Представлено метод оцінювання інформаційної стійкості соціотехнічних систем, які знаходяться під впливом спеціальних інформаційно-психологічних операцій, що проводяться в ході інформаційної війни. Метод використовує логіко-імовірнісну модель і імовірнісний показник для оцінки інформаційної стійкості системи. Імовірнісний показник базується на понятті мінімальної одиниці інформації, призначеної для зміни свідомості людини – мема. Запропонований метод доцільно використовувати для підготовки і прийняття рішень з управління комплексною інформаційною безпекою на рівні «підприємство-регіон-держава»

Ключові слова: інформаційна війна, інформаційна стійкість, інформаційно-психологічна операція, імовірнісний показник стійкості, інформаційний мем

Представлен метод оценивания информационной устойчивости социотехнических систем, которые находятся под воздействием специальных информационно-психологических операций, проводимых в ходе информационной войны. Метод использует логико-вероятностную модель и вероятностный показатель для оценки информационной устойчивости системы. Вероятностный показатель базируется на понятии минимальной единицы информации, предназначенной для изменения сознания человека – мема. Предложенный метод целесообразно использовать для подготовки и принятия решений по управлению комплексной информационной безопасностью на уровне "предприятие-регион-государство"

Ключевые слова: информационная война, информационная устойчивость, информационно-психологическая операция, вероятностный показатель устойчивости, информационный мем

УДК 004.056
DOI: 10.15587/1729-4061.2016.65691

МЕТОД ОЦЕНКИ ИНФОРМАЦИОННОЙ УСТОЙЧИВОСТИ СОЦИО-ТЕХНИЧЕСКИХ СИСТЕМ В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ВОЙНЫ

А. В. Дудатьев
Кандидат технических наук, доцент*
E-mail: dudatyev.av@gmail.com
В. А. Лужецкий
Доктор технических наук, профессор, заведующий кафедры*
E-mail: lva_zi@mail.ru
Д. А Коротаев
Аспирант*
E-mail: dmitriy.mymail5@gmail.com
*Кафедра защиты информации
Винницкий национальный технический университет
Хмельницкое шоссе, 95,
г. Винница, Украина, 21021

1. Введение

В условиях ведения информационной войны возрастает роль адекватного управления комплексной информационной безопасностью, обеспечивающего устойчивое функционирование социотехнических систем (СТС). Информационная война или информационное противодействие может возникнуть и проводиться на разных уровнях управления информационной безопасностью СТС – уровне отдельного предприятия, уровне отдельного региона, который может включать комплекс объектов защиты, и самом высоком уровне – уровне государства, который, в свою очередь, включает множество регионов. При этом очевидным является факт зависимости информационной защищённости уровней системы.

Социотехническая система, структура которой представлена на рис. 1, включает техническую и социальную части, а также различные среды, такие как информационная, технологическая, экологическая и т. п. Объектом, против которого проводятся специальные информационные операции, в частности информационно-психологические операции (ИПО), является человек как элемент социотехнической системы, а целью информационного воздействия является перепрограммирование его сознания.

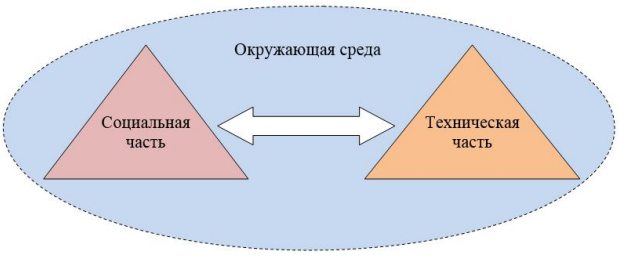

Рис. 1. Состав СТС

Эффективно проведенная ИПО способна вывести из управляемого состояния всю СТС, сделать её неу-

стойчивой и ввести в состояние управляемого извне хаоса. Использование технологий управляемого хаоса направлено на решение основной задачи – уменьшение численности конкурентов, представляющих определенную опасность, путем их ослабления или уничтожения и завоевания лидирующего положения на определённом сегменте рынка. Управляемый хаос может быть реализован путем проведения специальных информационных операций. Жизненный цикл СТС, которая находится в условиях внешнего информационного воздействия, представлен на рис. 2.

Проведение информационной войны сопровождается увеличением количества средств и угроз, расширением методов ведения информационного противодействия, о чём свидетельствует увеличение количества инцидентов в различных регионах мира.

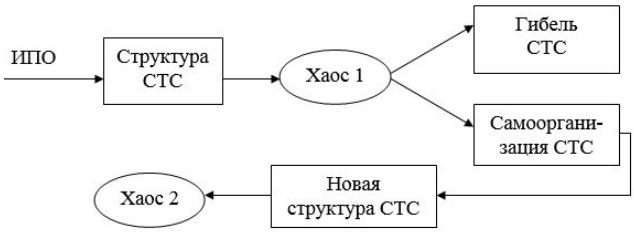

Рис. 2. Жизненный цикл СТС

Таким образом, актуальность исследования направлена на дальнейшее развитие методов обеспечения комплексной информационной безопасности и оценки информационной устойчивости СТС в условиях проведения специальных информационных операций.

