ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ С ИСПОЛЬЗОВАНИЕМ ПАРАМЕТРИЧЕСКИХ МОДЕЛЕЙ ЭВОЛЮЦИИ

Кубарев А.В.[1], Лапсарь А.П.[2], Федорова Я.В.[3]

Цель статьи: разработка метода повышения безопасности значимых объектов критической информационной инфраструктуры в условиях нештатного режима их эксплуатации, вызванного деструктивным информационным воздействием.

Методы: синтез диффузионной марковской модели исследуемого объекта в параметрическом виде; анализ имеющихся способов и математических моделей оценки состояния сложных технических систем и выбор оптимальной.

Полученный результат: на основе известного аппарата диффузионных марковских процессов в работе предложен оригинальный метод оперативной оценки состояния значимых объектов критической информационной инфраструктуры в процессе их функционирования для повышения безопасности их эксплуатации. Повышение оперативности оценки достигнуто путем разделения процесса оценки на два периода, при этом наиболее трудоемкий и длительный процесс получения базовых решений эволюционных уравнений, моделирующих поведение исследуемого объекта, проводится заблаговременно. Вычисление стохастических характеристик объекта критической информационной инфраструктуры, характеризующих его техническое состояние, проводится непосредственно при обнаружении деструктивного воздействия на основе полученных ранее базовых решений. Полученная оценка технического состояния позволяет спланировать меры по повышению безопасности объекта.

В работе также рассмотрен процесс синтеза эволюционных уравнений, описывающих поведение объекта исследования в параметризованном виде, получения их базовых решений, а также алгоритм реализации предложенного метода. Результаты проведенного исследования могут быть использованы при разработке технических заданий (частных технических заданий) на модернизацию систем безопасности объектов критической информационной инфраструктуры.

Ключевые слова: сложный технический объект, деструктивное воздействие, марковские модели, эволюционные уравнения, базовые решения, оценка состояния, оперативность оценки.

DOI:10.21681/2311-3456-2020-01-08-17

Введение

В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. №646, отмечается, что информационные технологии стали неотъемлемой частью всех сфер деятельности личности, общества и государства. При этом расширение областей применения информационных технологий, являясь фактором развития экономики и повышения производительности труда, одновременно порождает новые информационные угрозы, реализация которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка [1- 4].

Одним из основных негативных факторов, влияющих на состояние информационной безопасности Российской Федерации, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях. Большинством развитых зарубежных стран создаются специальные формирования, задачей которых является осуществление компьютерных атак на критическую информационную инфраструктуру противника. При этом ущерб, который они могут нанести часто бывает сравним с ущербом, наносимым традиционными средствами поражения. Именно поэтому в последние годы регулярно проходят учения зарубежных силовых структур, на которых от-

1 Кубарев Алексей Валентинович, преподаватель АНО ДПО «Учебный центр «Эшелон, г. Москва, Россия. E-mail: mr.kubarev@gmail.com

2 Лапсарь Алексей Петрович, кандидат технических наук, доцент, заместитель начальника отдела Управления ФСТЭК России по Южному и Северо-Кавказскому федеральным округам, г. Ростов-на-Дону, Россия. E-mail: lapsar1958@mail.ru

3 Федорова Яна Владимировна, доцент кафедры «Информационных технологий и защиты информации», ФГБОУ ВО Ростовский государственный экономический университет (РИНХ), г. Ростов-на-Дону, Россия. E-mail: fyv21@mail.ru

рабатываются тактики и приемы противодействия компьютерным атакам, а также осуществление таких атак. Кроме того, учитывая доступность средств проведения компьютерных атак и отсутствие необходимости наличия специальных навыков для их проведения, такие атаки активно проводятся преступными группировками и одиночными хакерами. Исходя из этого интенсивность, сложность и продолжительность деструктивного воздействия могут существенно различаться.

Каждую неделю в средствах массовой информации появляются сообщения об успешной реализации компьютерных атак на объекты информационной инфраструктуры различных стран. Успешная реализация компьютерной атаки на объекты критической информационной инфраструктуры может в отдельных случаях привести к катастрофическим последствиям. В связи с этим обеспечению защиты таких объектов информационной инфраструктуры от угроз безопасности информации необходимо уделять особое внимание.

В целях обеспечения устойчивого функционирования критической информационной инфраструктуры Российской Федерации при проведении в отношении нее компьютерных атак в 2017 году принят Федеральный закон «О безопасности критической информационной инфраструктуры». В соответствии с указанным Федеральным законом к критическим относятся информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети в сферах энергетики, топливно-энергетического комплекса, атомной энергии, оборонной, ракетно-космической, химической промышленности и других. Объекты критической информационной инфраструктуры, ущерб от нарушения функционирования которых в результате компьютерных атак имеет наибольшее значение, относятся к значимым объектам критической инфраструктуры информации (ЗОКИИ).

