УДК 004.042+004.274

Грызунов Виталий Владимирович
Канд. техн. наук, доцент
кафедры информационных технологий и
систем безопасности,
Российский государственный
гидрометеорологический университет,
e-mail: viv1313r@mail.ru

Украинцева Дарья Андреевна
Студент,
кафедра информационных систем
и систем безопасности,
Российский государственный
гидрометеорологический университет,
e-mail: ukrainceva2000@yandex.ru

АДАПТИВНОЕ УПРАВЛЕНИЕ АНАЛИЗОМ СОСТОЯНИЙ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ В ХОДЕ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ

Аннотация. Цель исследования – выбрать подходящий алгоритм анализа состояний информационно-вычислительной системы, деградирующей в ходе информационно-технических воздействий. Задача решалась посредством покомпонентного лексиографического построения результирующего отношения предпочтения. В результате предложен инструментарий выбора подходящего алгоритма анализа состояний. Приведены примеры применения предложенного инструментария.

Ключевые слова. информационно-технические воздействия, управления информационно-вычислительной системой, анализ состояний информационно-вычислительной системы.

Vitalii V. Gryzunov
candidate of technical Sciences,
Associate Professor of information technologies
and security systems, ,
Russian State Hydrometeorological University,
e-mail: viv1313r@mail.ru

Daria A. Ukrainceva
Student, Department of information systems and security systems,
Russian State Hydrometeorological University,
e-mail: ukrainceva2000@yandex.ru

ADAPTIVE CONTROL OF INFORMATION-COMPUTING SYSTEM STATE ANALYSIS DURING INFORMATION TECHNOLOGY IMPACTS

Annotation. The purpose of the study is to choose a suitable algorithm for analyzing the states of an information-computing system that degrades during information-technical impacts. The problem was solved by an exploded lexicographic construction of the resulting preference relationship. As a result, a toolkit for choosing a suitable algorithm of analyzing the states is proposed. Examples of the application of the proposed tools are given.

Keywords. information-technical impacts, control of information-computing system, analysis of the states of information-computing system.

Современное общество сильно зависит от защищённости информационно-вычислительных систем (ИВС) [1]. Сюда можно отнести ИВС критически важных объектов: атомные станции, газопроводы, системы управления движением; ИВС имеющие дело с чувствительной информацией: биржи, банки, медицинские учреждения, и другие ИВС, обрабатывающие, хранящие и передающие важную информацию. Нарушение любого аспекта информационной безопасности: целостности, конфиденциальности, доступности может привести к существенному ущербу, а значит, является сильным инструментом влияния на правительства и бизнес. Этим активно пользуются злоумышленники различного толка: от мающихся без дела ламеров (агрессивно настроенных чайников, считающих себя хакерами), до профессиональных киберпреступников, террористов и спецслужб. Как следствие, ИВС подвергается широкому диапазону информационно-технических воздействий: от простого IP-шторма через botnet до изощрённых pretexting.

На среднем предприятии, ИВС которого насчитывает 250-300 компьютеров, происходит несколько тысяч инцидентов, связанных с информационной безопасностью.

Противостоять такому объёму и скорости случайного и целенаправленного агрессивного воздействия статичными настройками средств информационной безопасности не представляется возможным. Необходим интеллект. Человеческий или искусственный. Адаптация является частью искусственного интеллекта [2].

Под **информационно-техническими воздействиями** (ИТВ) будем понимать воздействия на процесс генерации, обработки, хранения и передачи данных в ИВС, вызывающие сокращение доступного ресурса ИВС, то есть деградацию ИВС. Это определение включает воздействия, обусловленные естественными причинами и действиями злоумышленников.

Ресурсами ИВС являются: C, L, Sp, Tr – множества вычислителей, каналов связи, памяти, устройств ввода/вывода. Ресурсы оцениваются через производительности вычислителей, каналов связи, устройств ввода-вывода, накопителей: $\Omega = \Omega_C(t), \Omega_L(t), \Omega_{Tr}(t), \Omega_{Sp}(t)$, где Ω - комплексная производительность ИВС.