2. Анализ литературных источников и постановка проблемы

Для любого объекта защиты, например предприятия, стремящегося к выходу на новый конкурентный рынок или государства в целом, вопросы комплексной защиты информационных ресурсов и обеспечения устойчивого функционирования приобретают особую важность. Это обусловлено в первую очередь экономическими, политическими, геополитическими процессами, происходящими на том или ином уровне объекта защиты. Особую остроту эти вопросы приобретают, если данные объекты являются критическими и их жизнедеятельность происходит в условиях информационной войны.

Вопросам комплексной защиты информации посвящены работы многих зарубежных и украинских учёных [1–11].

Однако, данные исследования носят фрагментарный характер. Так в работах [1, 2] рассмотрены вопроса кибертерроризма и проблемы информационных рисков на воздушном и на водном транспорте. В работах [3, 4] приведены методики оценки эффективности систем защиты информации. Метод повышения уровня информационной безопасности транспортной системы Украины рассмотрен в работе [5]. Представленный метод позволяет повысить эффективность распознавания угроз для информационно – коммуникационных систем на наземном транспорте. В работе [6] рассматривается способ выявления информационных вызовов и оценки уровня их угроз. В работе [7] рассматриваются проблемы информационного противоборства различных с точки зрения мощности финансовых ресурсов, стран. В данной работе для противодействия хаосу и дестабилизации предложены механизмы институционального, финансового, экономического и информационного управления. В статье [8] предложена математическая модель, позволяющая проводить анализ устойчивости политических систем. Представленная модель использует понятия теории информационного поля, представляющего собой поле социальных ценностей. В работе [9] представлена матрица для анализа устойчивости (RAM – The Resillence Analysis Matrix) социотехнической системы под влиянием различных инцидентов. Результаты анализа матрицы, ориентированные на конкретный случай, позволяют визуализировать состояние всей системы и в дальнейшем решить задачу прогнозирования состояния СТС. В работе [10] представлен анализ подходов оценки состояния комплексных СТС в процессе внедрения новых технологий. В ряде работ приведены результаты исследований по анализу состояния СТС, которые базируются на понятии мема. Так, в работе [11] приведены результаты по исследованию передачи мемов, предложена модель, позволяющая получить вероятностную оценку возникновения пары мемов в информационном пространстве.

В перечисленных работах, представляющих интерес при решении задач, ориентированных на определённый случай или область применения, не решается проблема оценки комплексной информационной безопасности СТС, включающей анализ текущего уровня защищённости СТС и непосредственно оценку информационной устойчивости социальной части системы, находящейся под влиянием специальных информационных операций. Также необходимо сказать, что информационную безопасность СТС, находящейся в условиях информационной войны, вопросы управления комплексной информационной безопасностью, обеспечения устойчивого функционирования социальной части и всей системы в целом, являются вопросами комплексной безопасности государства.

3. Цель задачи исследования

Целью данной работы является разработка метода оценки информационной устойчивости СТС в условиях проведения специальных информационно-психологических атак.

Для достижения поставленной цели необходимо решить такие задачи:

– выполнить анализ технологий и механизмов реализации информационно – психологических операций против СТС;

– разработать вероятностный показатель информационной устойчивости социальной части СТС.

4. Обеспечение устойчивости жизнедеятельности СТС в условиях информационной войны как элемент комплексной информационной безопасности

Социотехнические системы, в большинстве случаев, являются открытыми и неравновесными система-

ми. Нарушение равновесия в них может возникнуть вследствие самых разнообразных как внутренних, так и внешних причин, в том числе, вследствие проведения ИПО, которые по своей природе являются случайными событиями.

Анализ статистики инцидентов информационной безопасности [12] показывает, что в центре концепции комплексной информационной безопасности находится социальная составляющая, более 95 % всех инцидентов происходят по вине человека. Особенно это актуально для критических объектов управления. В качестве примера можно привести выступление эксперта из Киберцентра НАТО в Эстонии Кеннета Гирса (Kenneth Geers), который высказал предположение, что успех атаки Stuxnet зависит исключительно от контактов с "нужными людьми" и элементарных USB-накопителей. Используя «человеческий фактор» или "специально подготовленного человека" были успешно поражены 1368 из 5000 центрифуг на заводе по обогащению урана в Натанзе, вследствие чего сорваны сроки запуска ядерной АЭС в Бушере [13]. Исходя из этого, все операции по управлению комплексной информационной безопасностью должны быть нацелены на то, чтобы минимизировать риски, связанные с проведением ИПО или специальных оперативных мероприятий.

