ОБ ОДНОЙ ПРОГРАММНОЙ МОДЕЛИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Шамугиа Рамаз

Сухумский физико-технический институт Ильи Векуа
Сухумский государственный университет

Аннотация

В с вязи с большой сложностью компьютерных сетей и невозможностью точного воспроизведения происходящих в них реальных событий, в том числе в силу некоторых возможных негативных последствий, исследовательское моделирование приобрело важную роль в исследованиях, связанных с защитой от компьютерных атак и разработкой механизмов и средств кибербезопасности. В связи с вышеизложенным в предлагаемом докладе представлено краткое изложение результатов исследования проведенного автором, в которой в качестве объекта моделирования рассматривается прооцесс функционирования сложной информационной системы, подверженной угрозам кибербезопасности. При этом, указанная информационная система представлена в виде сложной системы массового обслуживания, состоящей из подсистем, каждая из которых представляет собой многоканальную СМО с неограниченной очередью. Получены аналитические соотношения для характеристик описанной системы и на их основе разработана программная модель оценки эфективности функционирования.

Введение

Стремительное развитие информационных технологий и их всеобщее проникновение во все сферы человеческой деятельности, а также происходящие во всем мире пороцессы глобализации, при котором информационные системы всего мира слиты в единное, глобальное информационное пространство называемое киберпространством, приводят к необходимости обеспечения их гарантированной защиты от негативных воздействии извне.

Из за сложных структур и характера взаимодействия между элементами сложных информационных систем в вышеуказанном пространстве (информационные системы управления в энергетике, телекоммуникационных и транспортных сетях, кредитных и финансовых системах, в информационных системах государственного и военного назначения, представляющих собой пространственно-распределенные и многокомпонентные структуры, именуемые как КИ-критические инфраструктуры), анализ бесперебойного и эффективного функционирования с помощью традиционных методов неэффективен [1].

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

Моделирование процессов функционирования ИС подверженных угрозам различных внешних воздействий и мерам по предотвращению их последствий, широко используется при обеспечении информационной и кибербезопасности. На их основе анализируется уровень зашищенности объекта и выбираются критерии эфективности средств защиты, разрабатываются методики и регламенты реагирования на киберинциденты [2].

1.Постановка практической проблемы. Даннаый доклад посвящен разработке наиболее обобщенной, укрупненной и масштабируемой программной модели системы обеспечения кибербезопасности, которая представлена в виде сложной системы,

состоящей из определенного количества Многоканальных Подсистем Массового Обслуживания с неограниченной очередью, подверженных воздействию различных типов киберугроз, вызывающих нежелательные последствия в обслуживающих каналах [3].

Исследования проведены в предположении, что все каналы подсистем рассматриваемой информационной системы, в своем составе, наряду с устройствами непосредственно обслуживающими технологические требования, содержат комплексную интеллектуальную подсистему управления, контроля и защиты от последствий кибервоздействий соответствующего типа, обеспечивающую:

- постоянный мониторинг с целью обнаружения, идентификации и регистрации различных нарушений функционирования системы, происходящих, как в результате обычных причин (отказы), так и в результате кибервоздействий различных типов нарушающих целостность, конфиденциальность и доступность;

-инициирование процессов восстановления отказавщих устройств или ликвидаций последствий от кибервоздействий по любой из возможных причин, в соответствующих устройствх, предусмотренных в каналах и осуществляемых программными или аппаратными способами;

-возможность нахождения информационной стстемы под совместным воздействием различных типов киберугроз, в том числе запроса на несанкционированный доступ, вирусы, спам, удаленный взлом, фишинг, DoS/DDoS-атаки и т.д., происходящих случайным образом в соответствии с известными законами распределения вероятностей.

-наличие восстанавливающих средств соответстающих по своим назначениям, характеристикам и возможностям, ожидаемым типам кибервоздействий, а также устройств управления восстановлением как вышедших из строя каналов обслуживания, так и устранения последствий кибервоздействий, способствующих обеспечению эффективного функционирования информационной 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 ждущие восстановления;

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

- $N -$ максимальное количество подсистем в информационной системе;

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

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

-количество мест в очереди в r-ой подсистеме равно - m_r;

- количество находящихсяв каналах обслуживания r-ой подсистемы требований – l_r ;

-количество находящихся в очереди $r -$ ой подсистемы требований $- k_r$;

-восстановление обслуживающих каналов, а также устранение последствий кибервоздействий подчинено экспоненциальному закону с интенсивностью - μ_r, где r=$\overline{1,a}$;

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

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

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

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

2.Перечень решаемых задач. В докладе осуществлены решения следующих задач:

- в качестве основы моделирования выбрана одна из хорошо изученных в литературе моделей многоканальной системы массового обслуживания с неограниченной очередью;

-проведено обобщение, которое предусматривает рассмотрение вышеуказанной системы в качестве составной подсистемы, входящей в более общую, укрупненную и масштабируемую систему, представляющую собой совокупность нескольких аналогичных вышеописанному подсистем ;

-получены новые математические соотношения для различных характеристик указанной обобщенной, укрупненной и масштабируемой системы, как системы массового обслуживания, подверженной кибератакам различной природы и различной интенсивности;

- на основе полученных новых математических соотношения для различных характеристик данной обобщенной модели в программной среде Matlab 2020 разработана программная модель учитывающая все ее специфические особенности.