На доступных ресурсах ИВС решает множество задач K. Чтобы решение задач стало возможно, в ИВС необходимы все типы ресурсов.

Аксиома необходимости:

$$\Omega > 0 \Leftarrow \big((C \neq \emptyset) \wedge (L \neq \emptyset) \wedge (Tr \neq \emptyset) \wedge (Sp \neq \emptyset)\big) = 1.$$

Следовательно, для полного прекращение работы ИВС достаточно полностью вывести из строя любой из типов ресурса:

$$\Omega = 0 \Rightarrow \big((C = \emptyset) \vee (L = \emptyset) \vee (Tr = \emptyset) \vee (Sp = \emptyset)\big) = 1.$$

ИТВ вызывает сокращение одного или нескольких типов ресурса, то есть формирует $\Delta C, \Delta L, \Delta Tr, \Delta Sp$, что влечёт за собой сокращение количества решаемых задач ΔK за заданное время t.

Подробная модель ИВС, деградирующей в условиях информационно-технических воздействий, приведена в [4].

Назовём вектор, описывающий доступные производительности ИВС и распределённые по ним задачи, **состоянием ИВС**:

$$\langle \Omega_C(t), \Omega_L(t), \Omega_{Tr}(t), \Omega_{Sp}(t), K(t) \rangle.$$

Цель системы управления ИВС – организовать работу оставшихся ресурсов таким образом, чтобы решить все поставленные задачи точно и в срок, то есть $\Delta K \to 0$. В некоторых случаях допустимо решать задачи в приемлемые сроки с удовлетворительным качеством [6].

Система управления ИВС управляет структурой ИВС и алгоритмами распределения ресурсов.

Качество управления зависит от достоверности получаемых данных о текущем состоянии ИВС.

Предположим, управление реализовано посредством линейного оператора $F(x)$, где x – текущее состояние ИВС. Неточность в исходных данных даёт Δx, а значит, по определению линейного оператора:

$$F(x + \Delta x) = F(x) + F(\Delta x),$$

вызывает погрешность в управляющем воздействии $F(\Delta x)$.

В управлении, реализованном нелинейными операторами, как правило, погрешность управления, вызванная неточностью исходных данных, возрастает нелинейно.

Данные о текущем состоянии собираются в особые моменты времени – **контрольные точки ИВС**.

Достоверность данных о текущем состоянии ИВС зависит от объёма собираемых данных, алгоритмов анализа собранных данных, а также частоты сбора данных (количества контрольных точек в единицу времени). Объём собираемых данных должен быть достаточным, чтобы обеспечить наблюдаемость системы по Калману [5].

У ИВС, функционирующей в ходе ИТВ, есть особенность: чем интенсивнее ИТВ, тем больше деградирует ИВС между точками контроля, а значит, выше вероятность получить неадекватную модель ИВС. Что, в свою очередь, снижает качество управленческого решения по распределению целевых задач ИВС по ресурсам и влечёт за собой снижение вероятности решения целевых задач в ИВС за заданное время с требуемым качеством.

Одним из путей уменьшить неопределённость состояния ИВС и создать адекватную модель деградирующей ИВС является увеличение частоты получения контрольных точек и применение продвинутых алгоритмов анализа состояний ИВС. Поскольку процессы получения контрольных точек и анализа состояний сами по себе потребляют ресурсы ИВС, то в этом случае растёт нагрузка на оставшиеся ресурсы ИВС, и тем меньше ресурсов остаётся для выполнения целевых задач, а значит, ниже вероятность выполнения задач ИВС.

Некоторые продвинутые адаптивные алгоритмы с передаточной функцией, заданной аналитически, приведены в работе [3]. Здесь, как правило, чем сложнее и точнее алгоритм адаптации, тем больше ресурсов ИВС он потребляет, что обостряет противоречие.