Новые угрозы, появляющиеся на всех этапах жизнедеятельности СТС, могут вызвать определённые изменения, которые целесообразно анализировать через призму ведения информационной войны.

Проведение специальных информационных операций может вызвать различные изменения в СТС, связанные с изменением структуры или связей между элементами системы и интерпретированы как перевод системы из начального (устойчивого) состояния X_0 в некоторое другое (неустойчивое) состояние X_1. Следует также учитывать, что на каждом уровне управления комплексной информационной безопасностью (КИБ) многоуровневой системы "предприятие-регион-государство" соотношение технической и социальной частей различно, что может быть выражено в проведении характерных ИПО и механизмах их реализации, а также выборе источников влияния на соответствующие уровни СТС. На рис. 3. представлено соотношение социальной и технической частей СТС.

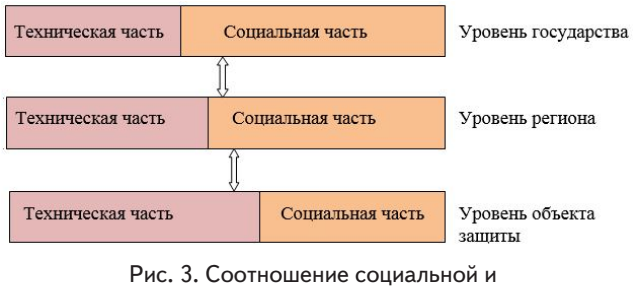

Рис. 3. Соотношение социальной и технической частей СТС

Проблема "ненасильственного перепрограммирования" социальной части СТС была решена Ричардом Доукинсом, который впервые ввёл понятие культурного гена социума – мема. Мем определяется как минимальное количество информации в сознании человека, предназначенное для его культурной эволюции. С точки зрения информационной безопасности, мемом можно назвать специально созданное информационное сообщение, которое распространяется в информационном пространстве и предназначено для формирования необходимой модели сознания человека и, как следствие, принятия соответствующих решений человеком. В работе приведена аксиоматика теории мема и функциональное сравнение мема и гена, которое для удобства приведено в табл. 1.

Таблица 1

Сравнение мема и гена

Ген	Мем
Клетка	Сознание
Биологический вирус	Информационный вызов или вирус
Набор генов	Набор мемов
Споры/микробы	Информационные сообщения
Гены и более высокие формы	Культура
Организм	Информационное пространство
Генетическая предрасположенность	Психологическая предрасположенность
Генетическая эволюция	Культурная революция

Сопоставление с генетикой относительно, поскольку распространение культурного мема сопровождается современными информационными технологиями: – "Сегодня мы располагаем иными средствами сохранения информации – носителями, которые позволяют воспроизводить, видоизменять и распространять информацию намного быстрее, чем это сделала бы ДНК." И далее: – " Новое средство сохранения информации занимает в нашей повседневной жизни значительно более важную роль, в результате генетическая эволюция и ее значение уже не играют для нас никакой роли. Оно называется сознанием, а эпликатор, который эволюционирует в нашем сознании, называется мемом." [11].

Существующие механизмы распространения мемов или проведения ИПО рассмотрены в [14]. В дальнейшем эти механизмы учтены при построении логико – вероятностной модели для оценки уровня информационной защиты социальной части СТС. Поскольку наличие ИПО или соответствующих угроз в информационном пространстве следует рассматривать как возникновение случайных событий, то и дальнейшее построение метода оценки информационной устойчивости СТС целесообразно проводить, используя вероятностные соотношения.

5. Метод оценки информационной устойчивости социотехнической системы в условиях информационной войны

Используя понятие мема, как специально созданную минимальную единицу информации, предназначенную для воздействия на сознание человека с учётом различных источников информационного влияния, представим комбинацию операций, реализующую вероятностный метод оценки информационной устойчивости социальной части социотехнической системы. Последовательность операций, реализующих предложенный метод, представлена на рис. 4.

Информационной устойчивостью социальной части СТС будем называть способность социальной части и СТС в целом возвращаться в исходное (устойчивое) состояние после нейтрализации информационно-психологической операции, нарушившей это состояние.

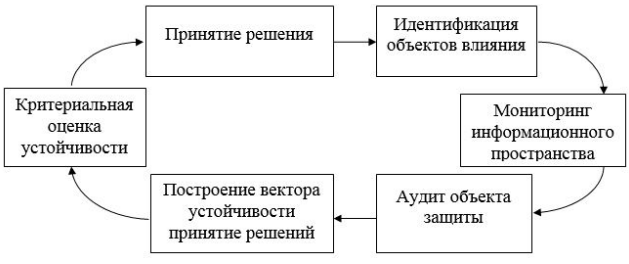

Рис. 4. Базовые процедуры процесса оценки информационной устойчивости СТС

Идентификация объектов влияния предполагает идентификацию источников распространения специально подготовленной информации.

Объектами влияния могут быть: различные средства массовой информации, телевидение, различные Internet ресурсы, социальные сети, непосредственно человек и т. п.