3.Изложение сути исследования. Суть иследования проведенной в данной работе состоит в создании аналитической и программной моделей процесса обеспечения кибербезопасности сложных информационных систем, которые позволят иммитировать (симулировать) процессы их работы с целью определения значений основных характеристик эффективности функционирования, при различных значениях входных параметров и путем их сравнительного анализа, давать возможность выбора наилучших вариантов структур таких систем, как в поцессе их проектирования, так и в процессе их рациональной эксплуатации.

Таблица 1 – Основные характеристики модели обеспечения кибербезопасности.

$p_0^a = \sum_{r=1}^{a} p_0^r = \sum_{r=1}^{a} \left[\sum_{k=0}^{n} \frac{\rho_r^k}{k_r!} + \frac{\rho_r^{n_r+1}}{n_r!*(n_r-\rho_r)} * \left(1 - \left(\frac{\rho_r}{n_r}\right)^{m_r}\right)\right]^{-1}$, k_r=0; r=$\overline{1,a}$	1	Суммарные предельные вероятности при k_r=$\overline{0,n_r}$, где k_r-количество подвержен-ных кибер-атакам каналов, а n_r-количество каналов в r-ой подсистеме,
$p_{k_r}^a = \sum_{r=1}^{a} \frac{\rho_r^{k_r}}{k_r} p_0^r$, r=$\overline{1,a}$, k_r=$\overline{1,n_r}$;	2	
$p_{n_r+l_r}^a$=$\sum_{r=1}^{a} \frac{\rho_r^{n_r+l_r}}{l_r} p_0^r$, r=$\overline{1,a}$, $n_r \le l_r \le m_r$;	3	Вероятность наличия в системе $(n_r + l_r)$ кибератак, из которых n_r – в процессе восстановления их последствий, а l_r – в ожидании такого процесса
$p_{\text{очер}}^a$=$\sum_{r=1}^{a} \sum_{l=0}^{n_r+m_r-1} p_{n_r+1}^r = \sum_{r=1}^{a} \sum_{l=0}^{n_r+m_r-1} \frac{\rho^{n_r}}{n_r!} * \frac{1-(\frac{\rho_r}{n_r})^{m_r}}{1-\frac{\rho_r}{n_r}} p_0^r$, r=$\overline{1,a}$	4	Суммарное вероятное количемтво обнаруженных кибератак, последствия которых, предстоит ликвидировать.
$p_{\text{отк}}^a$=$\sum_{r=1}^{a} p_{n_r+m_r}^r = \sum_{r=1}^{a} \frac{\rho^{n_r+m_r}}{n_r^{m_r}*n_r!} * p_0^r, k_r = n_r + m_r$, r=$\overline{1,a}$	5	Суммарная вероятность отказа в востановлении последствий кибератаки вследствии перегрузки системы восстановления
Q^a=$p_{\text{обсл}}^a$=1-$p_{\text{откл}}^a$ = $\sum_{r=1}^{a}(1 - \frac{\rho^{n_r+m_r}}{n_r^{m_r}*n_r!}*,)$, r=$\overline{1,a}$;	6	Суммарная относительная пропускная способность системы восстановления последствии кибератак
$A^a = \sum_{r=1}^{a} \lambda_r * Q^r = \sum_{r=1}^{a} \lambda_r * (1 - \frac{\rho^{n_r+m_r}}{n_r^{m_r}*n_r!}) * p_0^r$, r=$\overline{1,a}$;	7	Суммарная абсолютная пропускная способность системы восстановления последствий кибератак

$L_{\text{очер}} = \sum_{r=1}^{a} \sum_{i=1}^{m} \frac{\rho^{n_r+1}}{n_r * n_r!} * \frac{1-(\frac{\rho_r}{n_r})^{m_r}*[1+m_r(1-\frac{\rho_r}{n_r})]}{(1-\frac{\rho_r}{n_r})^2} p_0^r;$	r=$\overline{1,a};$ 8	Суммарнон среднее число кибератак ожидающих восстановления последствий
$L^a_{\text{обсл}}=\sum_{r=1}^{a} \frac{A^r}{\mu_r}=\sum_{r=1}^{a} \rho * (1 - \frac{\rho^{n_r+m_r}}{n_r^{m_r} * n_r!}) * p_0^r,$	r=$\overline{1,a};$ 9	Среднее число заявок обслуживаемых СМО за единицу времени
$L^a_{\text{смо}} = L^a_{\text{очер}} + L^a_{\text{обсл}}$	10	Суммарное среднее число киберинциндентов находящихся как в поцессе ликвидации их последствий, так и ожидающх такого процесса

4. Формулировка выводов:

-разработаны новая аналитическая и программная модели обеспечения кибербезопасности информационных систем, рассматриваемых, как сложные системы массового обслуживания подверженные кибератакам различной природы;

-в качестве основы (базы) рассматриваемой обобщенной системы принята хорошо известная в литературе и имеющая широкое практическое применение, многоканальная система массового обслуживания с неограниченной очередью;

-в результате соответствующего преобразования хорошо известных математических соотношений описывающих характеристики базовой СМО, получены новые аналитические соотношения, отображающие зависимости входных параметров и выходных характеристик обобщенной модели и описывающие ее функционирование в условиях кибератак;

-на основе полученных аналитических соотношений, в среде Matlab 2020, разработана программная модель позволяющая проводить симуляцию работы описанной обобщенной СМО под воздействием киберугроз и оценивать различные сценарии функционирования системы.

Список использованных источников

1.Bezkorovainy, M. and Tatuzov, A. Cybersecurity—Approaches to the Definition. Voprosi Kiberbezopasnosti, No. 1, 2014.

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

3.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