са разпределени по абцисата, а на риска (risk) - по ординатата.

Таблица 23. Оценка на риска с използване на резултати от симулационно моделиране на DoS - атака.

Сценарий	$T [s]$	m	P	C	R
1.	2	1	0.17	0.17	0.03
2.	1	1	0.17	0.17	0.03
3.	0.5	1	0.17	0.17	0.03
4.	0.25	2	0.33	0.33	0.11
5.	0.2	3	0.50	0.50	0.25
6.	0.15	2	0.33	0.33	0.11
7.	0.1	1	0.17	0.17	0.03
8.	0.05	2	0.33	0.33	0.11
9.	0.025	2	0.33	0.33	0.11



Фигура 41. Графична интерпретация на $R = f(P)$ за ЦКТ.

Максималните стойности на P и R са регистрирани в Сценарий 5. Качествената оценка на риска може да бъде направена въз основа на общоприетите стандарти за рисковите области. Средната стойност на риска в случая е 8%. Приема се, че $R < 20$ е

допустим и не са необходими специални мерки за неговото редуциране. Всъщност, относително е дали средният риск от 8% е нисък или висок, защото продължителността на симулацията е 30 [s], докато кибератаката може да бъде с по-голяма продължителност.

За намаляване на риска същият процес на симулация може да бъде повторен след поставянето на допълнителна защита между нападателя и суича в моделирания ЦКТ. Резултатите от симулацията от избраните три сценария са представени в *Таблица 24*, за да се покаже по-доброто филтриране, което се дължи на защитната стена, поставена на пътя на DoS - атаката. Броят на нежеланите събития при вмъкване на защитна стена е показан в *Таблица 25* съответно за Сценарий 1 (начален), 5 (междинен) и 10 (последен). Изводът е, че регистрираните нежелани събития също намаляват при поставяне на защитна стена.

Сравнението между средната стойност на риска за избраните три сценария в този случай и средната стойност на риска за съответните сценарии 1, 5 и 10 с вградена защита показва намаляване на риска от 10,3% на 4,67%, което е повече от 2 пъти по-малко [68].

3.3. Оценка на риска от въздействие на кибератаки върху системата за управление на транспорта с използване на метода на трите фактора.

Докато при експертния метод за оценка рискът се представя като функция на вероятността за реализиране на дадено нежелано събитие, то методът на трите фактора включва и друг много важен фактор – уязвимостта (V). Съществуват различни формулировки на този метод в зависимост от параметрите, включени във формулата.

Рискът може да бъде представен концептуално с основно уравнение

$$R = H * V * E, \quad (3)$$

където: H е опасност, V - уязвимост и E - експозиция в смисъл на рискови елементи (хора или активи). В този случай той се определя като вероятност от вредни последици или очаквани загуби (смъртни случаи, наранявания, имущество, поминък, икономическа дейност, разрушения) в резултат на взаимодействия между различни опасности и уязвими условия [77].

В конкретния случай е предпочетена формулировката

$$R = P * C * V, \quad (4)$$

където щетите (C) се изчисляват чрез условно експертно определяне на базата на броя на нежеланите събития. Например, C е максимум 1 (100%), ако $m = n = 6$. Когато $m = 1$ и $n = 6$, C се изчислява като съотношение на 1 към 6 и неговата стойност е съответно 2, 3, 4 или 5. пъти повече, ако $m = 2, 3, 4, 5$.

Най-уязвимите компоненти на системите за управление на транспорта са ЦКТ и системата за сигнализация на светофарите. Критичните уязвимости в компютърните системи могат да бъдат класифицирани и оценени с помощта на стандарта CVSS (Common Vulnerability Scoring System), чиято последна версия към настоящия момент е 3.0. При анализа на резултатите уязвимост в диапазона 7.0 -10.0 се определя като висока, 4.0 – 6.0 – като средна и 0 – 3.9 – като ниска [11].

