Georgian Scientists

ქართველი მეცნიერები

Vol. 3 Issue 4, 2021

https://doi.org/10.52340/gs.2021.11.07

Создание Программной Модели с Графическим Интерфейсом Пользователя для симуляции процессов функционирования подсистем информационной и кибер защиты Распределенных Информационных Систем Критических Инфраструктур

Рамаз Шамугиа

Сухумский Физико -Технический Институт им. Ильи Векуа,Тбилиси, Грузия

e-mail: rmz.shamugi@gmail.com; mob.:+995595538797; https://orcid.org/0000-0002-8141-1738

Анотация. Данная статья посвящена разработке программной модели с Графическим Интерфейсом Пользователя (ГИП) для иммитации процесса обеспечения информационной и кибер безопасности информационных систем (ИС) объектов Критической Инфраструктуры (КИ) на основе аналитической модели разработанной автором данной статьи раннее. Указанная программная модель с ГИП дает возможнось с помощью элементов управления расположенных на главной панели, задавать входные параметры моделируемого объекта и наблюдать его выходные характеристики с помощью соответствующих элементов визуализации таких, как специальные окна для отображения вычисляемых числовых значений основных характеристик исследуемых систем.

Ключевые слова: *информационные системы, инфобезопасность, кибербезопасность, критические инфраструктуры, моделирование, многоканальные системы массового обслуживания, графический интерфейс пользователя.*

1.Введение

На текущем этапе своего развития, компьютерные и информационные технологии охватили все отрасли экономики. Для любой современной компании информация становится одним из главных ресурсов, сохранение и правильное распоряжение которым имеет ключевое значение для развития бизнеса и снижения уровня разнообразных рисков. Особую актуальность проблема обеспечение информационной и кибер безопасности приобретает в случае распределенных информационных систем (РИС) объектов Критической инфраструктуры (РИСКИ).

Под информационной безопасностью РИСКИ понимают комплекс мер организационного и технического характера, направленных на сохранение и защиту информации и ее ключевых элементов, а также оборудования и систем, которые используются для обработки, хранения и

передачи информации. Этот комплекс включает технологии, стандарты и методы управления информацией, которые обеспечивают ее эффективную защиту.

Меры по обеспечению информационной безопасности помогают защитить всю информационную инфраструктуру РИСКИ от негативных воздействий. Такие воздействия могут носить как случайный, так и преднамеренный, как внутренний, так и внешний характер. Результатом таких вмешательств могут стать потеря важной информации, ее несанкционированное изменение или использование третьими лицами. Поэтому информационная и кибер безопасность - это важные аспекты защиты РИСКИ и обеспечения его непрерывного функционирования. Основными принципами эфективного внедрения систем информационной и кибер безопасности в РИСКИ являются обеспечение конфиденциальности, целостности и доступности.

Обеспечить полноценную и надежную информационную безопасность РИСКИ можно только при условии применения комплексного и системного подхода. Система инфо и кибер безопасности должна быть построена с учетом всех актуальных угроз и уязвимостей, также с учетом тех угроз, которые могут возникнуть в будущем. Поэтому важно обеспечить поддержку непрерывного контроля, который должен действовать постоянно. Необходимым условием является обеспечение эффективного контроля на каждом этапе жизненного цикла информации и технических подсистем, начиная с момента их поступления в РИСКИ и заканчивая потерей ими актуальности.

РИСКИ постоянно подвергаются многочисленным угрозам, которые по своему происхождению делятся на несколько видов: естественные и искуственные (преднамеренные и непреднамеренные), внутренние и внешние. Главную опасность представляют искусственные преднамеренные угрозы. Учитывая все более возрастающую роль ИС в критических инфраструктурах различных сфер и рост количества электронных транзакций, эти угрозы также бурно развиваются.

В поисках способов получения секретных сведений и нанесения вреда объектам Критической Инфраструктуры злоумышленники активно используют современные технологии и программные решения. Их действия могут наносить значительный ущерб, в том числе в виде прямых финансовых потерь или утраты интеллектуальной собственности. Поэтому информационная и кибер безопасность РИСКИ также должна строиться на базе передовых технологий с использованием актуальных средств защиты данных.

Средствами защиты информации называют устройства, приборы, приспособления, программное обеспечение, организационные меры, которые предотвращают утечку информации и обеспечивают ее сохранение в условиях воздействия всего спектра актуальных угроз.

Наиболее широкое распространение на сегодняшний день получили интеллектуальные программные средства защиты информации, такие, как средства обнаружения и идентификации угроз и уязвимостей, средства предотвращения атак и средства восстановления последствий кибератак. Они в полной мере отвечают требованиям эффективности и актуальности, регулярно обновляются, мгновенно реагируя на актуальные угрозы искусственного характера. Обеспечение информационной и кибер безопасности сегодня является насущной потребностью,

пренебрежение которой может иметь разрушительные последствия для РИСКИ. Широкий набор средств и решений, доступных на сегодняшний день для обеспечения защиты информации и технических средст информационных систем, может затруднить выбор в отношении объектов Критических Инфраструктур. Обеспечить безопасность IT-инфраструктуры позволяет определенный набор инструментов, который необходимо подбирать индивидуально. Это позволит реализовать многоуровневую систему защиты информации, которая обеспечит надежную нейтрализацию актуальных угроз.