Мониторинг информационного пространства проводится с целью выявления в нём специальных информационных сообщений – мемов, сформированных для изменения начального состояния СТС, а также признаков наличия специальных информационно-кибернетических операций (ИКО), которые могут быть реализованы непосредственно против технической составляющей СТС, а также опосредованно через специально подготовленного человека.

Выполнение данной функции может быть реализовано с помощью специальных программ, которые позволяют отследить информационные операции технической направленности. Отследить факты нарастания соответствующих атак можно, например, по ключевым словам, таким как: атака на DNS-сервер, DDos-атака, нарастание вирусных атак, отказ в обслуживании и т. д. Иными словами, наличие в информационном пространстве устойчиво сформированных мемов позволяет судить о возможных признаках информационных угроз.

Аудит объекта защиты проводится с целью оценки текущего уровня информационной безопасности объекта, наименее защищённых мест в системе защиты, анализа рисков, выработке рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности, оценке соответствия системы безопасности существующим стандартам в области информационной безопасности.

Решение данной задачи предлагается провести с использованием логико-вероятностной модели в виде «дерева событий», фрагмент которой представлен на рис. 5.

На рис. 5 в качестве базовых событий X_1–X_n рассматриваются события, которые могут произойти в системе, или события, характерные для системы. Например, X_1 – многократное дублирование одной информации, X_2 – дезинформирование, X_3 – комбинированое информирование с использованием различных источиков (правдивая информация + ложь), X_4 – наличие “специального человека” – распространителя неподтверждённой информации.

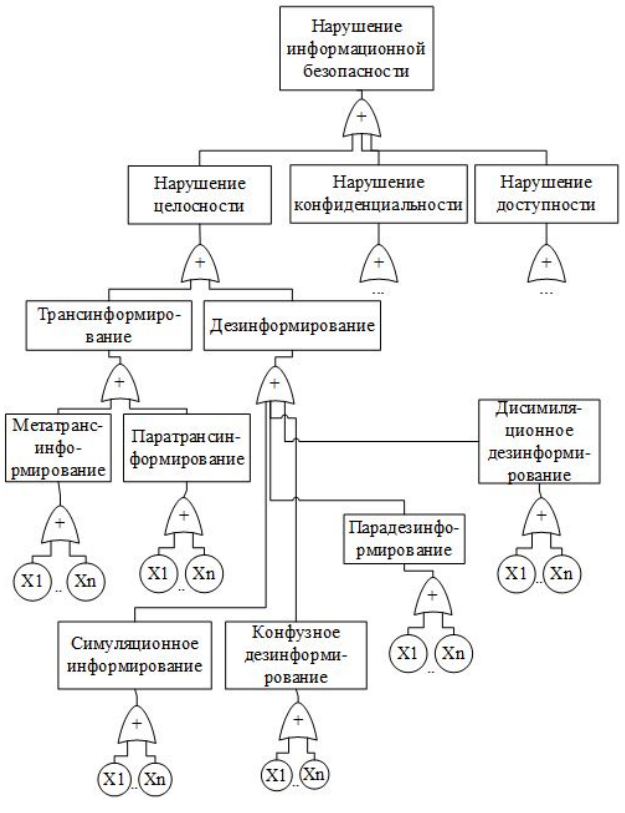

Рис. 5. Дерево событий для оценивания уровня защищённости социальной части СТС

При условии независимости базовых событий, расчет вероятностей возникновения всех событий, представленных моделью, выполняется таким образом:

– для логической функции «И»:

$$P = \prod_{j=1}^{k} P_j, \qquad (6)$$

где P_j – вероятность возникновения j-х событий, которые являются причинами появления выходного события, k – количество событий, влияющих на появление выходного события;

– для логической функции «ИЛИ»:

$$P = 1 - \prod_{j=1}^{k} (1 - P_j). \qquad (7)$$

Результатом моделирования будут вероятностные характеристики всех событий, входящих в модель, а также их ранги, что позволит построить эффективную политику безопасности [15]. Базовыми параметрами, характеризующими текущее состояние комплексной защищённости СТС, будут вероятностные оценки нарушения целостности, конфиденциальности и доступности социальной части СТС.

Результат моделирования позволит определить причинно-следственные связи, которые привели к нежелаемым событиям. Вероятностные оценки возникновения соответствующих событий являются базой для дальнейших исследований устойчивости системы.