В първата част на настоящото експериментално изследване стойностите на уязвимостта се задават последователно в три сценария, за които се въвеждат различни стойности на основния входен параметър T . Този симулационен модел се разглежда като целеви обект на вътрешна DoS - атака.

Таблицы 26, 27 и 28 съдържат обобщените резултати от всички три графики, показващи регистрираните пикови нива на изпратения (T_s) и получения (T_R) трафик като функции на T ($T_1 = 2$ [s], $T_2 = 1$ [s], и $T_3 = 0.2$ [s]) при системна уязвимост към кибератаки V от 5 до 100%. Продължителността на тази симулация се разделя на шест равни интервала от 5 секунди ([1, 5], [5, 10], [10, 15], [15, 20], [20, 25], [25, 30]).

Втората част на изследването има сходен принцип с предходната, но симулираната DoS - атаката към ЦКТ е външна, защото нейният източник се намира извън него. Резултатите от симулацията са представени в **Таблицы 29, 30 и 31**.

Таблица 32 съдържа броя на нежеланите събития (m) в резултат на промяна на уязвимостта на системата (V) за три избрани сценария под въздействието на вътрешна и външна DoS - атака върху ЦКТ. Броят на всички събития за всеки сценарий е $n = 6$, тъй като продължителността на симулацията е разделена на 6 равни интервала от 5 секунди. Следователно, в този случай вероятността се изчислява като съотношение на броя на нежеланите събития (m) към общия брой събития (n). Приема се, нежеланите събития се изразяват в аномални стойности на $T_{s, \max}$ и $T_{R, \max}$. Колонната диаграма на **Фиг. 41** показва зависимостта между вероятността P и уязвимостта V за Сценарий 10 съответно под въздействието на вътрешна (P_{internal}) и външна кибератака (P_{external}).

Симулационните резултати за оценка на риска по метода на трите фактора са представени в **Таблица 33**.

В този случай обобщената оценка, базирана на графичните и таблични резултати, показани на **Фиг. 43** и **Таблица 33**, е, че генерираните резултати от симулацията са надеждни и подходящи за оценка и анализ на риска. Закономерността на тези резултати е видима, защото нивата на риск са най-високи, когато уязвимостта на системата надвишава критичните 50%. Друг важен извод е, че рискът е по-голям под въздействието на външна кибератака.

Всъщност, основната разлика между вътрешната и външната кибератака е в местоположението на нападателя. В симулационната система външната кибератака се симулира от нападател, поставен извън ЦКТ. При вътрешна кибератака нападателят се поставя в ЦКТ. В Riverbed Academic Edition 17.5 нападателят е представен от работна станция със специфични настройки. Отрицателното въздействие на DoS - атаката е насочено към изчислителните ресурси на заразенния сървър и причинява изчерпване на честотната лента на канала за интернет връзка.

Минимизирането на риска може да се постигне чрез по-ефективен анализ на уязвимостта и своевременно идентифициране на кибернетичните заплахи и слабите места в системите чрез извършване на редовна цялостна оценка, мониторинг и превенция. Редуцирането на често срещаните уязвимости в системите за управление е възможно чрез използване на съвременни TCP / IP системи, както и сложни средства за защита, съчетаващи защитни стени, VPN, антивирусен софтуер и др. [69].

3.4. Оценка на вероятността от кибератаки върху градска автомобилна транспортна система

Това емпирично изследване е още един пример за оценка на вероятността на базата на резултати от симулации, получени при използване на Aimsun 8.0. Това е логично продължение на описаната ситуация, тъй като реализирането на DoS - атака върху ЦКТ може да доведе до нарушаване на нормалната сигнализация на светофарите. Методът за оценка също е аналогичен на предишния, но в този случай нежеланите събития са свързани с пътното движение и потенциалните екологични проблеми (виж **Приложение IV**).

Най-ниски нива на сризове се наблюдават при междинни нива на потока. Контролирането на плътността на трафика, а не на потока, също е от ключово значение, тъй като ниските потоци могат да се появят както при ненатоварени (високоскоростни), така и при претоварени (нискоскоростни) условия [73].