Выбор инструментов защиты корпоративной информации при создании подобных систем должен производиться с учетом целого комплекса факторов, таких как: сферы принадлежности Критической инфраструктуры, размера и уровня технической оснащенности Информационной Системы, уровня подготовки и опыта персонала и т.д..

Необходимость осуществления практических расчетов относительно возможных последствий различного рода нежелательных кибервоздействий на РИСКИ, требует разработки целых иерархий сложных математических моделей, способных с достаточной точностью описывать и учитывать комплексное воздействие на систему, как дестабилизирующих (таких как отказы, уязвимости, угрозы, атаки и т.д.), так и стабилизирующих их функционирование факторов (таких как обнаружение, восстановление, устранение, предотвращение последствий киберинциндентов, их блокирование, пресечение, локализация и т.д.).

Аналитическое и программное моделирование процессов функционирования объектов критической инфраструктуры подверженных угрозам различных внешних воздействий и при этом, имеющих в своем составе средства по выявлению и предотвращению их последствий, широко используется при обеспечении информационной и кибербезопасности.

На основе таких моделей на этапе проектирования или эксплуатации соответствующих РИСКИ анализируется уровень их зашищенности и выбираются критерии эфективности средств защиты, разрабатываются методики и регламенты реагирования на киберинциденты [1]-[8] .

2. Объект, цель и методы исследованиия.

С учетом актуальности указанной выше проблемы, в данной статье определены объект, цель и методы исследования:

Объект исследования: процессы обеспечение Информационной (ИБ) и Кибеор Безопасности (КБ) Распределенных Информационных Систем (ИС) объектов Критических Инфраструктур (КИ) рассматриваемых в виде Многоканальных Системы Массового Обслуживания, подверженных кибер угрозам и содержащих в своем составе интелектуальные программные и аппаратные средства контроля киберсостояния объектов, обнаружения кибкругроз и уязвимостей, а также устранения их последствий.

Цель исследования: на основе аналитической модели разработанной в работе [10], создание Программной Модели с Графическим Интерфейсом пользователя, для иммитации процессов связанных с обеспечением информационной и кибер безопасности информационных систем критических инфраструктур, рассматриваемых как системы массового обслуживания потоков кибератак.

Методы исследования: Созданию программной модели осуществленного с помощью приложения app. Designer входящего в состав программного пакета Matla2019, предшествовало аналитическое моделирование с использованием методов системного анализа, основанных на использовании Теории Вероятностей, Теории Надежности и Теории Систем Массового Обслуживания (СМО), позволяющие аналитически описывать вероятностные процессы нарушений ИБ и КБ в ИС-ах Критических Инфраструктур, вызванных реализацией кибер атак, влекущих экстремальные ситуации и процессы устранения их последствий.

Идея исследования, проводимого в данной работе, заключается в создании программной модели для оценки уровня кибербезопасности Сложных Информационных Систем, позволяющей оценить качество их работы путем определения значений основных характеристик эффективной работы при различных значениях входных параметров и посредством их сравнительного анализа предоставить возможность выбора лучших вариантов таких систем, как в процессе разработки проекта, так и для организации процессов их рациональной эксплуатации.

Предпосылкой к данной работе послужили исследования, проведенные в работах [11] - [15], где обосновывается особая роль моделирования в разработке систем обеспечении кибербезопасности, обсуждаются возможные типы кибер угроз и уязвимостей, встречающиеся в них, дается их классификация, приводятся методических концепций нейтрализации этих угроз на основе комплекса мер по обеспечению безопасности и стабильного функционирования объектов в экстремальных ситуациях, вызванных подобными воздействиями.

Данному исследованию также предшествовали работы автора по разработкам аналитических и имитационных моделей сложных технических систем, рассматриваемых, как многоканальные системы массового обслуживания, опубликованные в виде статей [16] - [21].

Новизна исследования. Элементом новизны в данной работе является разработка самого Графического Интерфейса Пользователя, основанного на результатах указанной выше статьи [10] касающейся математической модели обеспечения кибербезопасности Распределенных Информационных Систем Критических Инфраструктур разработанной автором данной статьи, в которой информационные системы указанного типа рассматриваются, как многоканальные Системы Массового Обслуживания, функционирующие в условиях кибер угроз и наличия программных и аппаратных средств для контроля киберсостояния обектов и восстановления их работоспособности после кибератак.