Результат расчёта разработанной модели для ветви, представляющей логическую последовательность событий, приводящих к нарушению целостности, представлен в табл. 2. Данные, на основе которых был проведен расчёт нарушения целостности, были получены во время проведения специального эксперимента, проводящегося в условиях реального учебного процесса на протяжении семестра. Суть эксперимента заключалась в доведении до студенческой группы (общим количеством 61 студент) определённых мемов и их сочетаний с использованием различных механизмов и источников реализации ИПО. Целью проведения эксперимента было выяснение информационной устойчивости группы (выполнение графика учебного процесса) по отношению к тем специальным информационным операциям, которые проводились против неё. Показатель эксперимента – "срыв пары, срыв выполнения учебного графика и т. п." Следует отметить, что группа была проинформирована о проведении эксперимента, а само проведение эксперимента сопровождалось трудностями, связанными с различной реакцией каждого представителя группы на тот или иной доводимый мем. В качестве мемов использовались, например, такие – «преподаватель заболел, но замена будет» или «преподаватель заболел, поэтому данную тему вам необходимо рассмотреть самостоятельно». Вероятностные оценки базовых событий получены авторами при проведении описанного эксперимента.

Таблица 2

Результаты расчета вероятности нарушения целостности информации после проведения ИПО

Базовые события	Вероятности возникновения базовых событий	Выходное событие	Результат расчёта
X_1, X_2	0,08; 0,1	A-симуляционное информирование	0,17
X_3, X_4	0,15; 0,2	B-конфузное дезинформирование	0,32
X_5, X_6	0,2; 0,3	C-парадез-информирование	0,44
X_7, X_8	0,25; 0,15	D-дисимиляционное дезинформирование	0,63
X_9, X_{10}	0,35; 0,4	E-метатранс-информирование	0,61
X_{11}, X_{12}	0,4; 0,3	F-паратранс-информирование	0,58
E, F	0,4; 0,45	G-трансинформирование	0,67
A, B, C, D	0,17; 0,32; 0,44; 0,63	M-дезинформирование	0,11
G, M	0,67; 011	T-нарушение целостности	0.7

Вероятностные оценки нарушения конфиденциальности и доступности также получены в процессе проведения описанного эксперимента и позволят получить общую оценку вероятности нарушения информационной безопасности СТС.

Графическая интерпретация и визуализация полученных на предыдущем этапе вероятностных оценок нарушения конфиденциальности, целостности и доступности предполагает построение так называемого вектора устойчивости социальной части СТС. Поскольку в данном случае вектор устойчивости характеризуется тремя координатами, $(P_К, P_Ц, P_Д)$ соответственно, вероятностными оценками нарушения конфиденциальности, целостности и доступности, то и представить вектор можно, как вектор, находящийся в трёхмерном пространстве или единичном параллелепипеде (рис. 6). Графическое представление результатов моделирования позволяет получить визуальную оценку контролируемых параметров СТС.

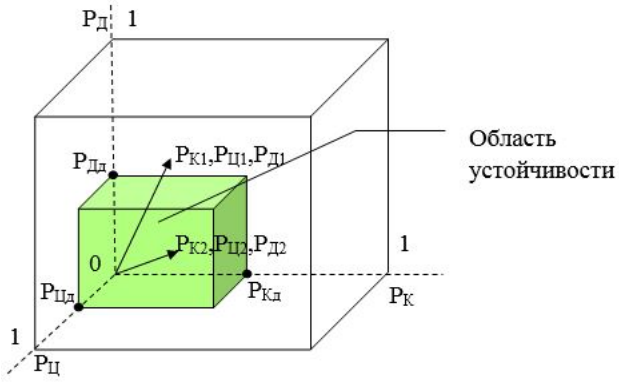

Рис. 6. Вектор устойчивости СТС

Принятие решения об устойчивости СТС после проведения ИПО или любой другой атаки на СТС базируется на анализе координат вектора устойчивости. Если одна из координат вектора устойчивости выходит за пределы внутреннего параллелепипеда, ограничивающего область устойчивости, то СТС может быть неустойчива. При этом область устойчивости ограничивается заданными значениями $(P_{Кд}, P_{Цд}, P_{Дд})$, где $P_{Кд}, P_{Цд}, P_{Дд}$, соответственно, допустимое значение нарушения информационной безопасности по конфиденциальности, целостности, доступности. Если полученные в результате моделирования значения больше значений ограничивающих область устойчивости, то СТС неустойчива. На рис. 6 вектор с координатами $(P_{К1}, P_{Ц1}, P_{Д1})$ выходит за пределы области устойчивости, что означает признак проведения эффективной атаки и вероятного входа системы в неустойчивое состояние.

Совокупность случайных значений $(P_К, P_Ц, P_Д)$, полученных в результате моделирования текущего состояния уровня защищённости социальной части СТС, можно рассматривать как n-мерный случайный вектор. Полученные случайные значения будут координатами вектора информационной устойчивости в единичном параллелепипеде, а вероятность попадания вектора с координатами $(P_К, P_Ц, P_Д)$ в область устойчивости вычисляется по формуле [16]:

$$P(P_Д < x_1, P_Ц < x_2, P_К < x_3) = F(x_1, x_2, x_3), \quad (8)$$

где $F(x_1, x_2, x_3)$ – многомерная функция распределения, которая, например, может быть получена с использованием специальных генераторов случайных значений.

