УДК 004.942

АНАЛИЗ УСТОЙЧИВОСТИ ДИНАМИЧЕСКОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ ТЕОРЕТИКО-МНОЖЕСТВЕННОЙ МОДЕЛИ

Мирошина И.Е., Сумин В.И., Чулюков В.А.

ФГБОУ ВПО «Воронежский государственный педагогический университет», Воронеж, e-mail: chul_130451@mail.ru

Рассматривается анализ возможностей теоретико-множественной модели системы безопасности информации в вычислительных сетях для исследования устойчивости системы к внешним воздействиям. Задача вызвана необходимостью формализации процесса динамической безопасности информации в условиях непрерывного эволюционирования динамики средств защиты и средств воздействия на них для разнородных вычислительных сетей. Для формализации предлагается использовать критерий устойчивости взаимовлияющих процессов. Приведены теоретико-множественная модель системы безопасности, интегральное уравнение движения системы. Даны три определения устойчивости динамической системы безопасности: устойчивости по Ляпунову, асимптотической устойчивости и устойчивости по Лагранжу. Определения интерпретированы с точки зрения их использования для анализа устойчивости динамической системы безопасности к внешним воздействиями, сформулированы условия их применимости.

Ключевые слова: модель, безопасность информации, вычислительные сети

THE STABILITY ANALYSIS OF DYNAMIC SYSTEM SECURITY INFORMATION BASED ON THE SET-THEORETIC MODEL

Miroshina I.E., Sumin V.I., Chulyukov V.A.

Voronezh State Pedagogical University, Voronezh, e-mail: chul_130451@mail.ru

Discusses the analysis of capabilities of the set-theoretic model of information security in computer networks to study the stability of the system to external influences. The problem is caused by need of formalization of process of dynamic safety of information in the conditions of a continuous evolution of dynamics of means of protection and means of influence on them for heterogeneous computer networks. For formalization it is offered to use criterion of stability of the processes mutually influencing. Shows the set-theoretic model for security and the integral equation of motion of a system. Given three definitions of sustainability dynamic safety systems: stability of the Lyapunov, asymptotic stability and stability of the Lagrangian. Definitions are interpreted from the point of view of their use for the analysis of stability of dynamic systems security to external influences, formulated the conditions for their applicability.

Keywords: model, information security, computer network

Динамическую систему безопасности информации в вычислительных сетях можно представить в виде взаимовлияющих множеств: комплексов средств защиты информации (СЗИ), средств воздействия, угроз, неправомерных действий (СНД) и отношений взаимовлияния отдельных компонентов комплексов средств защиты информации и средств воздействия [5].

Будем считать, что воздействия СНД являются внешними по отношению к СЗИ, то есть будем учитывать влияние процессов системы угроз на процессы, происходящие как с СЗИ в целом, так и с их компонентами в отдельности, так и с самой защищаемой информацией. Кроме того, эти внешние воздействия могут быть постоянными или изменяться во времени.

Как отмечалось в [2], любая динамическая система (а значит, и динамическая система обеспечения безопасности информации в вычислительных сетях) может находиться в разомкнутом или замкнутом состоянии (рис. 1). Динамической системой в замкнутом состоянии является система, функционирующая с обратной связью. Динамической системой в разомкнутом состоянии – система с разорванной обратной связью. На рисунке показана точка разрыва.

На рис. 1:

– управляющие воздействия на динамическую систему с защищаемой информацией носят внешний характер и обозначаются как *Y*;

– возмущающие воздействия на процессы выражаются в изменении условий функционирования комплекса систем защиты информации (КСЗИ) и обозначены *y(t)* с индексом, соответствующим каждому процессу;

– $\hat{C}$, $\hat{G}$ и $\hat{H}$ – операторы отношений между процессами, а под «возмущающим воздействием» понимается независимость параметров воздействия (угрозы) от параметров СЗИ (системы управления).