Значимые объекты критической инфраструктуры различаются по назначению, свойствам, принципам работы, условиям функционирования, однако имеют ряд общих признаков и особенностей. Процессы, происходящие в ЗОКИИ, носят случайный характер, вызванный как внутренними процессами в объекте, так и воздействием внешних факторов: смежных систем, окружающей среды информационного пространства и иных. На них влияет широкий спектр многофакторных воздействий, связанных со спецификой их функционирования. Эти же воздействия оказывают влияние на информационно-управляющие системы ЗОКИИ, что приводит к тому, что процессы измерения и контроля являются нестационарными случайными процессами с априори неизвестными статистическими свойствами. Физические процессы и информационные деструктивные воздействий, предшествующих возникновению аварийной ситуации, нештатной ситуации и последующему нарушения штатного режима функционирования ЗОКИИ слабо изучены и не формализованы. Вместе с тем, в ЗОКИИ имеет место определенная параметрическая избыточность, что позволяет повысить надежность и безопасность их функционирования, а также обеспечивает возможность оценки их состояния на некотором интервале времени [5,6].

Исходя из вышесказанного и учитывая, что ЗОКИИ состоят из большого числа разнородных элементов, блоков, подсистем, названные объекты необходимо рассматривать как сложные технические системы. Из теории систем известно [2,6,7], что система является сложной, если она состоит из большого числа взаимосвязанных и взаимодействующих между собой элементов (подсистем) и способна выполнять сложную функцию. Основной отличительной особенностью сложного объекта является то, что его отказ не наступает внезапно, а является следствием снижения качества и дрейфа показателей его функционирования за границы области допустимых значений. Однако построение единой универсальной модели оценки технического состояния ЗОКИИ, связанной со снижением заложенного при вводе в эксплуатацию ресурса, чрезвычайно затруднено. Широко используемые в теории надежности модели регрессии не отражают специфики функционирования ЗОКИИ [6-11].

Возникает проблема выбора или синтеза модели, учитывающей не только техническое состояние объекта, но и его взаимодействие с внешней средой и смежными системами. При этом необходимо учитывать возможность целенаправленного деструктивного воздействия на ЗОКИИ с целью нарушения режима его штатного функционирования [12-14].

Одной из основных задач, решаемых при эксплуатации ЗОКИИ является поддержание их функционирования с требуемой надежностью, безопасностью и готовностью к использованию по назначению, в том числе и при возникновении нештатной ситуации. Поскольку нештатная ситуация может развиваться на протяжении продолжительного времени, остро встает задача планирования поддержания ЗОКИИ в работоспособном состоянии в течение некоторого времени, необходимого для проведения мероприятий по нейтрализации негативных последствий. Известны случаи, когда продолжительность деструктивного воздействия на объект составляла несколько недель [12].

Результатами деструктивного информационного воздействия могут быть полный или частичный отказ объекта, нарушение штатного режима функционирования, ухудшение его качества, снижение эффективности системы безопасности объекта и другие. Кроме прямых потерь от нарушения штатного режима функционирования объекта следует учитывать и косвенные. К ним относятся репутационные потери, судебные издержки, расход ресурсов на отражение деструктивного воздействия и ликвидацию его последствий: расход времени, материальных средств, человеческих ресурсов, блокировка участков памяти и других.

В работах по надежности важных и потенциально опасных технических объектов в качестве защиты от неисправности и усугубления последствий развития аварии предлагается прекращать работу объекта [7,8,10,13]. Такой подход возможен и применительно к ЗОКИИ, однако при этом должны быть учтены последствия остановки объекта и не только экономический

ущерб, но и социальные, политические, экологические и другие последствия [2-4]. Потери от выхода из строя ЗОКИИ при аварии, вызванной деструктивным воздействием, как правило, существенно выше, чем при реализации мер по предупреждению развития аварийной ситуации: плановой остановке объекта, отключении отдельных подсистем, проведении дополнительных мероприятий по обеспечению нормального функционирования объекта.

Принятие решения о составе и объеме мероприятий по купированию угроз информационной безопасности должно базироваться не только на оценке текущего состояния ЗОКИИ, но и на прогнозе развития аварийной ситуации. Для этого требуется оценить состояние объекта на некоторый последующий период времени, что осуществляется на базе эффективных моделей. Это особенно актуально для социально значимых объектов, имеющих непрерывный цикл работы, таких как системы отопления, энерго и водоснабжения, очистные сооружения, системы жизнеобеспечения и других. При этом следует отметить, что проблему обеспечения безопасности функционирования ЗОКИИ в условиях деструктивного информационного воздействия не следует рассматривать в отрыве от обеспечения технической надежности и безопасности объекта. Оценку состояния объектов КИИ будем рассматривать в широком смысле, то есть не только в текущий момент времени, но и на некоторую перспективу, обусловленную спецификой решаемых задач по эксплуатации ЗОКИИ [5,6,9,11,13].

Выбор модели оценки состояния значимого объекта критической информационной инфраструктуры

В настоящее время известно множество моделей оценки технического состояния и надежности сложных технических объектов, к которым относятся и ЗОКИИ [5,8,11,13-15]. Однако абсолютное большинство таких моделей описывают штатную эксплуатацию технического объекта и базируются на процессах регрессии. Поэтому все классические методы неприменимы в условиях деструктивного информационного воздействия из-за следующих особенностей возникающего при этом нештатного режима эксплуатации:

- дефицит времени на оценку состояния объекта и принятие решения по выработке управляющих воздействий;
- расширение области определения параметров объекта в связи с их выходом за границы области допусков и возрастания параметрической неопределенности;
- существенное повышение уровня внутренних шумов и внешних помех, снижающих достоверность оценки;
- резкое возрастание динамической погрешности оценки даже при незначительном изменении параметров объекта;
- необходимость оценки последствий принятых решений с целью исключения усугубления нештатной ситуации.