Графическая интерпретация результатов моделирования может ответить на вопросы:

1) устойчива ли СТС при заданном значении ее параметров?

2) в каких диапазонах можно изменять параметры системы, не нарушая ее устойчивости?

Координаты вектора устойчивости при необходимости можно разложить на две составляющие, например, $P_К$ и $P_Ц$, которые соответствуют вероятностным оценкам нарушения конфиденциальности и целостности. Пример области устойчивости СТС по двум координатам приведен на рис. 7.

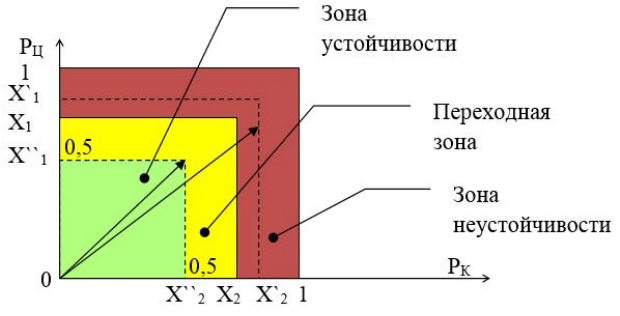

Рис. 7. Вектор устойчивости по 2-м параметрам

Для двумерного вектора устойчивости вероятность попадания в область устойчивости СТС:

$$P(a_1 \le X_1 < b_1, a_2 \le X_2 < b_2 = \\ = F(b_1,b_2) - F(b_1,a_1) - F(a_1,b_2) + F(a_1,a_2). \quad (9)$$

В расчёте, приведенном в табл. 1, вероятность нарушения целостности равна 0,7. Для заданной границы зоны устойчивости, ограниченной значениями, например, X_1=0,5 и X_2=0,5, видно, что представленные на рис. 7 два вектора демонстрируют состояние устойчивости СТС для двух результатов. Вектор с координатами $(x``_1, x``_2)$ не выходит за пределы зоны устойчивости, ограниченной координатами (x_1, x_2) а вектор с координатами $(x`_1, x`_2)$ выходит за пределы зоны устойчивости, в частности по показателю нарушения целостности, что является признаком неустойчивого состояния СТС.

Показатель информационной устойчивости формализует процесс анализа состояния информационной среды на предмет наличия в нём мема, реализующего деструктивное информационное влияние, и мема, нейтрализующего это влияние. Оценить эффективность воздействия мема сложно, поскольку процесс восприятия человеком информации, распространение этой информации сопровождается многими неопределенностями и ограничениями, которые обобщенно можно определить, как возможности и способности объективно анализировать информацию. Очевидно, что такую систему «источник влияния – объект воздействия» с соответствующими ограничениями можно рассматривать как систему массового обслуживания (СМО) разомкнуто-комбинированного типа. Такому типу СМО соответствует наличие одновременно внешнего и внутреннего источников. Внешний источник формирования мемов находится вне объекта, на который направлено влияние, и одновременно источник влияния, тиражирующий деструктивное информационное сообщение, может находиться внутри объекта воздействия.

Используя теорию меметики, будем считать изменения состояния информационной среды результатом наличия в нем нового мема или мема, на факт присутствия которого отсутствует адекватная реакция. Результатом обслуживания нового мема будем считать его нейтрализацию или формирование адекватной защиты, а факт отсутствия нейтрализации этого мема будем считать эффективно проведенной ИПО, способной вывести СТС из состояния равновесия.

Поскольку оценка текущего состояния уровня защищённости получена в виде вероятностных оценок, то и показатель информационной устойчивости целесообразно представить в виде вероятностного соотношения.

Пусть имеется k источников распространения деструктивного мема (источников влияния). При этом i-й источник направляет влияние на n_i объектов социальной части СТС. Пусть также вероятность подпадания под влияние i-го источника равна p_i. Учитывая это, количество $M_{дм}$ объектов социальной части СТС, подпавших под влияние деструктивного мема, вычисляется по формуле:

$$M_{МД} = \sum_{i=1}^{k} p_i n_i . \quad (10)$$

Пусть для нейтрализации результата влияния деструктивного мема используется т источников распространения, компенсирующего мема, из которых j-й источник направляет влияние на n_j объектов социальной части СТС. Пусть вероятность нейтрализации j-м источником равна q_j. Тогда количество $M_{КМ}$ объектов социальной части СТС, возвратившихся в исходное состояние, определяется по формуле:

$$M_{КМ} = \sum_{j=1}^{m} q_j n_j . \quad (11)$$

Показатель информационной устойчивости социальной части СТС определяется как отношение:

$$S = \frac{M_i - M_j}{N} = \frac{\sum_{i=1}^{k} p_i n_i - \sum_{j=1}^{m} q_j n_j}{N}, \quad (12)$$

где N – количество объектов социальной части СТС.