Результаты исследования и их значимость. Разработанный Графический Интерфейс, с помощью управляющих элементов расположенных на ее панели, дает возможность изменения входных параметров рассматриваемой СМО и наблюдения за соответствующими изменениями ее характеристик с помощью элементов визуализации, таких как графические и числовые окна. Таким образом исследователям предоставляется возможность удобного и быстрого анализа исследуемых системы указанного типа на предмет оптимального и эффективного соответствия между их параметрами и характеристикаи функционирования.

3.Постановка задачи. На рисунках приведенных ниже даны схематические изображения следующих объектов, замещающих собой исследуемую РИСКИ :

- многоканальной система массового обслуживания с ограниченной очередью, представляющую собой основу каждого канала рассматриваемой единной сложной СМО с изображением соответствующего графа переходов ее состояний-Рис.1.

- исследуемой многоканальной СМО, каждый канал которого представлен в виде СМО представленной на Рис.1, с устройствами непосредственного обслуживания требований, дополненных устройствами контроля и управления каналов, а также устройствами восстановления и устранения последствий кибервоздействий-Рис.2.

-задача исследования состоит в создании математической модели, связывающей входные параметры и выходные характеристики исследуемой системы.

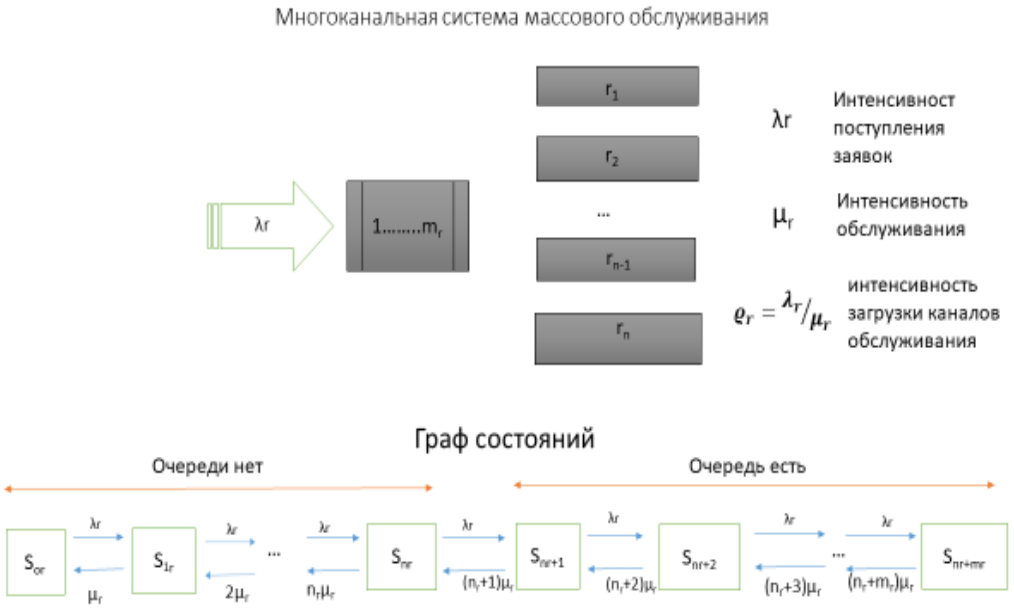


Рис.1. Структурная схема многоканальной система массового обслуживания с ограниченной очередью.

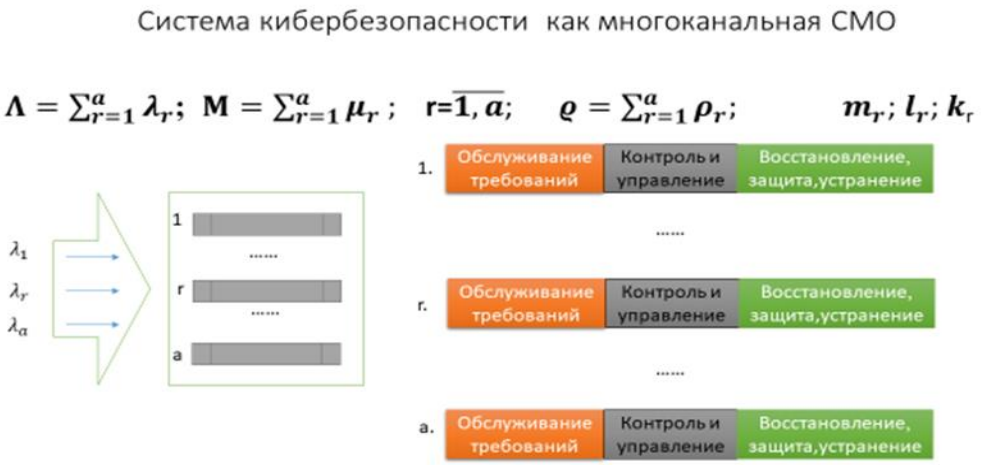


Рис2. Структурная схема исследуемой многоканальной СМО, каждый канал которого представлен в виде СМО представленной на рис.1