Значимый объект критической информационной инфраструктуры как сложная система при отказе отдельных элементов, блоков и даже подсистем не всегда теряет работоспособность, зачастую только снижаются характеристики ее эффективности. Отказ ЗОКИИ следует определять как событие, заключающееся в выходе характеристик его функционирования за установленные пределы.

Для формального описания нештатного режима эксплуатации ЗОКИИ требуется выбрать или синтезировать соответствующую модель. Модель, используемая для решения задачи оценки технического состояния ЗОКИИ в условиях нештатного режима эксплуатации, должна быть максимально адекватной исследуемому объекту. Предъявляемому требованию наиболее соответствуют модели, синтезированные на основе диффузионных (эволюционных) марковских процессов [6,16,17], которые в настоящее время находят все более широкое применение. В основе таких моделей лежит стохастическое дифференциальное уравнение в форме Ито[4]:

$$dx = f(x,t)dt + g(x,t)dw(t),$$

где $f(x,t)$, $g(x,t)$ – коэффициенты сноса и диффузии марковского процесса соответственно, w – винеровский процесс.

Отличительной особенностью марковских моделей является отсутствие последействия, что позволяет применять их в условиях нештатного режима эксплуатации, связанного с развитием аварийной ситуации. Отсутствие последействия означает, что при оценке поведения процесса в последующий момент времени существенным является только знание состояния этого процесса в настоящий момент времени. Поведение диффузионного марковского процесса применительно к конкретному ЗОКИИИ полностью описывается его стохастическими характеристиками, то есть коэффициентами сноса, характеризующим среднее значение локальной скорости, и диффузии – локальную скорость изменения дисперсии приращения марковского процесса.

Синтез параметризованной марковской модели значимого объекта критической информационной инфраструктуры

Рассмотрим использование диффузионных марковских процессов применительно к задаче оценки состояния ЗОКИИ в условиях нештатного режима эксплуатации, связанного с развитием аварийной ситуации, вызванной деструктивным информационным воздействием.

Пусть вектор технического состояния $x(t) \in R^r$ некоторого ЗОКИИ описывается стохастическим дифференциальным уравнением

$$\frac{dx(t)}{dt} = f_л(x,t) + g_л(x,t)n_ф(t), \quad x(t_0) = x_0 \ , \qquad (1)$$

где $f_л(x,t) \in R^r, g_л(x,t) \in R^r \times R^r$ – детерминированные функции соответствующих аргументов, удовлетворяющие условию Липшица

4 Ито Киёси — японский математик-статистик.

$$|f_л(x_2,t)-f_л(x_1,t)|+|g_л(x_2,t)- \\ -g_л(x_1,t)|\le L|x_2-x_1|,\ L>0, \quad (2)$$

$n_ф(t)\in R^r$ – формирующий нормальный белый шум с известными статистическими характеристиками:

$$M\left[n_ф(t_1)n_ф^T(t_2)\right]=\frac{N_ф}{2}\delta(t_2-t_1),$$

$M\left[n_ф(t)\right]=0$, $N_ф$ – спектральная плотность шума.

Если в качестве отказа (нарушения работоспособности) объекта принять выход хотя бы одного параметра $x_i(t)$, $i\in 1,r$, за границу допустимой области $G_{Д,i}\subset R^1$, то вероятность безотказной работы ЗОКИИ:

$$P_N(x,s)\equiv P\{x(t)\in G_Д,\forall t\in \\ \in[s,T]|x(s)\in G_Д\},\ G_Д\subset R^r, \quad (3)$$

где $P_N(x,s)$ – вероятность того, что процесс $x(t)$ ни разу не выйдет за границы допустимой области $G_{Д,i}\subset R^1$, на интервале $[s,T]$ при условии, что в начальный момент времени он находился в допустимой области $G_Д$,, то есть объект был исправен.

Для скалярного случая ($r=1$) вероятность $P_N(x,s)$ удовлетворяет дифференциальному уравнению в частных производных

$$-\frac{\partial P_N(x,s)}{\partial s}=a(x,s)\frac{\partial P_N(x,s)}{\partial x}+ \\ +\frac{1}{2}b(x,s)\frac{\partial^2 P_N(x,s)}{\partial x^2} \quad (4)$$

при начальном условии $P_N(x,T)=1$.

Сделав замену переменных $t=T-s$, получим

$$\frac{\partial P_N(x,t)}{\partial t}=a(x,t)\frac{\partial P_N(x,t)}{\partial x}+ \\ +\frac{1}{2}b(x,t)\frac{\partial^2 P_N(x,t)}{\partial x^2},\ U(x,t_0)=1. \quad (5)$$

Очевидно, что второму (прямому) уравнению Фоккера-Планка-Колмогорова удовлетворяет плотность вероятности $p(x,t)$:

$$\frac{\partial p(x,t)}{\partial t}=-\frac{\partial}{\partial x}[a(x,t)p(x,t)]+ \\ +\frac{1}{2}\frac{\partial^2}{\partial x^2}[b(x,t)p(x,t)],\ p(x,t_0)=p_0(x). \quad (6)$$

Таким образом, при назначенных граничных условиях, исходя из конкретной задачи, характеристики ЗОКИИ в момент выхода за границы области допустимых значений параметра $x_i(t)$ могут быть получены из соотношений (4)-(6). Границы допустимой области определяются исходя из требований стандартов предприятий, технических заданий (условий), других проектных и эксплуатационных документов.