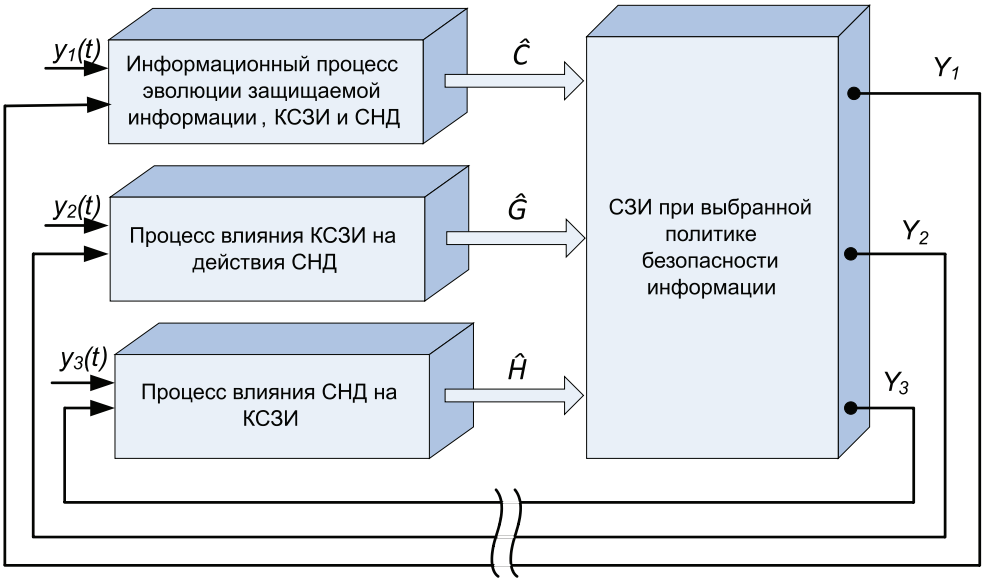

Рис. 1. Структурная схема динамической системы в замкнутом и разомкнутом состоянии

Воздействия внешних угроз на компоненты защиты или в целом на средства защиты требуют их постоянной подстройки. Если внешние угрозы не оказывают никакого воздействия на СЗИ (или их компоненты), то поведение системы защиты информации при выбранной политике безопасности (ПБ) оценивается ее устойчивостью. Устойчивость в этом случае определяется как способность поддерживать заданный режим работы по выполнению целевой функции с определенной точностью длительное (в идеале бесконечное) время вне зависимости от изменения внешних воздействий со стороны СНД. У такой СЗИ эволюция средств защиты идет впереди эволюции средств угроз, а схема динамической системы такого вида (рис. 1) подобна схеме разомкнутой системы автоматического регулирования.

Для случая, когда эволюция СЗИ отстает от эволюции угроз, схема динамической системы подобна схеме замкнутой системы автоматического регулирования (точка разрыва обратной связи на рис. 1 отсутствует). Поведение всей системы защиты информации под воздействием СНД на параметры как отдельных СЗИ, так и комплекса защиты в целом (для выбранной ПБ) также будем оценивать устойчивостью. Однако устойчивость системы в разомкнутом состоянии еще не достаточна для устойчивости замкнутого контура. Устойчивость в этом случае необходимо определять как свойство системы по поддержанию отклонений выходных параметров СЗИ относительно эталонных значений в пределах заданных малых величин. При этом именно замкнутость системы определяет особенности решения задач устойчивости эволюции процессов, происходящих в вычислительных сетях со средствами защиты, а выбранный метод оценки устойчивости дает возможность оценить такие динамические параметры эффективности СЗИ, как запас устойчивости, степень устойчивости, отклонения параметров динамической системы. Рассмотрим подробнее эти показатели.

Запас устойчивости позволяет системе СЗИ устойчиво функционировать при отклонении любого параметра этой системы в определенных пределах, то есть определяет степень удаленности параметров функционирования системы СЗИ от границы устойчивости.