4.Параметры исследуемой системы. Относительно параметров структуры рассматриваемой информационной системы приняты следующие предположения:

-киберугрозы в системе подразделяются в соответствии со статусом: **обнаруженные и переданные на восстановление, обнаруженные но ожидающие восстановления (в виртуальной очереди);**

$\boldsymbol{a}$ -количество многоканальных подсистем массового обслуживания составляющих систему, где $\mathbf{a} = \overline{\mathbf{1,N}}$;

$\boldsymbol{N}-$ максимальное количество подсистем в информационной системе;

$\boldsymbol{n_r}$-количество восстанавливаемых обслуживающих каналов в каждой подсистеме, где $\mathbf{r} = \overline{\mathbf{1,a}}$;

$\boldsymbol{\lambda_r}$-интенсивность кибератак вызывающих отказы и другие нарушения в обслуживающих каналах, подчинены закону Пуассона с интенсивностью, где $\mathbf{r}=\overline{\mathbf{1,a}}$;

$\boldsymbol{m_r}$-количество мест в очереди в r-ой подсистеме;

$\boldsymbol{l_r}$-количество находящихся в каналах обслуживания $\boldsymbol{r}-$ подсистемы требований;

-вероятностные процессы восстановлений обслуживающих каналов, а также устранений последствий кибервоздействий описываются экспоненциальным законом с интенсивностью - $\boldsymbol{\mu_r}$, где $\mathbf{r}=\overline{\mathbf{1,a}}$;

-интенсивность загрузки каналов обслуживания: $\boldsymbol{\varrho_r} = {}^{\boldsymbol{\lambda_r}}/_{\boldsymbol{\mu_r}}$;

-суммарная интенсивность кибер угроз на систему: $\boldsymbol{\Lambda} = \sum_{r=1}^{a} \boldsymbol{\lambda_r}$;

-суммарная интенсивность восстановления обслуживающих каналов: $\mathbf{M} = \sum_{r=1}^{a} \boldsymbol{\mu_r}$;

-суммарная загрузка системы: $\boldsymbol{\varrho} = \sum_{\mathbf{r=1}}^{\mathbf{a}} \boldsymbol{\rho_r}$;

5.Показатели эффективности функционирования исследуемой системы.

Для целей моделирования в качестве основных характеристик эффективности функционирования исследуемой РИСКИ, приняты приведенные ниже характеристики, значения которых определяются значениями выше перечисленных параметров вероятностного характера.

$p_{k_r}^a$-суммарные предельные вероятности количества подверженных кибератакам каналов;

$p_{n_{r+l_r}}^a$-вероятность наличия в системе $(n_r + l_r)$ кибератак;

p_{query}^a –суммарное вероятное количество обнаруженных кибератак, последствия которых предстоит ликвидировать;

$p_{failure}^a$- суммарная вероятность отказа в востановлении последствий кибератаки вследствии перегрузки системы восстановления;

Q^a- суммарная относительная пропускная способность системы восстановления последствии кибератак;

A^a- суммарная абсолютная пропускная способность системы восстановления последствий кибератак;

L_{queue}- суммарное среднее число последствий кибератак ожидающих восстановления последствий;

$L_{service}$- среднее число заявок обслуживаемых СМО за единицу времени;

L_{qs}- суммарное среднее число киберинциндентов находящихся как в поцессе ликвидации их последствий, так и ожидающх такого процесса.

6. Математическая модель исследуемой системы кибербезопасности. В результате соответствующих преобразований функциональных зависимостей, описывающих исходную базовую модель многоканальной СМО с неограниченной очередью, получена новая модель функционирования исследуемой системы в виде приведенных ниже математических соотношений описывающих взаимосвязи между ее входными параметрами и выходными характеристиками:

$$p_0^a = \sum_{r=1}^{a} p_0^r = \sum_{r=1}^{a} \left[\sum_{k=0}^{n} \frac{\rho_r^k}{k_r!} + \frac{\rho_r^{n_r+1}}{n_r!*(n_r-\rho_r)} * \left(1 - \left(\frac{\rho_r}{n_r}\right)^{m_r}\right)\right]^{-1}, \quad k_r=0; \quad r=\overline{1,a}; \qquad (1)$$

Суммарные предельные вероятности при $k_r=\overline{0,n_r}$, где k_r-количество подверженных кибератакам каналов, а n_r-количество каналов в r-ой подсистеме,

$$p_{k_r}^a = \sum_{r=1}^{a} \frac{\rho_r^{k_r}}{k_r} p_0^r, \quad r=\overline{1,a}, \quad k_r=\overline{1,n_r}; \qquad (2)$$

$$p_{n_r+l_r}^a = \sum_{r=1}^{a} \frac{\rho_r^{n_r+l_r}}{n_r^{l_r} * n_{r!}} p_0^r, \quad r=\overline{1,a}, \quad n_r \le b_r \le m_r; \qquad (3)$$