В реальных условиях функционирования объекта исследования возникает необходимость решения уравнений (4)-(6) в случае зависимости исследуемого процесса от некоторых параметров $\omega\in\Omega\subset R^m$. Наиболее значимые для оценки работоспособности ЗОКИИ параметры определяются начальными и граничными условиями, внешней средой, реальными условиями функционирования объекта, внешними воздействиями и т. п. Для решения задачи оценки состояния ЗОКИИ в условиях нештатного режима эксплуатации к наиболее информативным параметрам следует отнести свойства деструктивного информационного воздействия, например его вид, интенсивность, продолжительность, сложность, критичность атакуемых узлов и управляемых ими процессов.

Названные параметры определяют значения коэффициентов сноса и диффузии исследуемого процесса, а также другие составляющие диффузионных уравнений. Тогда, на основании (3)

$$P_N(x,\omega,s)\equiv P\{x(\omega,t)\in G_Д, \\ \forall t\in[s,T]|x(\omega,s)\in G_Д\}. \quad (7)$$

Уравнения (4)-(6) в этом случае примут вид:

$$-\frac{\partial P_N(x,\omega,s)}{\partial s}=a(x,\omega,s)\frac{\partial P_N(x,\omega,s)}{\partial x}+, \\ +\frac{1}{2}b(x,\omega,s)\frac{\partial^2 P_N(x,\omega,s)}{\partial x^2},\ P_N(x,\omega,T)=1 \quad (8)$$

$$\frac{\partial P_N(x,\omega,t)}{\partial t}=a(x,\omega,t)\frac{\partial P_N(x,\omega,t)}{\partial x}+, \\ +\frac{1}{2}b(x,\omega,t)\frac{\partial^2 P_N(x,\omega,t)}{\partial x^2},\ P_N(x,\omega,t_0)=1 \quad (9)$$

$$\frac{\partial p(x,\omega,t)}{\partial t}=-a(x,\omega,t)\frac{\partial p(x,\omega,t)}{\partial x}+ \\ +\frac{1}{2}b(x,\omega,t)\frac{\partial^2 p(x,\omega,t)}{\partial x^2},\ p(x,\omega,t_0)=p_0(x,\omega) \quad (10)$$

Как известно, плотность распределения стохастического процесса является наиболее его информативной характеристикой. Синтезировав решение (8)-(10), получим другие значимые для принятия решения о последующей эксплуатации ЗОКИИ характеристики.

На базе решения уравнения (3) можно оценить параметрическую надежность ЗОКИИ в заданных точках интервала оценки состояния (в том числе и на некоторый последующий интервал времени), время достижения границ допустимой области, потенциальную опас-

ность деструктивного информационного воздействия на объект, назначить оптимальные допуска и ограничения на параметры функционирования.

Математическая постановка задачи оценки состояния ЗОКИИ выглядит следующим образом.

Рассмотрим в некотором нормированном пространстве W_0 эволюционные уравнения (ЭУ) в частных производных характеризующие r - мерный марковский процесс технического состояния объекта $x(t)$

$$\frac{\partial p(x,\omega,t)}{\partial t} = L^{(r)}_{\omega,t}\left\{p(x,\omega,t)\right\}, p(x,\omega,t)\in W, \quad (11)$$

$$x\in X\subset R^r,\ t\in\tilde{T}\subset R^1,$$

где $L^{(r)}_{\omega,t}$ – оператор эволюционного уравнения: априорный или апостериорный, $\tilde{T}=T+\tau$. Оператор $L^{(r)}_{\omega,t}$ зависит от вещественного векторного параметра ω, принимающего значения из ограниченной выпуклой многомерной области $\Omega\subset R^m$.

Искомое решение $p_\omega(x,\omega,t)$ уравнения (11) для всех $\omega\in\Omega\subset R^m$ подчинено дополнительным условиям вида

$$\Gamma_j\left[p_\omega(x,\omega,t)\right]\Big|_{(x,t)\in S_i} = \phi_j(S_i), \quad =1, \quad (12)$$

$$i=\overline{1,L_0},\ j=\overline{1,L_1}$$

где Γ_j – линейный непрерывный оператор, действующий в W, S_i - некоторое многообразие в области $X\times\tilde{T}$, число измерений которого меньше $r+1$, $\phi_j(S_i)$ – заданная функция, определенная на многообразии S_i.

В условиях нештатного режима функционирования ЗОКИИ получение информации о его текущем состоянии и оценка основных стохастических характеристик на некоторый период является необходимым условием предотвращения развития аварийной ситуации и безопасности его дальнейшей эксплуатации. Задача оценки стохастических характеристик состоит из двух частных задач: определение плотности распределения стохастического процесса $p_\omega(x,\omega,t)$ и собственно вычисление требуемых характеристик. При этом первая частная задача, связанная с решением уравнений эволюции, является наиболее трудоемкой, требует существенных временных затрат, а также разработки нового метода решения для синтеза искомой плотности распределения процесса сразу в параметризованном виде.