Следователно нежеланите събития, наблюдавани от автора предимно в две кръстовища под въздействието на потенциална кибератака, могат да бъдат класифицирани в три основни категории:

- **задръствания** – наблюдават се в един интервал от време съответно в Сценарии 1 и 2. Съществуват предпоставки за задръствания в два интервала от време в Сценарии 3 и 4, които също се отчитат като нежелани събития.
- **инциденти** - Сценарий 1 симулира произшествие.
- **повишени нива на замърсители във въздуха** - замърсяването е особено интензивно в Сценарий 1 поради повишените нива на всички изследвани замърсители.

Таблица 34 съдържа аномални стойности, регистрирани във всеки от общо 5 сценария въз основа на анализ на графичните резултати от симулацията. Симулациите се изпълняват за времеви интервал от 10:00:00 до 11:00:00 ч., който е разделен на 6 равни интервала от 10 [min]. Следователно броят на всички събития за всеки сценарий е $n = 6$.

В Aimsun 8.0 при $D = 1$ [s] в Сценарий 5 се симулира потенциалната фатална ситуация, когато светофарът престане да функционира абсолютно под отрицателното въздействие на кибератака. Въз основа на графичните и табличните резултати, получени за характеризиращите трафика параметри, се приема, че в последния сценарий $m = n = 6$. Стойностите на риска в интервала от 25% до 100% могат да бъдат определени и анализирани въз основа на графиката, показана на **Фиг. 44**.

ИЗВОДИ ОТ ТРЕТА ГЛАВА

1. Разработената методика осигурява необходимия инструментариум, с който може да се извърши цялостно изследване в симулационна среда, което да включва оценка на системната уязвимост с цел планиране на мерки за повишаване на устойчивостта на системата за управление на транспорта (т. 3.1.).
2. Предимствата на метода на симулационно моделиране пред „тестовите за пробив“, обосновани в т. 3.1., като:
 - *директното инсталиране на симулационен софтуер на даден компютър не крие заплаха от инфектиране;*
 - *оценката на уязвимостите предшества изпълнението на симулацията, което спестява време в търсене на слаби места в системата;*
 - *клиентът не е ангажиран през цялото време с процеса по изпълнение на тестовите за пробив, а получава завършен краен продукт.*

предполагат използването му за оценка на уязвимостта на системата към кибератаки.
3. Извършената оценка на риска от реализиране на DoS атака върху ЦКТ в зависимост от вероятността за реализация на DoS атаката и експертното (условното) определяне на свързаните с това щети показват, че той

намалява повече от два пъти при усъвършенстване на защитата с поставяне на „Защитна стена“ (т. 3.2.).

4. Извършената оценка на риска от реализиране на външна и вътрешна кибератака върху системата за управление на транспорта по метода на трите фактора (опасност, уязвимост и щети) показват, че нивата на риск са най-високи, когато уязвимостта на системата надвишава критичните 50%, като рискът е по-голям под въздействието на външна кибератака (т. 3.3.)
5. Анализът на получените симулационни резултати показва, че рискът от реализиране на кибератака нараства с повишаване на системната уязвимост. Това е свързано с повишаване на нежеланите събития по пътищата, класифицирани от автора в три основни категории – задръствания, инциденти и повишени нива на замърсители във въздуха (т. 3.4. и приложение 4).

ИЗВОДИ

1. Общи изводи

- 1.1 На база на библиографски източници, свързани с обекта и предмета на дисертационния труд, са анализирани проблемите на съвременната киберсигурност.
- 1.2 Оценката и анализът на резултатите от направеното теоретично и емпирично изследване, включващо изграждане и оптимизиране на симулационен модел на ЦКТ, симулиране на кибератака върху него и върху системата за сигнализация на светофарите, доказват работната хипотеза и ефективността на метода на симулационно моделиране при провеждане на подобни изследвания.
- 1.3 При провеждане на експерименти за оценка на системната уязвимост се потвърждава надеждността на получените симулационни резултати и респективно предимствата от използването им за оценка на риска от кибератаки.