Степень устойчивости характеризуется видом и скоростью возвращения переходного процесса к равновесному режиму работы системы после парирования возмущений. Причем чем значительнее степень устойчивости, тем быстрее происходит ликвидация негативных воздействий от угроз.

Параметры показателей системы при внешних угрозах определяются в соответствии с техническим заданием, в котором указываются тип решаемой задачи, формализация задачи, определяются критерии (надежность, своевременность, полнота, конфиденциальность и достоверность) для оценки показателей и т.д.

Целью исследования является анализ возможностей теоретико-множественной модели системы безопасности информации в вычислительных сетях для исследования устойчивости системы к внешним воздействиям.

Структурный элемент СЗИ при выбранной политике безопасности можно представить в таком виде, как на рис. 2. В такте n воздействие $I_k(n)$ поступает на вход k-го блока, действие которого описывается функцией R. На этом этапе внешнее описание системы, характеризуемое состоянием

$$X_k(n) = X_k(n-1+\tau_{\tau\to 0}) = R((n-1), X(n-1), I(n-1)),$$

где запись $n-1+\tau_{\tau\to 0}$ означает момент времени непосредственно после окончания n–1-го такта. Выход $O_k(n)$ функции R получается за счет входных воздействий на нее $I(n)$ и $X(n)$. В результате n-го такта значение функции состояния изменяется на $X(n+\tau_{\tau\to 0}) = R(X(n), I(n))$ и поступает на вход этого блока в такте $n+1$ в качестве X($n+1$). Далее рассмотренный цикл повторяется на такте $n+1$ и так далее для всех $n=\overline{1,N}$ на всем временном интервале функционирования.