Метод получения базовых решений параметризованных уравнений эволюции

Представим задачу (11) с граничными условиями вида (12) в виде одного точного операторного уравнения по аналогии с [6,18]

$$p(x,\omega,t)-\lambda K(\omega)p(x,\omega,t)=f(x,\omega,t), \quad (13)$$

$$f(x,\omega,t)\in W,$$

где $K(\omega)$ – линейный непрерывный оператор, действующий в нормированном пространстве $W\subset W_0$, λ – некоторая постоянная, не являющаяся характеристическим значением оператора $K(\omega)$ для $\omega=\left(\omega_0^T,\omega_1^T,...,\omega_{L_1}^T\right)^T\in\Omega=\Omega_0\times\Omega_1\times...\times\Omega_{L_1}\subset R^m=R^{m_0}\times R^{m_1}\times...\times R^{m_{L_1}}$, $f(x,\omega,t)$ – заданная функция из W.

Полагаем, что по результатам решения первой частной задачи может быть построено аналитико-параметрическое решение $p_\omega(x,\omega,t)$ операторного уравнения (13), а затем определена совокупность искомых стохастических характеристик ЗОКИИ $Y_i(\omega)=F_i\left[p_\omega(x,\omega,t)\right]$, $i=\overline{1,M_0}$, $\omega\in\Omega$, где $F_i[\cdot]$ – ограниченные непрерывные функционалы.

Поскольку вместо $p_\omega(x,\omega,t)$ можно определить лишь приближенное решение $\tilde{p}(x,\omega,t)$ уравнения $=1,$ (13), то и вместо $\left\{Y_i(\omega)\right\}_{i=1}^{M_0}$ вычисляется лишь семейство $\left\{\tilde{Y}_i(\omega)\right\}_{i=1}^{M_0}$ приближенных стохастических характеристик.

Таким образом, необходимо с учетом принятых моделей и ограничений разработать метод оперативного оценивания стохастических характеристик ЗОКИИ как марковских параметрических систем с приемлемой точностью.

По аналогии с [17-19] запишем приближенное уравнение (13)

$$\tilde{p}(x,\omega,t)-\lambda\ PK(\omega)\tilde{p}(x,\omega,t)=Pf(x,\omega,t), \quad (14)$$

где P – непрерывный линейный оператор, проектирующий W на свое полное подпространство $\tilde{W}$.

Решение уравнения (14) считается приближенным решением исходного уравнения (13) и представляется в виде $\tilde{p}(x,\omega,t)=\sum_{i=1}^{\infty}c_i(\omega)\gamma_i(x,t)$, где $\gamma_i(x,t)\in\tilde{W}$

Уравнение (14) представим в параметрическом (зависящем от параметра ω) виде с использованием метода Галеркина [18,19]

$$\sum_{k=1}^{\infty} c_k(\omega) D_j[\gamma_k(x,t)] - \lambda \sum_{k=1}^{\infty} c_k(\omega) D_j[PK(\omega)\gamma_k(x,t)] = D_j[Pf(x,\omega,t)], j = 1,2,..., \quad (15)$$

где $\{D_j\}$ – система функционалов, биортогональная базису $\{\gamma_k(x,t)\}$.

Основным методом определения неизвестных коэффициентов $c_k(\omega)$ считается метод, заключающийся в составлении бесконечной системы линейных алгебраических уравнений с последующим ограничением их числа

$$c_j(\omega) - \lambda \sum_{k=1}^{\infty} a_{jk}(\omega) c_k(\omega) = b_j(\omega), \qquad j = 1,2,..., \quad (16)$$

где

$$\sum_{j,k=1}^{\infty} |a_{jk}(\omega)|^2 < \infty, \quad \sum_{j=1}^{\infty} |b_j(\omega)|^2 < \infty, \quad \sum_{k=1}^{\infty} |c_k(\omega)|^2 < \infty, \quad \omega \in \Omega.$$

Конечная система линейных алгебраических уравнений метода Галеркина, полученная из (16) путем «усечения», записывается так [18,19]

$$c_j(\omega) - \lambda \sum_{k=1}^{n} a_{jk}(\omega) c_j(\omega) = b_j(\omega), \quad j = \overline{1,n}, \quad \|c_n(\omega)\|_{l_n^2} = \left[\sum_{k=1}^{n} |c_k(\omega)|^2\right]^{1/2}. \quad (17)$$

Суть предлагаемого метода состоит в том, что область Ω возможных значений параметра ω разбивается на подобласти, в каждой из которых значение ω считается квазипостоянным, а затем строится сетка узлов мощностью N. Далее для каждого фиксированного узла ищется частное решение соответствующей конечной системы линейных алгебраических уравнений

$$c_{nj}(\omega_{(i)}) - \lambda \sum_{k=1}^{n} a_{jk}(\omega_{(i)}) c_{nj}(\omega_{(i)}) = b_j(\omega_{(i)}), \quad j = \overline{1,n}, \quad i \in \overline{1,N}, \quad (18)$$

где $\{\omega_{(i)}\}$ – узлы сетки. Коэффициенты $c_{nj}(\omega)$ найденных частных решений затем интерполируются для нахождения обобщенных коэффициентов $\tilde{c}_{[n]}(\omega)$, которые являются непрерывными функциями от параметра ω.

