НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ *ISSN 1681-4886*

4 (83)' 2010

Виходить 6 разів на рік

Видається з 23 квітня 1996 р.

ІНФОРМАЦІЙНО -КЕРУЮЧІ СИСТЕМИ НА ЗАЛІЗНИЧНОМУ ТРАНСПОРТІ

INFORMACIJNO-KERUÛCI SISTEMI NA ZALIZNICNOMU TRANSPORTI

УДК 681. 326

КРИВУЛЯ Г. Ф., д.т.н., профессор,
КУЧЕРЕНКО Д. Е., аспирант (ХНУРЭ)

Информационная угроза для компьютерных систем управления как следствие ошибок пользователя

1. Введение

Внедрение компьютерных систем управления (КСУ) во все сферы человеческой деятельности, часто как необходимый компонент жизнеобеспечения, обуславливает высокие требования к качеству и надежности КСУ. Одной из важнейших функций компьютеров является хранение информации, которая представляет основную ценность в любой КСУ, а её обработка и передача – лишь следствие данного факта. В большинстве случаев потеря данных на компьютерных носителях при отказах аппаратно-программных средств КСУ представляет значительную информационную угрозу для управляемого объекта.

Главные причины потери данных представлены на рис. 1 [1].

Рисунок 1 – Причины потери данных

Изучение причин и видов ошибок пользователя при эксплуатации КСУ, а также их устранение, является важным источником обеспечения безотказной и надежной работы системы в целом. Последствия ошибок пользователя не менее значительны, чем последствия аппаратных или программных отказов. Во многих видах деятельности операторов цена ошибки чрезвычайно велика. Следствием ошибки оператора может быть авария, катастрофа, экологическое бедствие.

Под информационной угрозой будем понимать возможность возникновения на каком-либо этапе жизнедеятельности КСУ такого явления, процесса или события, следствием которого могут быть нежелательные воздействия на информацию.

Различают два основных типа информационных угроз:

- естественные угрозы, вызванные воздействиями на КСУ объективных физических процессов или стихийных природных явлений, не зависящих от человека;
- искусственные угрозы, вызванные деятельностью человека.

Среди искусственных информационных угроз, исходя из мотивации действий, можно выделить непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании КСУ и ее компонентов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п. Эти ошибки являются самыми частыми и самыми опасными с точки зрения размера ущерба. Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок.

2. Классификация основных непреднамеренных угроз

Основные непреднамеренные искусственные угрозы КСУ – это действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из

любопытства, но без злого умысла:

1. Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

2. Неправомерное отключение оборудования или изменение режимов работы устройств и программ;

3. Неумышленная порча носителей информации;

4.Запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

5.Нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

6. Заражение компьютера вирусами;

7. Неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;

8. Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

9. Проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

10. Игнорирование организационных ограничений (установленных правил) при работе в системе;

11. Вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);

12. Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;

13. Пересылка данных по ошибочному адресу абонента (устройства);

14. Ввод ошибочных данных;

15. Неумышленное повреждение каналов связи.

3. Постановка задачи

Одной из важнейших задач обеспечения безопасности КСУ является определение, анализ и классификация возможных информационных угроз безопасности. Перечень значимых угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа рисков и формулирования требований к системе информационной защиты КСУ. Целью данной работы является оценка информационной угрозы и рассмотрение ее зависимости от следующих составляющих: технического состояния компьютерной системы, компетентости пользователя КСУ и сложности решаемой задачи.

4. Моделирование технических состояний КСУ

Для диагностики сложных технических объектов ключевое значение имеют не только точные, математически обоснованные данные, но и модели, содержащие качественную информацию, которая включает многолетний опыт эксплуатации и важные сведения о данной области знаний. Для моделирования рассуждений эксперта наиболее адекватным математическим аппаратом является язык нечётких множеств, который позволяет максимально сократить переход от вербального словесного качественного описания объекта, которое характеризует человеческое мышление, к численным количественным оценкам его состояния и сформулировать на этой основе простые и эффективные алгоритмы..

Для оценки состояния КСУ вводим лингвистическую переменную “Дефект” и термы данной переменной: {“нет”, “легкий”, “умеренный”, “сильный”, “разрушительный”}. Каждое терм (значение) лингвистической переменной характеризуется нечетким множеством [2].