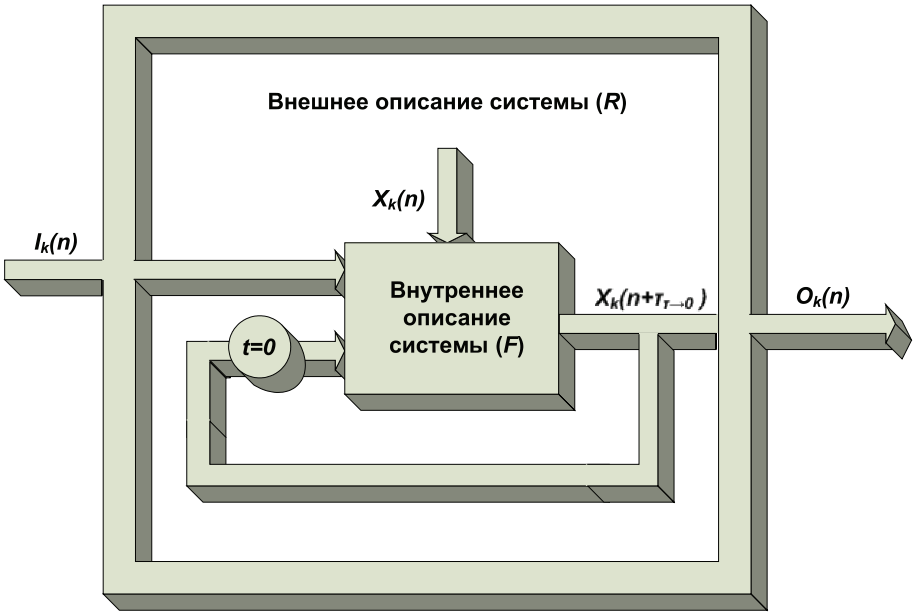

Рис. 2. Структурный элемент СЗИ при выбранной политике безопасности

Разработаем структурную модель функционирования СЗИ при выбранной ПБ. Для этого будем рассматривать множество подсистем системы $S = \{S_1, S_2, ..., S_N\}$, среди которых могут быть такие подсистемы, как конкретное средство защиты, его программное обеспечение, используемый метод защиты, защищаемая информация, отдельное внешнее воздействие при выполнении программно-технических операций и т.д. В этом множестве для каждой пары подсистем S_i определим квадратную матрицу связей M^{ij} размерностью $L\times L$, $L = \max(n_i, m_j)$ где n_i, – размерность вектора O_i и m_j – размерность вектора I_j. Элемент матрицы связей M^{ij} принимает значение 1, если соответствующая составляющая (координата) вектора O_i становится составляющей (координатой) вектора I_j, в противном случае элемент матрицы равен 0. Таким образом, предполагается существование и матриц вида M^{ii}, т.е. возможность обратной связи на элементе S_i. Если же связь между S_i и S_i отсутствует, то $M^{ii} = 0$. В случае, когда часть выходов подсистемы S_i передается на входы подсистемы S_j, справедливо равенство:

$$I_j = M^{ij} O_i. \quad (1)$$

Следовательно, можно построить матрицу M размерностью $N\times N$ с элементами, в виде матриц связей:

$$M^{ij}/M^S = (M^{ij})_{NN}.$$

При взаимодействии S_i и S_j, $i, j = \overline{1,N}$ для каждой подсистемы S_j существует глобальная реакция R_i, представляющая определенное действие:

$$R_j : (X_i \times I_i) \to O_i,\ R_j(x_i, in_i) = ou_i, \quad (2)$$

где $x_i \in X_i$, $in_i \in I_i$, $ou_i \in O_i$, $i = \overline{1,N}$.

Преобразуя равенство (1) с учетом (2), получим

$$ou_j^i = M^{ij} R_j \left(x_i, in_i\right). \quad (3)$$

Если обозначить $M^{ij}R_i$ через Φ_{ij}, то выражение (1) примет вид

$$in_{ij} = \Phi_{ij}\left(x_i, in_i\right),\ i,j = \overline{1,N}\ . \quad (4)$$

Представим сложный вектор новых значений входов по всем S_i, полученный в результате воздействия сложного вектора первоначальных значений $in_i = (in_1, ..., in_N)$ как $in' = \left(in'_1, \ldots, in'_N\right)$. Тогда действие системы можно формализовать как

$$in' = \Phi\left(x, in\right) \quad (5)$$

Основываясь на (5), можно отслеживать изменения входов подсистемы S_i для всех $in \in I$ при $i = \overline{1,N}$.

Распишем (5) с учетом временных изменений. Для этого будем считать, что вход и выход СЗИ при выбранной ПБ можно представить в виде сложных векторов, которые в каждый момент времени $t > t_0$, $t \in [t_0, t_k]$ принимают значения $I(t) = (I_1(t), ..., I_N(t))$ и $O(t) = (O_1(t), ..., O_N(t))$ соответственно. Следовательно, I, O и X означают множества

$$I = \left\{ t, I(t)\Big|_{t\in[t_0,t_k]} \right\},\ O = \left\{ t, O(t)\Big|_{t\in[t_0,t_k]} \right\},\ X = \left\{ t, X(t)\Big|_{t\in[t_0,t_k]} \right\}. \quad (6)$$

Используя выражение (5), можно записать

$$in(t) = \Phi(x(t - \mathrm{t}),\ in(t - \mathrm{t})), \quad (7)$$

где

$$t, t-\tau\big|_{\tau\geq 0},\ t \in \left[t_0, t_k\right],$$

$in(t) = (in_1(t),\ in_2(t),\ ...,\ in_N(t))$ – сложный вектор входов в момент времени t;
$in(t - \mathrm{t}) = (in_1(t - \mathrm{t}),\ in_2(t - \mathrm{t}),\ ...,\ in_N(t - t))$ – сложный вектор входов в момент времени t-t;

$$in_j(t) = (in_j^1(t), in_j^2(t), \ldots, in_j^N(t)),$$

$$j = \overline{1,N}.$$

Анализ выражения (7) показывает, что значения выходного вектора системы СЗИ в момент времени t зависит от значений входного вектора в момент времени $(t - \mathrm{t})$ и длительности t, где t Î $[t_0, t_k]$.