2. Научно-приложни приноси на дисертацията

- 2.1 Актуализиран е модел на „Адаптивна архитектура на система за кибернетична защита, в която топологичен анализ на уязвимостите може да бъде направен на втория етап (Превенция) чрез използване на симулационно моделиране за създаване на мрежови конфигурации, включващи техните уязвимости, както и за усъвършенстване на модела на четвъртия етап (Реагиране).
- 2.2 Разработен е модел, който представя връзката между базовия концептуален модел „Триъгълник на кибер заплахата“ от една страна и средствата за симулация и визуализация, чрез които могат да бъдат открити и редуцирани уязвимостите от друга.
- 2.3 Създаден е модел на ЦКТ в симулационна среда Riverbed Modeler Academic Edition 17.5, на база на който са направени оценка и анализ на въздействието на DoS - атака върху градска автомобилна транспортна система.
- 2.4 Симулационният модел на ЦКТ е оптимизиран чрез въвеждане на защитна стена и са проведени експерименти съответно с настройки по подразбиране на защитната стена и след преконфигурирането ѝ, които имат за цел да покажат, че функционалността на оптимизирания в сравнение с първоначалния референтен модел е подобрена.
- 2.5 Разработени са алгоритми за изпълнение в използваните симулационни среди, които представят последователност от стъпки, която е препоръчително да се спазва при провеждане на други аналогични изследвания.
- 2.6 Разработена е методика за оценка на уязвимостта и планиране на мерки за повишаване на устойчивостта на системата за управление на транспорта чрез използване на резултати от симулационно моделиране с цел минимизиране на финансовите разходи и избягване на реални щети за системата при реализиране на кибератака върху нея.

2.7 Направени са оценка и анализ на екологичните ефекти под въздействие на кибератака върху системата за сигнализация на градска автомобилна транспортна система в симулационна среда Aimsun 8.0.

3. Приложни приноси на дисертацията

3.1 Обяснена е логиката на функциониране на система за управление на транспорта и в частност на ЦКТ, като нейна основна подсистема.

3.2 Анализирани са симулационен модел на кибератака срещу управленска структура, разработен със софтуер NetLogo, по отчетни данни от картата на глобалните рискове за 2012 г. и е приложен за създаване на аналогични модели по отчетни данни за други години (в случая 2015 г.).

3.3 Поради съществуването на множество симулационни продукти с различна сложност и предназначение, са анализирани възможностите на три напълно различни по тези два показателя продукта, които използват агентно-базирано моделиране, като за провеждане на експериментите е избрано да бъдат комбинирани два от тях и един е определен като неподходящ (Втора глава).

3.4 Направена е сравнителна характеристика на двата основни публично известни метода за оценка на уязвимостта на системата към кибератаки – симулационното моделиране и „тестовите за пробив“.

3.5 Извършена е оценка на риска по два метода въз основа на получените резултати от симулационно моделиране, която показва, че проведеното изследване доказва работната хипотеза относно негативното въздействие на кибератаки върху система за управление на транспорта.

3.6 Извършен е сравнителен анализ между симулационното изследване със софтуер Aimsun 8.0 и избрано аналогично изследване с Visual C++ 6.0 и MatLab 7.0 с цел да се провери достоверността на получените резултати (2.2.4.).

ЗАКЛЮЧЕНИЕ

При разработката на трите глави в дисертационния труд са описани и приложени едни от най-иновативните методи и средства за реализация от гледна точка на съвременните научни източници.