Различные виды отказов КСУ характеризуются классификационными признаками, которые будем рассматривать как нечеткие диагностические признаки. Каждый рассматриваемый признак – это нечеткое множество, определено лингвистически. Рассмотрим следующие диагностические признаки, которые описывают состояние дефекта: область возникновения отказов = {“значительная”, “средняя”, “незначительная”}, характер изменения параметров во время отказа = {“значительный (внезапный)”, “средний”, “незначительный (постепенный)”}, характер существования отказа во времени = {“значительный (длительный)”, “средней длительности”, “незначительный (кратковременный)”}, возможность обнаружения = {“сложная”, “средняя”, “несложная”}, обусловленность другими отказами = {“значительная”, “средняя”, “незначительная”}, возможность восстановления работоспособности после отказа = {“сложная”, “средняя”, “несложная”}, причина возникновения = {“сложная”, “средняя”, “несложная”}, тяжесть последствий = {“значительная”, “средняя”, “незначительная”}.

5. Моделирование уровня компетентности пользователя КСУ

При исследовании ошибок пользователей КСУ выделяют ряд причин, среди которых основное значение

имеют личные факторы. С точки зрения способности пользователя решать задачу в определенной области рассмотрим такой фактор, как компетентность пользователя. Основные методы, используемые для анализа компетентности, могут включать в себя следующие: интервьюирование, анкетирование пользователя; наблюдения; обсуждения в группах; экспертные методы. Последние представляют наибольший интерес, так как основаны на суждениях высококвалифицированных специалистов, представленных в виде качественной оценки объекта.

Описать уровень компетентности пользователя КСУ количественно можно с использованием аппарата нечеткой логики. При этом можно ввести нечеткие понятия, которые качественно соответствуют различным уровням компетентности. Пусть U – универсальное множество всех критериев a_i, по которым оценивается компетентность пользователя $U = \{a_i, i = \overline{0,N}\}$. Пусть В – нечеткое множество, определяющее степень компетентности пользователя $B =< U, \mu >= \{a_1 \mid \mu_1 + a_2 \mid \mu_2 + ... + a_N \mid \mu_N\}$. В качестве формы функции принадлежности μ_i выберем гауссову кривую, которая описывается формулой $\mu(a_i) = e^{-\frac{(a_i - n)^2}{\sigma}}$, где n – центр нечеткого множества, σ – крутизна функции. Функция принадлежности μ_i показывает, в какой мере пользователь обладает компетентностью a_i. Относительно нечеткого множества B вводим лингвистическую переменную “Компетентность” ={"нулевая", "низкая", "средняя", "выше среднего", "высокая"}.

6. Оценка сложности задачи, решаемой пользователем КСУ

В деятельности любого пользователя компьютерной системы встречаются задачи различной сложности. Сложные задачи поручаются только наиболее опытным специалистам или тем, кто прошел соответствующие испытания. Сложность задачи определяется тем, насколько быстро и легко удается специалисту освоить критические операции, необходимые для ее выполнения, причем сложность задачи тем выше, чем больше одиночных, уникальных подзадач содержится в ней.

Временная сложность алгоритма – это функция размера входных и выходных данных, равная максимальному количеству элементарных операций, выполняемых алгоритмом для решения экземпляра задачи указанного размера. Во многих задачах размер выхода не превосходит или пропорционален размеру входа – в этом случае можно рассматривать временную сложность как функцию размера только входных данных. По аналогии с временной сложностью определяют пространственную сложность алгоритма, только здесь говорят не о количестве элементарных операций, а о количестве затраченной памяти.

В связи с бурным развитием компьютерной техники и уменьшением её стоимости проблема аппаратных затрат стоит уже не так остро. Главный акцент при анализе сложности задачи делается на время её выполнения.

Для оценки сложности задачи воспользуемся следующей шкалой сложности задачи (табл. 1).

Таблица 1 – Шкала сложности задачи

Уровень сложности	Описание
«Высокий»	Разработка новых или оптимизация существующих процедур/процессов/технологий
«Выше среднего»	Реализация задачи требует выполнения различных функций и использования знаний из разных предметных областей
«Средний»	Выполнение задачи базируется на анализе новых данных, использовании различных источников информации
«Ниже среднего»	При выполнении задачи используются поверхностные заключения и заранее разработанные процедуры
«Низкий»	Выполнение стандартных задач, не требующих обдумывания

Учитывая то, что понятие сложность задачи (complexity) описывается естественным языком, воспользуемся аппаратом нечеткой логики. Получим следующую функцию принадлежности для описания лингвистической переменной «Complexity» (рис. 2), каждый терм которой отвечает типу задачи от самого сложного уровня до легкого уровня.