Для оценки информационной устойчивости предлагается шкала, представленная в табл. 3

Таблица 3

Шкала устойчивости

Значение S	Оценка
$0 \le S \le 0,4$	устойчива
$0,4 < S \le 0,6$	условно устойчива
$0,6 < S \le 1$	неустойчива

Описанный цикл операций представляет систематизированную совокупность моделей, инструментов, различных средств и организационных решений, которые, собственно, и формализуют предложенный метод (рис. 8). Это позволяет решить следующие задачи: выявить потенциальные угрозы и уязвимости, которые могут быть использованы для реализации ИПО; определить причинно-следственные связи триады – «угроза-уязвимость-последствия», оценить устойчивость СТС и принять решение по нейтрализации данных угроз.

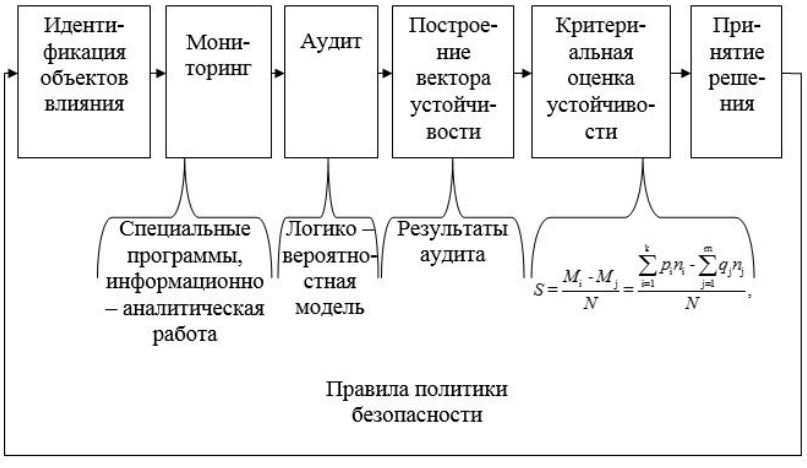

Рис. 8. Структурно-функциональная схема процесса оценки информационной устойчивости СТС

Принятие решения сопровождается процессом принятия и реализации управленческого решения, обеспечивающего для объекта защиты необходимый или достаточный уровень защищённости.

6. Обсуждение результатов исследования метода оценки информационной устойчивости социотехнической системы

Представленные логико-вероятностная модель оценки уровня защищённости СТС и вероятностный показатель оценки информационной устойчивости представляют практический интерес при решении задач оценки и обеспечения комплексной информационной безопасности, которая заключается как в защите собственных информационных ресурсов, так и защите от деструктивной информации. Трудоёмкость, сопровождающая разработку логико-вероятностной модели, компенсируется простым и понятным результатом, показывающем вероятности возникновения всех событий. Представленный метод в целом позволяет получить количественную оценку уровня защищённости и информационной устойчивости СТС в условиях информационной войны и тем самым обосновать защитные мероприятия по обеспечению комплексной информационной безопасности.

Перспективы дальнейших исследований заключаются в применении представленного метода для исследования максимально широкого класса объектов (человек – общество – государство), находящихся в условиях информационной войны.

7. Выводы

1. Результаты проведенных исследований показали, что эффективной технологией проведения ИПО является распространение информационных мемов с применением различных источников воздействия. Воздействие мема на социальную часть может вывести ее из устойчивого состояния и, как следствие, всю систему.

2. Предложенный метод оценки информационной устойчивости СТС, находящейся под воздействием ИПО, базируется на логико-вероятностной модели оценки степени нарушения информационной безопасности социума и показателе информационной устойчивости социальной части СТС. Показатель информационной устойчивости учитывает наличие в информационном пространстве так называемых деструктивных и компенсирующих мемов и вероятности подпадания под влияние мемов объектов социальной части СТС.

Метод представляет практический интерес, поскольку позволяет учитывать фактически слабоформализованный класс угроз – информационно-психологические операции, целью проведения которых является деструктивное влияние на социальную часть СТС.

Литература

1. Харченко, В. П. Кибертерроризм на авиационном транспорте [Текст]: зб. наук. пр. / В. П. Харченко, Ю. Б. Чеботаренко, О. Г. Корченко, Є. В. Паціра, С. О. Гнатюк // Проблеми інформатизації та управління. – 2009. – Вип. 4 (28). –С. 131–140.
2. Вильский, Г. Б. Информационные риски судовождения [Текст] / Г. Б. Вильский // Наук. Вістник ХДМА. – 2012. – № 1(4). – С. 17–26.
3. Дудикевич, В. Б. Проблеми оцінки ефективності систем захисту [Текст] / В. Б. Дудикевич, І. А. Прокопишин, В. Ф. Чекурін // Вісник Національного університету «Львівська політехніка». Сер.: Автоматика, вимірювання та керування. – 2012. – № 741. – С. 118–122.
4. Мірошник, М. А. Розробка методів оцінки ефективності захисту інформації в розподілених комп'ютерних системах [Текст] / М. А. Мірошник // Інформаційно-керуючі системи на залізничному транспорті. – 2015. – № 4 (113). – С. 39–43.
5. Лахно, В. А. Підвищення кібербезпеки транспорту в умовах деструктивного впливу на інформаційно-комунікційні системи [Текст] / В. А. Лахно, А. В. Грабарєв // Восточно-Европейский журнал передовых технологий – 2016. – Т. 1, № 3 (79). – С. 4–11. doi: 10.15587/1729-4061.2016.60711