Приближенное аналитическое решение бесконечной системы линейных алгебраических уравнений (17) строится в виде

$$\tilde{c}_{[n]}(\omega) = \{\tilde{c}_{n1}(\omega), \tilde{c}_{n2}(\omega), ..., \tilde{c}_{nn}(\omega), 0, 0, ...\} = \{\theta_n(\omega, v_1), \theta_n(\omega, v_2), ..., \theta_n(\omega, v_n), ...\}, \quad (19)$$

где $\theta_n(\omega, v_i)$ – интерполяционная функция, v_i – вектор коэффициентов, $i = \overline{1,n}$. Если в качестве интерполирующей функции принять степенной полином, то решение (16) с учетом (19)

$$\tilde{c}_{[n]}(\omega) = \left\{\sum_{k=1}^{N} v_{1k} \omega^k, \sum_{k=1}^{N} v_{2k} \omega^k, ..., \sum_{k=1}^{N} v_{nk} \omega^k, 0, 0, ...\right\}, \quad (20)$$

если интерполяционный полином Лагранжа, то

$$\tilde{c}_{[n]}(\omega) = \left\{\sum_{k=1}^{N} c_{n1}(\omega_{(k)}) L_k(\omega), \sum_{k=1}^{N} c_{n2}(\omega_{(k)}) L_k(\omega), ..., \sum_{k=1}^{N} c_{nn}(\omega_{(k)}) L_k(\omega), 0, 0, ...\right\}, \quad (21)$$

где $L_k(\omega) = \prod_{\substack{p=0 \\ p \neq k}}^{N} \frac{\omega - \omega_{(p)}}{\omega_{(k)} - \omega_{(p)}}$

Точность решения параметризованного ЭУ для отрезка $\Omega = [\omega_1, \omega_2]$, где ω_1 и ω_2 верхнее и нижнее значения $\omega \in \Omega$. соответственно, на основе интерполяционного полинома Лагранжа оценивается выражением [20,21]

$$\sup_{\omega} \left\| [c(\omega)]_n - \tilde{c}_{[n]}(\omega) \right\| \leq 2 \left(\frac{d_2 - d_1}{4}\right)^N \frac{G_N}{N!} n^{1/2}, \quad (22)$$

$$G_N = \max_j \sup_{\omega} \left| \frac{d^N c_j(\omega)}{d\omega^N} \right|.$$

Приближенное решение на основе степенного полинома с учетом (20)

$$\tilde{p}_n(x,\omega,t) = \sum_{i=1}^{n} \sum_{k=1}^{N} v_{ik} \omega^k \gamma_i(x,t), \quad (23)$$

а решение на основе интерполяционного полинома Лагранжа

$$\tilde{p}_n(x,\omega,t) = \sum_{i=1}^{n} \sum_{k=1}^{N} c_{ni}(\omega_{(k)}) L_k(\omega) \gamma_i(x,t). \quad (24)$$

Оценка точности решения параметризованного ЭУ разработанным методом применительно к (23) и (24) производится по формуле [20, 21]

$$\left\| p(x,\omega,t) - \tilde{p}(x,\omega,t) \right\| \le \frac{q}{1-q} \left\| \tilde{p}(x,\omega,t) \right\|, \quad (25)$$

$$q = |\lambda| \varepsilon \| I - P \| \left\| \left(I - \lambda K(\omega) \right)^{-1} \right\| < 1,$$

где ε – заданное число, I – единичный оператор. Соответственно для случая (25) справедлива оценка

$$\left\| \tilde{p}(x,\omega,t) - \tilde{p}_n(x,\omega,t) \right\| \le \left\| \sum_{i=1}^{n} \left[c_i(\omega) - c_{ni}(\omega) \right] \gamma_i(x,t) \right\| + \left\| \sum_{i=n+1}^{\infty} c_i(\omega) \gamma_i(x,t) \right\|. \quad (26)$$

Таким образом, заранее задавая значение ε, характеризующее точность интегрирования (15), по формулам (25), (26) находятся параметры сетки интерполяции, обеспечивающие заданную точность расчетов.

На базе приближенного решения $\tilde{p}(x,\omega,t)$ для плотности вероятности $p(x,\omega,t)$ несложно получить аналитические зависимости для оценки стохастических характеристик ЗОКИИ. Наиболее значимыми для оценки состояния объекта, подвергнувшегося деструктивному информационному воздействию, можно считать вероятность безотказной работы в течение заданного времени, время достижения параметрами функционирования границ допустимой области, потенциальную опасность объекта после окончания воздействия [6-8, 14, 17]. На основе полученных стохастических характеристик можно оперативно принять решение о дальнейшем использовании объекта, выработать стратегию устранения последствий деструктивного воздействия и повышения устойчивости к таким воздействиям.

С учетом найденного решения $\tilde{p}(x,\omega,t)$ найдем семейство оценок искомых приближенных стохастических характеристик: $\tilde{Y}_i(\omega) = F_i\left[\tilde{p}(x,\omega,t) \right], \quad i = \overline{1, M_0}$.

Очевидно, что точность оценки складывается из двух составляющих: точности получения $\tilde{p}(x,\omega,t)$ – решения параметризованных ЭУ и точности вычисления стохастических характеристик, определяемой свойствами функционалов $F_i[\cdot]$, $i = \overline{1, M_0}$.

Соотношения для искомых стохастических характеристик, представим в следующем виде (считая для простоты $F_i[\cdot]$ линейными функционалами)

$$\tilde{Y}_i(\omega) = F_i\left[p_\omega(x,\omega,t) + \Delta p(x,\omega,t) \right] = F_i\left[p_\omega(x,\omega,t) \right] + F_i\left[\Delta p(x,\omega,t) \right] = \tilde{Y}_i(\omega) + \Delta Y_i(\omega). \quad (27)$$

Предложенный метод оценивания стохастических характеристик ЗОКИИ может быть положен в основу синтеза систем оценки состояния объекта, работающих в масштабе времени, близкому к реальному [17, 22, 23].