Вероятность наличия в системе $(n_r + b_r)$ кибератак, из которых n_r – в процессе восстановлен их последствий, а

		b_r -в ожидании такого процесса
$p^a_{query}=\sum_{r=1}^{a}\sum_{l=0}^{n_r+m_r-1} p^r_{n_r+1}=\sum_{r=1}^{a}\sum_{l=0}^{n_r+m_r-1}\frac{\rho^{n_r}}{n_r!}*\frac{1-(\frac{\rho_r}{n_r})^{m_r}}{1-\frac{\rho_r}{n_r}}p^r_0,$ r=$\overline{1,a}$	4	Суммарное вероятное количемтво обнаруженных кибератак, последствия которых, предстоит ликвидировать.
$p^a_{failure}=\sum_{r=1}^{a} p^r_{n_r+m_r}=\sum_{r=1}^{a}\frac{\rho^{n_r+m_r}}{n_r^{m_r}*n_r!}*p^r_0,\ \ k_r=n_r+m_r,$ r=$\overline{1,a}$	5	Суммарная вероятность отказа в востановлении последствий кибератаки вследствии перегрузки системы восстановления
$Q^a=p^a_{service}=1-p^a_{failure}=\sum_{r=1}^{a}(1-\frac{\rho^{n_r+m_r}}{n_r^{m_r}*n_r!}*,),$ r=$\overline{1,a}$;	6	Суммарная относительная пропускная способность системы восстановления последствии кибератак
$A^a=\sum_{r=1}^{a}\lambda_r*Q^r=\sum_{r=1}^{a}\lambda_r*(1-\frac{\rho^{n_r+m_r}}{n_r^{m_r}*n_r!})*p^r_0,$ r=$\overline{1,a}$;	7	Суммарная абсолютная пропускная способность системы восстановления последствий кибератак
$L_{queue}=\sum_{r=1}^{a}\sum_{i=1}^{m}\frac{\rho^{n_{r+1}}}{n_r*n_r!}*\frac{1-(\frac{\rho_r}{n_r})^{m_r}*[1+m_r(1-\frac{\rho_r}{n_r})]}{(1-\frac{\rho_r}{n_r})^2}p^r_0$ r=$\overline{1,a}$;	8	Суммарнон среднее число кибератак ожидающих восстановления последствий
$L^a_{service}=\sum_{r=1}^{a}\frac{A^r}{\mu_r}=\sum_{r=1}^{a}\rho*(1-\frac{\rho^{n_r+m_r}}{n_r^{m_r}*n_r!})*p^r_0,$ r=$\overline{1,a}$;	9	Среднее число заявок обслуживаемых СМО за единицу времени
$L^a_{qs}=L^a_{queue}+L^a_{service}$	10	Суммарное среднее число киберинциндентов находящихся как в поцессе ликвидации их последствий, так и ожидающх такого процесса

Таблица 1. Основные характеристики модели обеспечения кибербезопасности.