Задача выбора алгоритма анализа состояний и частоты получения контрольных точек может формулироваться следующим образом:

1) выбрать такую частоту получения контрольных точек и алгоритм анализа состояний ИВС, которые обеспечат допустимую адекватность модели ИВС и потратят допустимое количество ресурсов ИВС: выбор из равнозначных альтернатив;

2) выбрать такую частоту получения контрольных точек и алгоритм анализа состояний ИВС, которые обеспечат максимальную адекватность модели ИВС и потратят допустимое количество ресурсов ИВС: максимизация одного показателя при сохранении в допуске других;

3) выбрать такую частоту получения контрольных точек и алгоритм анализа состояний ИВС, которые обеспечат допустимую адекватность модели ИВС и потратят минимальное количество ресурсов ИВС: минимизация одного показателя при сохранении в допуске других.

Для решения поставленной задачи применим покомпонентное лексикографическое построение результирующего отношения предпочтения.

Такой подход подразумевает создание системы координат, где количество осей равно количеству оптимизируемых показателей. Если показателей N, то размерность системы $N \times N$.

Решение задачи в формулировке №1 (см. выше), когда реализуется выбор из равнозначных альтернатив, лежит не выше поверхности, размерностью $(N-1) \times (N-1)$, расположенной перпендикулярно биссектрисе, выходящей из начала координат. Все ограничения, накладываемые на показатели, должны быть не ниже этой поверхности.

Задача в формулировке №2 и 3 (см. выше). Оптимизируется один из показателей, а от остальных требуется удовлетворять предъявляемым требованиям. Решение ищется относительно поверхности размерностью $(N-1) \times (N-1)$, расположенной параллельно оси оптимизируемого показателя. Все ограничения, накладываемые на остальные показатели, должны быть не ниже этой поверхности.

Пример.

Сопоставим каждому рассматриваемому i-ому алгоритму анализа состояний ИВС вектор, описывающий ресурсоёмкость алгоритма

$$\langle \Omega_C, \Omega_L, \Omega_{Tr}, \Omega_{Sp} \rangle_i.$$

Нанесём в системе координат точки, соответствующие каждому алгоритму (рисунок 1). На рисунке для наглядности без нарушения общности сделано упрощение, – ресурсоёмкость алгоритма описывается скаляром.

Из рисунка 1 видно, что алгоритм 3 даёт наибольшую вероятность получить достоверные сведения и потребляет среднее количество ресурсов самой ИВС. Больше всего ресурсов потребляет алгоритм 4, при этом даёт самую маленькую вероятность.

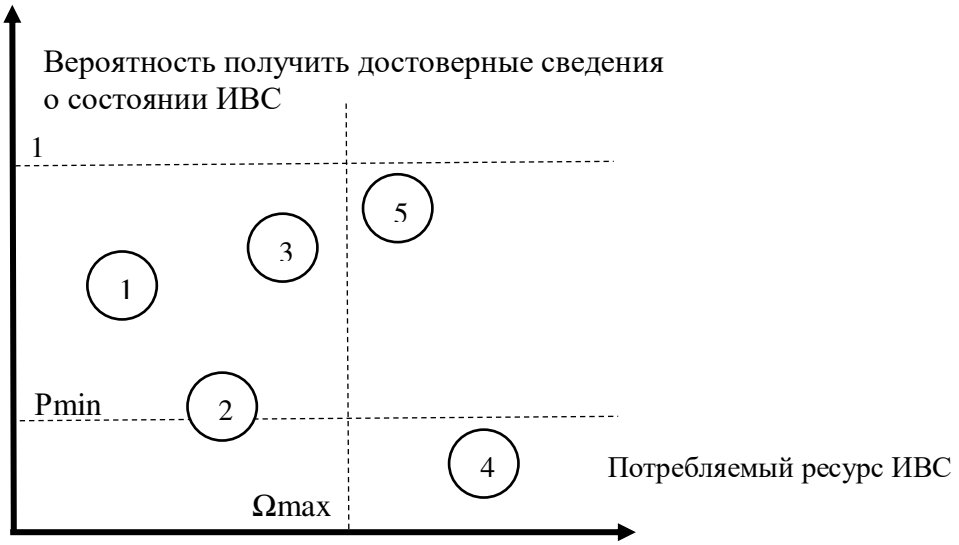

Рис. 1. Множество альтернатив для выбора алгоритма анализа контрольных точек ИВС*

*Составлено автором

Ситуация 1. Радиоконтроль орбиты космического аппарата в ходе ведения радиоэлектронной борьбы.