Алгоритм выработки управляющих воздействий для обеспечения функционирования ЗОКИИ в условиях нештатного режима эксплуатации

Жизненный цикл ЗОКИИ условно разобьем на несколько этапов.

1. Предварительный этап начинается с момента создания объекта и внедрения на нем системы защиты от последствий нештатного режима эксплуатации.

Основное содержание этого этапа состоит в накоплении информации о поведении характеристик объекта во времени в разных режимах его работы, исследование возможных деструктивных информационных воздействий на него и их последствий. Итогом данного этапа является синтез марковской модели ЗОКИИ в виде параметризованных эволюционных уравнений и оценка области определения параметров Ω. Здесь же осуществляется контроль состояния безопасности и оценка необходимости и состава мероприятий по модернизации ЗОКИИ.

2. Этап штатной эксплуатации – это основной этап. Он завершается в момент обнаружения деструктивного воздействия. Следует отметить, что после прекращения деструктивного воздействия и ликвидации его последствий штатная эксплуатация восстанавливается и данный этап продолжается.

Основное содержание этапа – получение дополнительной информации о ЗОКИИ в параметризованной форме, уточнение модели объекта и базовых решений, расширение и корректировка области возможных деструктивных воздействий, исследование их свойств.

3. Этап нештатного режима эксплуатации начинается с момента обнаружения деструктивного информационного воздействия (ДИВ) специально созданной системой или получения информации о воздействии от смежного объекта или системы высшего уровня.

На данном этапе производится оценка параметра воздействия, оперативное вычисление стохастических характеристик ЗОКИИ, принятие решения о его дальнейшей эксплуатации и формирование управляющих воздействий по восстановлению штатной эксплуатации объекта.

Заключение

В работе предложен метод повышения надежности и безопасности ЗОКИИ в условиях нештатного режима эксплуатации, вызванной деструктивным информационным воздействием. В качестве основы для разработанного метода был использован аппарат диффузионных марковских процессов. Модели на основе диффузионных марковских процессов позволяют решать задачи о достижении границ допустимой области случайным процессом функционирования ЗОКИИ, получать другие его характеристики, что дает возможность оценить состояние объекта и принять оперативное решение о его

дальнейшем использовании, принять дополнительные меры, направленные на повышение устойчивости его функционирования. Такие модели могут быть применены для уникальных высоконадежных объектов и построены даже по одной реализации.

С учетом особенностей, вызванных необходимостью получения оценки состояния ЗОКИИ в масштабе времени, близком к реальному, решения эволюционных уравнений марковской модели получены в параметрическом виде. При этом сам процесс оценки состояния ЗОКИИ, то есть получения стохастических характеристик его функционирования, разбивается на два периода. На первом, включающем в себя первые два этапа жизненного цикла, обеспечивается формирование, хранение и уточнение базовых решений параметризованных эволюционных уравнений. Второй период реализуется в момент обнаружения деструктивного информационного воздействия. Базовые решения, полученные во время первого периода в аналитико-параметрическом виде, используются для оперативной оценки важнейших стохастических характеристик объекта, что, в свою очередь, позволяет принять обоснованное решение о дальнейшем использовании ЗОКИИ и о составе дополнительных мер, направленных на повышение устойчивости его функционирования.

Предложенный метод может быть применен для синтеза внедряемых на объектах ЗОКИИ систем безопасности. Системы безопасности, синтезированные с использованием разработанного метода и интегрированная в общую информационно-управляющую систему, разделяется на две подсистемы. От первой, реализующей первый период, не требуется высокого быстродействия. Она призвана обеспечить формирование базовых решений для оценки состояния сложных и уникальных объектов критической информационной инфраструктуры и может быть выполнена на основе стандартных стационарных ЭВМ и вычислительных комплексов. Вторая подсистема, обеспечивающая хранение базовых решений и оперативное получение оценки состояния объекта, может быть реализована в компактном и мобильном исполнении.

В настоящее время материалы данного исследования используются в разрабатываемых технических заданиях на создание системы защиты от деструктивных информационных воздействий сложных промышленных объектов, классифицированных как ЗОКИИ.

Рецензент: *Цирлов Валентин Леонидович, кандидат технических наук, доцент Московского государственного технического университета им. Н.Э. Баумана, г. Москва, Россия. E-mail: v.tsirlov@bmstu.ru*