В дисертационния труд са използвани професионални симулационни продукти от висок клас за симулиране на кибератаките, което гарантира резултати с висока степен на достоверност в сравнение с резултатите от използването на продукти от по-нисък клас, които разполагат с ограничени параметри и базови възможности за описание на алгоритми със средствата на програмен език. В тази връзка използваните тясно специализирани софтуерни продукти предлагат и богати възможности за визуализация на конкретната среда с всички необходими типове и модели мрежови компоненти за изграждането ѝ. Освен това професионалните софтуерни продукти позволяват във виртуална среда да бъдат проиграни множество сценарии с възможности за извършване на сигурна оптимизация на трафика и комуникационните мрежи, както и на други сложни системи.

Авторът използва метода на логическия анализ при обобщената оценка на резултатите от експерименталните изследвания. Подходът за моделиране на ЦКТ и симулирането на кибер-въздействия върху него е самостоятелен. Получените изходни резултати могат да бъдат използвани при други подобни проучвания и разработки.

Дисертацията дава възможност за правилен подбор на средства за защита и вграждането им в мрежовите конфигурации с цел повишаване на киберсигурността.

Натрупаният от проведените изследвания опит дава основание да се формулират следните препоръки относно бъдещи изследвания и експериментална работа:

- разширяване на обхвата и дълбочината (детайлността) на моделирането на архитектурата на системата за информационна сигурност до обхващане на всичките ѝ подсистеми и функционалности;
- изследване на интензивността на кибератаката и в частност на зависимостта между броя получени заявки за единица време и потока от превозни средства.

III. НАУЧНИ ПУБЛИКАЦИИ ПО ТЕМАТА

РЕЗУЛТАТИТЕ ПО ДИСЕРТАЦИЯТА СА ПУБЛИКУВАНИ В:

- **международни реферирани списания на английски език:**

Ivanova, Y. ASSESSMENT OF THE PROBABILITY OF CYBERATTACKS ON TRANSPORT MANAGEMENT SYSTEMS. Publication of Union of Scientists in Bulgaria: International Journal on Information Technologies and Security (IJITS), Issue №4 (December), 2018 (volume 10), pp. 99 – 106.

Ivanova, Y. ASSESSING THE VULNERABILITY OF A TRANSPORT MANAGEMENT SYSTEM TO CYBER ATTACKS FOR APPLICATION IN THE METHOD OF THE THREE FACTORS. Publication of Union of Scientists in Bulgaria: International Journal on Information Technologies and Security (IJITS), 11(1), 2019, pp. 85-94.

- **научни списания в България:**

Иванова, Йоана. АНАЛИЗ НА ВЪЗДЕЙСТВИЕТО НА КИБЕР ЗАПЛАХИ ВЪРХУ СИСТЕМА ЗА УПРАВЛЕНИЕ НА ТРАНСПОРТА, Доклад, София: Годишник на Военна академия, 2018.

БЛАГОДАРНОСТИ

Бих искала да изкажа специални благодарности на научния си ръководител Полк. Доц. Д-р Иван Христозов и на Доц. Д-р Костадин Цветков за професионалните им препоръки, свързани със съдържанието, цялостното оформление и структуриране на дисертационния труд.

Най-искрени благодарности поднасям на Полк. Проф. Д-р Камен Калчев, ръководител на Катедра „Комуникационни и информационни системи“ към Факултет „Командно-щабен“ на Военна академия „Георги С. Раковски“ за професионалните му препоръки и оказаното съдействие за реализиране на направеното експериментално изследване.

Отправлям специални благодарности към Доц. Д-р Веселина Александрова и Проф. д-тн Андон Лазаров в качеството им на рецензенти за направените от тях конструктивни препоръки, свързани с формулировката на изводите и научно-приложните резултати от дисертационния труд.

Дължа най-дълбока благодарност на Проф. д.т.н. Тодор Стоилов и асистент Йорданка Бонева от Института по информационни и комуникационни технологии на БАН за предоставения ми достъп до ресурси за изпълнение на симулацията на кибератака върху участък от градска автомобилна транспортна система.

Не на последно място благодаря на родителите си за проявеното търпение и оказваната подкрепа, както и на всички, които пряко или косвено са допринесли за реализирането на този дисертационен труд.