При условии непрерывности действия на всем интервале времени $[t_0, t_k]$ закон движения системы в векторной форме можно представить в виде интегрального уравнения:

$$I\left(t\right) = \int_{t_0}^{t_k} \Phi\left(X\left(t-\tau\right), I\left(t-\tau\right)\right)dt. \quad (8)$$

Далее объектом рассмотрения будет интегральное уравнение (8) в евклидовом пространстве I. Будем считать, что для (8) в некоторой области $\Omega \in I$ выполнены условия существования и единственности решения, а также что Ω совпадает со всем пространством I. Интересными являются решения (8), начинающиеся в момент t_0. Обозначим метрику пространства I через ρ, а через $I\left(t, I_0\right)$, $t \subset \left[t_0, t_k\right]$ – решение (8) с начальным условием $I(t_0) = I_0$.

Рассмотрим классическое определение устойчивости Ляпунова и некоторые его модификации. Анализ устойчивости по Ляпунову дает ответ на вопрос о том, насколько отличается возмущенное движение системы от невозмущенного. Под невозмущенным движением понимается некоторое фиксированное решение (8), а под возмущенным – решение этого же уравнения, полученное при варьировании начальных условий.

Результаты исследования и их обсуждение

Основываясь на вышеизложенном и полученных научных результатах в работах [1, 3, 4], понятие устойчивости функционирования СЗИ при выбранной ПБ, являющееся модификацией определения устойчивости по Ляпунову [3], можно сформулировать следующим образом.

Определение 1. Решение (невозмущенное) $I(t,\ I_0)$ интегрального уравнения (8) устойчиво по Ляпунову, если для всякого $\theta > 0$ существует такое $\delta(\theta) > 0$, что при любом I'_0, удовлетворяющем условию $\rho\left(I_0, I'_0\right) < \delta$, $\rho\left[I\left(t, I_0\right), I\left(t, I'_0\right)\right] < \theta$ при всех $t \subset \left[t_0, t_k\right]$.

Иначе говоря, в нашем случае устойчивость по Ляпунову уравнения (8) есть равномерно непрерывная зависимость его решений на конечных интервалах времени, что выполняется для достаточно широкого класса функций [7].

Так называемая асимптотическая устойчивость помимо непрерывности требует, чтобы возмущенная траектория при $t \to t_k$ стремилась к невозмущенной в смысле расстояния ρ.

Определение 2. Решение (невозмущенное) $I(t,\ I_0)$ интегрального уравнения (8) асимптотически устойчиво, если оно устойчиво

по Ляпунову и $\lim_{t \to t_k} \rho\left[I\left(t, I_0\right), I\left(t, I_0'\right)\right] = 0$ при всех $t \subset \left[t_0, t_k\right]$.

Если все решения уравнения (8) ограничены при $t \subset \left[t_0, t_k\right]$, то говорят об устойчивости по Лагранжу [3, 6], которое в этом случае при рассмотрении качественных свойств СЗИ использовать целесообразней. Для этого случая понятие устойчивости функционирования СЗИ при выбранной политике безопасности можно сформулировать следующим образом.

Определение 3. Система защиты информации при выбранной политике безопасности устойчива, если для любого $I\left(t_0\right) \subset \Im_0$ имеет место решение $I\left(t\right) \subset \Im$ уравнения (8) для $t > t_0$, $t \subset \left[t_0, t_k\right]$.

В определении: $\Im_0$ – множество допустимых начальных состояний защищаемой информации при выбранной политике безопасности в момент $t = t_0$; $\Im$ – множество допустимых состояний защищаемой информации.

Выводы

Анализ устойчивости динамической системы безопасности на основе теоретико-множественной модели позволяет сделать следующие выводы.