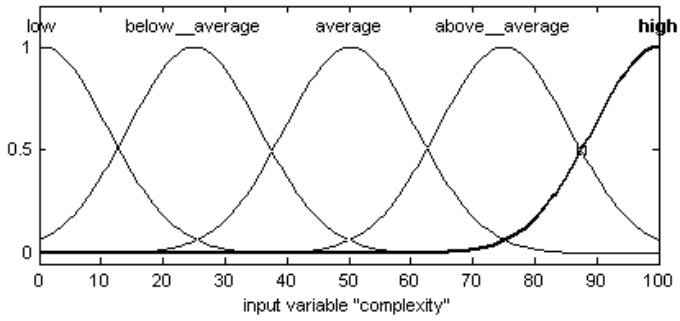

Рисунок 2 – Функция принадлежности переменной «Complexity»

7. Оценка информационной угрозы КСУ

Информационная угроза (ИУ) представляет собой опасное для объекта событие в информационной сфере, при реализации (свершении) которого наносится ущерб (У) для информационной сферы управляемого объекта. Вероятность события может быть одной из оценочных характеристик ИУ, но, как показывает практика, рассчитать её аналитически или корректно определить статистически - почти невыполнимая задача. Поэтому чаще всего её определяют экспертным путём как коэффициент псевдовероятности. Важно определить взаимосвязь ИУ с различными информационными рисками, т.е. возникает необходимость принятия решений в условиях вероятностной неопределенности.

Оценку ИУ также определим в терминах нечеткой логики. Поскольку ущерб, наносимый КСУ, может иметь различный характер, вводим лингвистическую переменную «Величина ущерба» с термами - {"нулевой", "низкий", "ограниченный", "выше среднего", "значительный"}.

Используя понятия «компетентность пользователя», «состояния компьютерной системы» и «сложность задачи», можно оценить величину ИУ с использованием продукционных правил для экспертной системы.

Для составления правил имеется три входные переменные: уровень компетентности пользователя, величина дефекта КСУ, сложность решаемой задачи и одна выходная переменная – величина ущерба за счет возникшей ИУ. Ниже приведен пример продукционных правил:

1. if (компетентность – нулевая) and (дефект – нет) and (уровень сложности задачи высокий) then (ущерб – "значительный);
2. if (компетентность – нулевая) and (дефект – разрушительный) and (уровень сложности задачи – высокий) then (ущерб – "значительный);
3. if (компетентность – низкая) and (дефект – разрушительный) and (уровень сложности задачи – средний) then (ущерб – значительный);
4. if (компетентность – выше среднего) and (дефект – разрушительный) and (уровень сложности задачи – средний) then (ущерб – ограниченный);
5. if (компетентность – высокая) and (дефект – разрушительный) and (уровень сложности задачи – низкий) then (ущерб – низкий).

8. Выводы

Изучение причин и видов ошибок пользователя при эксплуатации компьютерной системы является важным источником для моделирования его деятельности. Моделирование *методами* нечеткой логики компетентности пользователя, состояний КСУ и уровня сложности решаемых задач позволило сформулировать продукционные правила для определения величины ущерба при нарушении информации в КСУ.

Литература

1. *David Smith,* The Cost of Lost Data // Storage Management Solutions. – 1999. – No. 4. –Pp. 60-64.
2. *Кривуля Г.Ф., Кучеренко Д.Е., Механа Сами.* Классификационные признаки для диагностики компьютерных неисправностей с использованием нечетких экспертных систем // Радіоелектронні і комп'ютерні системи. – 2009. – № 5 (39). – С. 127-133.
3. *Кривуля Г.Ф., Кучеренко Д.Е.* Интеллектуальные средства диагностирования состояний компьютерных систем управления // «Інфомаційно-керуючі системи на залізничному транспорті». –2009. – №4. – С. 23-28.
4. *Кривуля Г.Ф., Дудар З.В., Кучеренко Д.Е., Лаптев М.А.* Диагностика компьютерных неисправностей с использованием нечетких экспертных систем / Материалы конференции «Интеллектуальные системы принятия решений и проблемы вычислительного интеллекта» (ISDMCI'2009) . Евпатория, 2009.

Резюме

Методами нечеткой логики в виде продукционных правил рассмотрена зависимость информационного ущерба от сложности решаемых задач, компетентности пользователя и технического состояния компьютерной системы

Методами нечіткої логіки у вигляді продукційних правил розглянута залежність інформаційного збитку від складності вирішуваних завдань, компетентності користувачів та технічного стану комп'ютерної системи

The dependence of informational loss on the complexity of solved tasks, users competence and technical state of the computer system was considered by methods of fuzzy logic in the form of productional rules

Ключові слова: компьютерная система управления, ошибки пользователя, информационная угроза, определение величины ущерба

Поступила 18.06.2010 г.