6. Артёмов, А. А. Теоретические основы информационного управления [Текст] / А. А. Артёмов // Информационные войны. – 2015. – № 3. – С. 83–97.
7. Цыганов, В. В. Глобальное информационное противоборство [Текст] / В. В. Цыганов // Информационные войны. – 2015. – № 2. – С. 7–13.
8. Малков, С. Ю. Модель устойчивости/дестабилизации политических систем [Текст] / С. Ю. Малков, С. Э. Билюга // Информационные войны. – 2015. – № 1. – С. 7–18.
9. Lundberg, J. The resilience analysis matrix (RAM): visualizing functional dependencies in complex socio-technical systems [Text] / J. Lundberg, W. Rogier // 5th symposium on resilience engineering managing trade-offs, 2013.
10. Oosthuizen, R. An analysis methodology for impact of new technology in complex sociotechnical systems [Text] / R. Oosthuizen, L. Pretorius // 2013 International Conference on Adaptive Science and Technology, 2013. doi: 10.1109/icastech.2013.6707508
11. Simmons, M. P. Memes Online: Extracted, Subtracted, Injected, and Recollected [Text] / M. P. Simmons, L. A. Adamic, E. Adar // ICWSM. – 2011. – Vol. 11. – P. 17–21.
12. IBM Security Services 2014. Cyber Security Intelligence Index [Electronic resource]. – Available at: http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf
13. Андрєєва, О. М. Кіберзброя та аналіз її деструктивної діяльності на прикладі впливу вірусу нового покоління STUXNET на іранську ядерну програму [Текст] / О. М. Андрєєва, К. Мусієнко // Actual problems of international relations. – 2014. – Т. 1, № 103.
14. Остапенко, Г. А. Информационные операции и атаки в социотехнических системах [Текст] / Г. А. Остапенко – М.: Горячая линия – Телеком, 2007. – 134 с.
15. Дудатьєв, А. В. Моделі для організації протидії інформаційним атакам [Текст] / А. В. Дудатьєв // Захист інформації. – 2015. – № 2. – С. 157–162.
16. Чистяков, В. П. Курс теории вероятностей [Текст] / В. П. Чистяков – М.: Наука,1987. – 240 с.

Розглянуті способи передачі даних між програмними одиницями при виконанні інженерних розрахунків технологічного обладнання засобами Фортрану 90 і більш високого рівня. Наведено приклади, які зустрічаються в інженерній практиці машинобудівельних та споріднених їй спеціальностей. Можливість застосування різних способів передачі даних між програмними одиницями дає можливість виконувати ефективні обчислення в наукових і інженерних розрахунках

Ключові слова: втрата точності, програмна одиниця, передача даних, Фортран, інженер-механік, інженерні розрахунки

Рассмотрены способы передачи данных между программными единицами при выполнении инженерных расчетов технологического оборудования средствами Фортрана 90 и более высокого уровня. Приведены примеры, которые встречаются в инженерной практике машиностроительных и родственных ей специальностей. Возможность применения различных способов передачи данных между программными единицами дает возможность выполнять эффективные вычисления в научных и инженерных расчетах

Ключевые слова: потеря точности, программная единица, передача данных, Фортран, инженер-механик, инженерные расчеты

УДК 004.2.007.2
DOI: 10.15587/1729-4061.2015.65475

АНАЛИЗ ПРИМЕНЕНИЯ СПОСОБОВ ПЕРЕДАЧИ ДАННЫХ МЕЖДУ ПРОГРАММНЫМИ ЕДИНИЦАМИ В ИНЖЕНЕРНЫХ РАСЧЕТАХ

Д. Э. Сидоров
Кандидат технических наук, доцент*
E-mail: dsts1@ukr.net
И. А. Казак
Кандидат педагогических наук, доцент*
E-mail: AsistentIA@meta.ua
*Кафедра химического, полимерного и силикатного машиностроения
Национальный технический университет Украины «Киевский политехнический институт»
пр. Победы, 37, г. Киев, Украина, 03056

1. Введение

В современное время актуальным вопросом для инженеров-механиков является выполнение инженерных расчетов разнообразного технологического оборудования. Такая потребность постоянно существует для оценки эффективности работы оборудования на основе расчетов параметрических, кинематических, прочностных, характеристик производительности, нагрузок и т. п. Ресурсоемкие инже-