7.Разработка программной модели

```
  % Callbacks that handle component events
    methods (Access = private)

 % Button pushed function: STARTCALCULATIONButton
   function STARTCALCULATIONButtonPushed(app, event)
   syms   ro  Po s aa  Lambda Miu k P P0 SPo Pk SPk SPni Pn s1 s2 s3 s4 s5 s6 s7 s8 s9
   syms f1 f2 f3 Sf1 Sf2 r a b  m  I K Q A SPfailure SLqueue Lqs SSLquery SPo

           r=int16(app.rKnob.Value);
           a=int16(app.aKnob.Value);
           n=int16(app.nKnob.Value);
           m=int16(app.mKnob.Value);
           Lambda=int16(app.LambdaKnob.Value);
           Miu=int16(app.MiuKnob.Value);
           b=int16(app.bKnob.Value) ;
           k=int16(app.kKnob.Value);

             for rr=1:r
               for aa=1:a
                for kk=1:k
                    for nn=1:n
                      for mm=1:m
                        for bb=1:b

                     ro(rr)=int16(Lambda(rr))/int16(Miu(rr)) ;

for kk=1:k


     f1 =(ro(rr)^kk(rr))/factorial(kk(rr))
     s=0
     s=s+f1(rr)
     Sf1=(sum(s,rr))

     f2=(ro(rr)^n(rr))/(factorial(n(rr))*(n(rr)-ro(rr)))
     f3=(1-((ro(rr)/n(rr))^mm(rr)))
     Po=(Sf1+f2+f3)^(-1)  % финальная вероятность состояния системы кибербезопасности
%при к=0, когда в системе не  фиксируются последствия кибератак;
     s1=0
     s1=s1+Po
     SPo=sum(s1,rr)
     end
 Pk=(ro(rr)^kk(rr)/factorial(kk))*SPo;  %финальные вероятности состоянии системы
%кибербезопасности при k>0,  когда в системе фиксируются k последствий кибер атак,
% требующих восстановления;
      s2=0;
      s2=s2+Pk;
      SPk=sum(s2,kk);
```

```
Pnb= ro(rr)^(n(rr)+b(rr))/(n(rr)^b(rr)*factorial(n(rr)))*SPo;  %вероятность того, что из
общего количества последствий кибератак (n+b), n-находятся в процессе восстановления,
%a b-находятся в поцессе ожидания восстановления;
    s3=0;
    s3=s3+Pnb;
    SPnb=sum(s3,rr);

Pquery=ro(rr)^n(rr)/factorial(n(rr))*((1-(ro(rr)/n(rr))^m(rr))/(1-ro(rr)/n(rr))*SPo);   %
суммарное количество ожидаемых последствий кибератак,  требующих восстановлений;
    s4=0;
    s4=s4+Pquery;
    SPquery=sum(s4,rr);
    Pfailure=ro^(n(rr)+m(rr))/(n(rr)^m(rr)*factorial(n(rr)))*SPo;  % суммарная %вероятность
отказов в восстановлении последствий кибератак в результате перегрузки
% системы восстановления;
    s5=0;
    s5=s5+Pfailure;
    SPfailure=sum(s5,rr);
Q=1-SPfailure(rr);  % Относительная пропускная способность системы восстановления
последствий кибератак.
A=Lambda(rr)*Q(rr); % Абсолютная пропускная способность системы восстановления последствий
кибератак;
Lqueue=(ro(rr)^n(rr)/(n(rr)*factorial(n(rr)))*((1-(ro(rr)/n(rr))^m(rr))*(1+m(rr)*(1-
ro(rr)/n(rr))))/(1-ro(rr)/n(rr))^2)*Po(rr);
   s6=0;
   s6=s6+Lqueue;
   SLqueue=sum(s6,mm);
   SSLqueue=double(sum(SLqueue,rr));% Суммарное среднее число кибер-инциндентов ожидающих
процесса устранения их последствий;
Lservice=A(rr)/Miu(rr);
   s7=0;
   s7=s7+Lservice;
SLservice=sum(s7,rr); % Среднее число сервисов по восстановлению последствий ибератак,
требующихся в единицу времени;

Lqs=double(SSLqueue)+double(SLservice); %Суммарное среднее число последствий  кибер-
% ициндентов  находящихся, как в процессе  устранения их последствий, так и ожидающих
такого процесса;

            % Вывод результатов расчетов функциональных характеристик системы
                        % обеспечения кибер безопасности ИС

   app.SPoEditField.Value=double(SPo)
   app.SPkEditField.Value=double(SPk)
   app.SPnbEditField.Value=double(SPnb)
   app.SPqueryEditField.Value=double(Pquery)
   app.SPfailureEditField.Value=double(SPfailure)
   app.SSLqueueEditField.Value=double(SSLqueue)
   app.AEditField.Value=double(A)
   app.QEditField.Value=double(Q)
   app.LserviceEditField.Value=double(Lservice)
   app.LqsEditField_2.Value=double(Lqs)
```

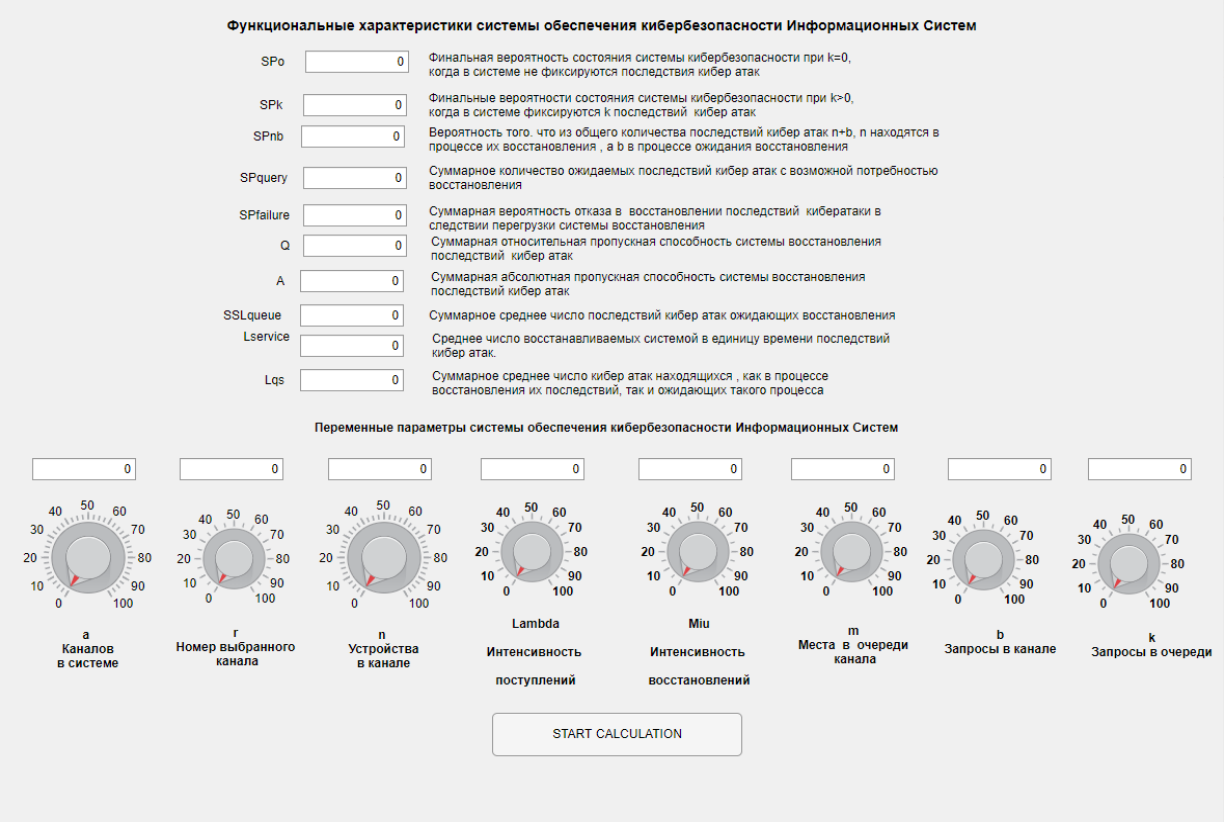
```
            end
        end

    end
end

end
```