В определениях 1 и 2 допускается существование достаточно малой области в пространстве возмущающих параметров, воздействующих на СЗИ при выбранной политике безопасности, при которых система будет устойчива по Ляпунову или даже асимптотически устойчива. В реальных прикладных задачах не всегда удается использовать достаточно малую окрестность возмущений. В этом случае используют понятие устойчивости по Лагранжу, которое можно интерпретировать как сохранение свойства траекторий СЗИ находиться в допустимой области пространства состояний (заданное качество СЗИ) при действии возмущений произвольной величины на начальные состояния. Как правило, множества $\Im_0$ и $\Im$ задаются на основе экспертных оценок и ограничений функционирования СЗИ при выбранной политике безопасности.

Список литературы

1. Айзерман М.А. Техническая кибернетика. Теория автоматического регулирования. Кн.1 / под ред. В.В. Солодовникова. – М.: Машиностроение, 1967. – 768 с.

2. Амрахов И.Г. Анализ и синтез технологической системы обработки деталей на основе динамической устойчивости: дис. ... д-ра техн. наук. – Воронеж, 1999. – 275 с.

3. Бусленко Н.П. Лекции по теории сложных систем / Н.П. Бусленко, В.В. Калашников, И.Н. Коваленко. – М.: Сов. радио, 1973. – 440 с.

4. Ляпунов А.М. Собрание сочинений. Т.2. – М.-Л.: Академия наук СССР, 1956. – 437 с.

5. Мирошина И.Е., Чулюков В.А. Распределенная информация, средства защиты и средства воздействия в модели вычислительной сети // Сборник научных трудов Sworld. – Вып. 3. Т. 5. – Одесса: КУПРИЕНКО, 2013. – С. 36–39.

6. Острём К. Системы управления с ЭВМ / К. Острём, Б. Виттенмарк. – М.: Мир, 1987. – 480 с.

7. Понтрягин Л.С. Обыкновенные дифференциальные уравнения. – М.: Наука, 1974. – 331 с.

References

1. Ajzerman M.A. Tehnicheskaja kibernetika. Teorija avtomaticheskogo regulirovanija. Kn.1 / pod red. V.V. Solodovnikova. M.: Mashinostroenie, 1967. 768 p.

2. Amrahov I.G. Analiz i sintez tehnologicheskoy sistemy obrabotki detaley na osnove dinamicheskoy ustoichivosti: dis. dokt. tehn. nauk. Voronezh: 1999. 275 p.

3. Buslenko N.P. Lekcii po teorii slozhnyh sistem / N.P. Buslenko, V.V. Kalashnikov, I.N. Kovalenko. M.: Sov. radio, 1973. 440 p.

4. Lyapunov A.M. Sobranie sochineniy. T.2. M.-L.: Akademiya nauk SSSR, 1956. 437s.

5. Miroshina I.E., Chuliukov V.A. Raspredelennaya informaciya, sredstva zaschity i sredstva vozdeistviya v modeli vychislitel'noy seti // Sbornik nauchnyh trudov Sworld. Vypusk 3. Tom 5. Odessa: KUPRIENKO, 2013. pp. 36–39.

6. Ostrem K. Sistemy upravleniya s EVM / K. Ostrem, B. Vittenmark. M.: Mir, 1987. 480 p.

7. Pontryagin L.S. Obyknovennye differencial'nye uravneniya. M.: Nauka, 1974. 331 p.

Рецензенты:

Астахова И.Ф., д.т.н., профессор кафедры математического обеспечения ЭВМ, ФГБОУ ВПО «Воронежский государственный университет», г. Воронеж;

Дубровин А.С., д.т.н., профессор кафедры управления и информационно-технического обеспечения, ФКОУ ВПО «Воронежский институт Федеральной службы исполнения наказаний», г. Воронеж/

Работа поступила в редакцию 28.10.2014.