Интенсивность ИТВ высока, значит, ИВС деградирует быстро.

Особенность радиокотроля такова, что можно пренебречь отдельными измерениями, главное проводить их на всём заданном интервале времени. Следовательно, на первый план выходит необходимость сохранить ресурс ИВС для целевых задач на весь заданный интервал времени. В этом случае предпочтение отдаётся алгоритмам, которые дают вероятность не меньше P_{min} и потребляют минимум ресурса ИВС. На рисунке 1 это алгоритм 1. Поверхность, размерности 1 параллельна оси оптимизируемого показателя – потребляемый ресурс ИВС и проходит через P_{min}.

Ситуация 2. Проведение банковских транзакций во время вирусного заражения ИВС.

Интенсивность ИТВ средняя, значит, ИВС деградирует со средней скоростью.

Особенность транзакций состоит в том, что нужно обеспечить максимальную вероятность выполнения целевой задачи, временем можно пожертвовать. В этом случае предпочтение отдаётся алгоритмам, которые дают максимальную вероятность и потребляют ресурс ИВС, не больше чем Ω_{max}. На рисунке 1 это алгоритм 3. Поверхность, размерности 1 параллельна оси оптимизируемого показателя – вероятность получить достоверные сведения о состоянии ИВС и проходит через Ω_{max}.

Предложенный инструментарий может применяться как в реальном режиме времени, так и в отложенном. В отложенном режиме заранее анализируются все возможные варианты и заносятся в таблицу соответствия. В дальнейшем система управления ИВС выбирает варианты непосредственно из таблицы, что является самым быстрым и экономным способом работы с альтернативами.

Таким образом, анализ текущего состояния ИВС в ходе ИТВ необходим для реализации качественного управления ИВС. Подходящий алгоритм может быть выбран путём покомпонентного лексикографического построения результирующего отношения предпочтения.

Список использованной литературы

1. В.Андрианов, С.Зефиров, В.Голованов, Н.Голдуев Обеспечение информационной безопасности бизнеса [Электронный ресурс]: учебник / Андрианова В.В. - 2-е изд. – М. : ООО «Альпина», 2010. – 265 с. – URL: https://pqm-online.com/assets/files/lib/books/andrianov.pdf (дата обращения 2.09.2019).

2. Andreas Kaplan, Michael Haenlein Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence [electronic resource]: article / Andreas Kaplan, Michael Haenlein// BusinessHorizons.2018. URL: https://www.researchgate.net/publication/328761767_Siri_Siri_in_my_hand_Who's_the_fairest_in_the_land_On_the_-interpretations_illustrations_and_implications_of_artificial_intelligence (дата обращения 2.09.2019).

3. Цикунов А.М. Адаптивное и робастное управление динамическими объектами по выходу. – М.: ФМЗМАТЛИТ, 2009.- 268с.

4. Грызунов В.В. Модель информационно-вычислительной системы, деградирующей в условиях информационно-технических воздействий // Военно-космическая академия им. А.Ф.Можайского : труды. Вып. 646.Март/ под общ. ред. Ю.В. Кулешова.– СПб.: ВКА им. А.Ф. Можайского, 2015.– С.93-102.

5. Калинин В. Н. Теоретические основы системных исследований: краткий авторский курс лекция для адъюнктов академии. – СПб.: ВКА им. А.Ф. Можайского, 2011. – 278 с.

6. Грызунов В.В. Методика решения измерительных и вычислительных задач в условиях деградации информационно-вычислительной системы // Вестник СибГУТИ. – 2015. – № 1. – С.35-44.