Графический Интерфейс Пользователя описанной выше программной модели.

На рисункн внизу показан Графический Интерфейс Пользователя программнной модели который был описан выше.он представляет собой программную панель на которой размещены элементы управления, такие, как вращающиеся рукоятки для ввода цифровых значений переменных значений модели, редактируемые окна для отображения вводимых значений переменных,а также редактируемые окна для вывода значений функциональных характеристик моделируемой системы. Указанный графический интерфейс позволяет исследовать зависимость функциональных характеристик различных вариантов построения систем кибер безопасности описанной выше структуры, от значений входных параметров, которые легко могут менятся с помощью соответствующих регуляторов.



8.Заключение. В данной статье в соответствии с ее целью, при помощью приложения App Designer программной среды Matlab 2019 и на основании аналитической модели обеспечения кибербезопасности Распределенных Информационных Систем Критических объектов,

разработанной автором данной статьи в [10], создан Графический Интерфейс, позволяющий исследовать зависимости характеристик исследуемых систем от изменений их параметров.

Тем самым обеспечивается возможность оценки уровня киберзащищенности различных вариантов, проектируемых или эксплуатируемых РИСКИ с целью выбора наилучшего с точки зрения характеристик инфо и киберзашищенности.

Литература

[1] Klimov S.M., Polikarpov C.B., Rijov B.C., Tichonov R.I.,Shpirnja I.V. Metodika obespechenija ustoichivosti funkcionirovanija kriticheskoi informacionni infrastrukturi v uslovijax informacionnix vozdeistvii// Voprosi kiberbezopasnosti. 2019. № 6(34).

[2] Kondakov C.E., Mesherjakov T.B., Scril C.B., Stadnik A.H., Suvorov A.A. Verojtnostnoe predstavlenie uslovii sovremennogo reagirovanija na ugrozi kompiuternix atak // Вопросы кибербезопасности. 2019. № 6(34).

[3] Zaxarchenko R.I.,Koroliov I.D. Model funkcionirovanija avnomatizirovannoi informacionnoi sistemi v kibrprostranstve // Voprosi kiberbezopasnosti. 2019. № 6(34).

[4] Gapanovich V.A., Chubinskii I.B., Zamuchljev A.M. Metod ozenki riskov sistemu iz raznotipnuch elementov// Nadezhnost. 2016. Tom 16. №2 s.49-53.

[5]. Klimov S.M., Kotjchev N.N. Metod regulirovanij riskov kompleksov sredstv avtomatizacii v uslovijch kompjyternuch atak// Nadezhnost. 2013. №2 s. 93-107.

[6] Chubinskii I.B., Funkcionalnaj nadezhnost informacionnuch system. Metodu analiza/ I.B Chubinskii. - Uljnovsk: Oblastnaj tipografij «Pechatnui dvor», 2012. 296 s.

[7] Bezkorovainy, M. and Tatuzov, A. (2014) Cybersecurity—Approaches to the Definition. Voprosi Kiberbezopasnosti, No. 1.

[8] Starovojtov, A.V. (2011) Cybersecurity as an Actual Modern Problem. Informatization and Communication, 6, 4-7.

[9] Bezkorovajnyj, M.M., Losev, S.A. and Tatuzov, A.L. (2011) Cybersecurity in the Modern World: Terms and Content. Informatization and Communication, 6, 27-32.

[10] Shamugia, R.R. (2020) Development of an Analitical Model of the Process of Cybersecurity Protection of Distributed Information Systems of Critical Infrastructure. International Journal of Communications, Network and System Sciences, 13, 161-169. https://doi.org/10.4236/ijcns.2020.1310010

[11] Saati, T.L. (1965) Elements of Queuing Theory and Its Application. Sovetskoe Radio, Moscow, 510.

[12] Cherkesov, G.N. (1974) Dependability of Technical Systems with Time Redundancy. Sovetskoe Radio, Moscow, 296.

[13] Gnedenko, B.V. and Kovalenko, I.N. (2012) Introduction to Queuing Theory. LKT, 400.

[14] Feller, W. (1971) An Introduction to Probability Theory and Its Applications. Vol. 2, John Willey and Sons, New York, 766.

[15] Shubinski, I.B. (2016) Nadejnie otkazoustoichivie informacionnie sistemi. Metodi sinteza- M. Jurnal Nadejnost, 546 str.il.

[16] Shamugia R.R. (2014) On One Model of Complex Technical Queuing System with Unreliable Devices and with Time Redundancy. International Journal of Communications, Network and System Sciences, 7, 257-264. https://doi.org/10.4236/ijcns.2014.78028.

[17] Shamugia R.R. (2014) On One Model of Multichannel Queuing System with Unreliable Repairable Servers and Input Memory. International Journal of Communications, Network and System Sciences, 7, 279-285. https://doi.org/10.4236/ijcns.2014.78030

[18] Shamugia R.R. (2015) On One Analytical Model of a Probability Estimation of Quality and Efficiency of Functioning of Complex Technical Queuing Systems. International Journal of Communications, Network and System Sciences, 8, 295-303. https://doi.org/10.4236/ijcns.2015.88029

[19] Shamugia R.R. (2016) Probabilistic Model of Technical Queuing Systems with Subsystems for Detection and Recovery of Failures. International Journal of Communications, Network and System Sciences, 9, 305-310. https://doi.org/10.4236/ijcns.2016.98027

[20] Ramaz R. Shamugia, Development of the Software Application with Graphical User Interface for One Model Cyber Security, International Journal of Communications, Network and System Sciences Vol.12 No.12, Pub. Date: December 13, 2019, DOI: 10.4236/ijcns.2019.1212014 ;

[21] Shamugia, R.R. (2018) Development and Investigation of the Program Model of Multichannel Queueing System with Unreliable Recoverable Servers in Matlab Environment. International Journal of Communications, Network and System Sciences, 11, 229-237. https://doi.org/10.4236/ijcns.2018.1111014

Ramaz Shamugia

Creation of a Software Model with a Graphical User Interface for simulating the processes of functioning of subsystems of information and cyber protection of Distributed Information Systems of Critical Infrastructures

Annotation. This article is dedicated to the development of a software model with a Graphical User Interface (GUI) to simulate the process of ensuring information and cyber security of information systems (IS) of Critical Infrastructure objects (CI) based on the analytical model developed by the author of this article. The specified software model with a GUI makes it possible, using the controls located on the main panel, to set the input parameters of the simulated object and observe its output characteristics using appropriate visualization elements such as special windows for displaying calculated numerical values of the main characteristics of the systems under study.

რამაზ შამუგია

მომხმარებლის გრაფიკული ინტერფეისის მქონე პროგრამული მოდელის შემუშავება კრიტიკული ინფრასტრუქტურის განაწილებული საინფორმაციო სისტემების ინფორმაციული და კიბერ უსაფრთხოების უზრუნველმყოფი ქვესისტემების ფუნქციონირების პროცესების სიმულაციისათვის.

ანოტაცია. წარმოდგენილი სტატია ეძღვნება ავტორის მიერ ადრე შემუშავებული ანალიტიკური მოდელის ბაზაზე, მომხმარებლის გრაფიკული ინტერფეისის მქონე (მგი) პროგრამული მოდელის შემუშავებას, კრიტიკული ინფრასტრუქტურების ობიექტების საინფორმაციო სისტემებისათვის, ინფორმაციული და კიბერ უსაფრთხოების უზრუნველმყოფი ქვესისტემების მუშაობის პროცესების სიმულაციისათვის. აღნიშნული პროგრამული მოდელი გრაფიკული ინტერფეისით, მის მთავარ პანელზე განთავსებული რეგულირების ელემენტების საშუალებით, შესაძლებელს ხდეის მოდელირების ობიექტების შემავალი პარამეტრების მნიშვნელობების ფორმირების და გამომავალ ფუნქციონალური მახასიათებლებზე დაკვირვების წარმოების შესაძლებლობას ვიზუალუიზაციის შესაბამისი ელემენტების მეშვეობით.