Литература

1. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. №2. С. 2-15. DOI: 10.21681/2311-3456-2018-2-2-15
2. Госькова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. №2. С.42-49. DOI:10.21681/2311-3456-2019-2-42-49
3. Колосок И.Н., Гурина Л.А., Повышение кибербезопасности интеллектуальных энергетических систем методами оценивания состояния // Вопросы кибербезопасности. 2018. №3. С. 63-69. DOI:10.21681/2311-3456-2018-3-63-69
4. Васильева В.И., Кириллова А.Д., Кухарев С.Н. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4. С. 66-74.
5. Северцев Н.А. Системный анализ и моделирование безопасности. М.: Высшая школа, 2018. 462 с.
6. Пугачев В.С., Синицын И.Н. Теория стохастических систем. М.: Логос, 2000. 1000 с.
7. Викторова В. С., Степанянц. А.С. Модели и методы расчета надежности технических систем. М.: Ленанд, 2014. 256 с.
8. Острейковский В.А. Теория надежности. М.: Высшая школа, 2004. 462 с.
9. Данилюк С.Г., Мурашко А.А. Применение вероятностно-лингвистического подхода при решении задач оценивания уязвимости систем обеспечения безопасности эксплуатации важных технических объектов // Известия Института инженерной физики, 2016 № 2. С. 5-10.
10. Гурина Л.А., Зеркальцев В.И., Колосок И.Н., Коркина И.С., Мокрый И.В. Оценивание состояния электроэнергетической системы: алгоритмы и примеры линеаризованных задач. Иркутск: ИСЭМ СО РАН, 2016. 37 с.
11. Лифшиц И.И., Фаткиева Р.Р. Модель интегрированной системы менеджмента для обеспечения безопасности сложных объектов // Вопросы кибербезопасности. 2018. №1. С. 64-71. DOI:10.21681/2311-3456-2018-1-64-71
12. Число DDoS – атак в 2018 году снизилось, но они стали сложнее [Электронный ресурс] https://www.itweek.ru/security/news-company/detail. php?ID=205254 (дата обращения к ресурсу: 14.03.2019 г.).
13. Братченко А.И., Бутусов И.В., Кобелян А.М., Романов А.А. Применение метода нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления // Вопросы кибербезопасности. 2019. №1. С. 18-24. DOI:10.21681/2311-3456-2019-1-18-24
14. Андрюхин Е.В., Ридли М.К., Правиков Д.И., Прогнозирование сбоев и отказов в распределенных системах управления на основе моделей прогнозирования временных рядов // Вопросы кибербезопасности. 2019. №3. С. 24-32. DOI:10.21681/2311-3456-2019-3-24-32

15. Пяткова Н.И., Береснева Н.М. Моделирование критических инфраструктур энергетики с учетом требований энергетической безопасности. // Информационные и математические технологии в науке и управлении. 2017. № 3. С 54-65.
16. Тихонов В.И., Миронов М.А. Марковские процессы. – М.: Советское радио, 1977. 488с.
17. Кочнев С.В., Лапсарь А.П. Синтез измерительно-управляющих систем для потенциально опасных сложных технических объектов на базе параметризованных марковских моделей // Проблемы безопасности и чрезвычайных ситуаций. 2014. №5. С. 77-85.
18. Канторович Л.В., Акилов Г.П. Функциональный анализ. – М.: СПб: BHV, 2017. 816 с.
19. Танана В.П. Методы решения операторных уравнений. – М.: Наука, 2015. 160 с.
20. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М. Численные методы. – М.: Бином, 2011. 640 с.
21. Самарский А.А., Гулин А.В. Численные методы математической физики. – М.: Альянс, 2016. 432 с.
22. Гришко А.К., Лысенко А.В., Моисеев С.А. Прогнозирование и оптимизация управления процессов проектирования сложных систем в масштабах реального времени // Надежность и качество сложных систем. 2018. №1. С. 40-45.
23. Кудинов Ю.И, Келина А.Ю, Кудинов И.Ю., Пащенко А.Ф. Нечеткие модели и системы управления. М.: Ленард, 2017. 237 с.

INCREASE THE SECURITY OF IMPORTANT CRITICAL INFRASTRUCTURE USING PARAMETRIC MODELS OF EVOLUTION

Kubarev A. V. [5]***, Lapsar A. P.*** [6]***, Fedorova Ya.V.*** [7]

The purpose *of the article is to develop a method to improve the security of important objects of critical information infrastructure in the conditions of non-standard mode of their operation caused by destructive information impact.*

Methods: *analysis of available methods and mathematical models for assessing the state of complex technical systems and the choice of optimal; synthesis of diffusion Markov model of the object under study in parametric form.*

The result: *the basis of the well-known apparatus of diffusion Markov processes, the paper proposes an original method of rapid assessment of the state of important objects of critical information infrastructure in the process of their functioning to improve the safety of their operation. Increasing the efficiency of evaluation is achieved by dividing the evaluation process into two periods, with the most time-consuming and time-consuming process of obtaining basic solutions of evolutionary equations modeling the behavior of the object under study, carried out in advance. Calculation of stochastic characteristics of the object of critical information infrastructure, characterizing its technical condition, is carried out directly upon detection of destructive impact on the basis of previously obtained basic solutions. The resulting assessment of the technical condition allows you to plan measures to improve the safety of the object.*

The paper considers the process of synthesis of evolutionary equations describing the behavior of the object of study in parameterized form, obtaining their basic solutions, as well as the algorithm for the implementation of the proposed method. The results of the study can be used in the development of technical specifications (private technical specifications) for the modernization of security systems of critical information infrastructure.

Keywords: *complex technical object, destructive influence, non-standard operation mode, safety, Markov models, evolutionary equations, basic solutions, condition assessment, score state, speed of assessment.*

References

1. Zegzhda D.P., Vasil`ev Yu.S., Poltavceva M.A., Kefeli I.F., Borovkov A.I. Kiberbezopasnost` progressivny`x proizvodstvenny`x texnologij v e`poxu cifrovoj transformacii // Voprosy` kiberbezopasnosti. 2018. №2. S. 2-15. DOI:10.21681/2311-3456-2018-2-2-15
2. Gos`kova D.A., Massel` A.G. Texnologiya analiza kiberugroz i ocenka riskov kiberbezopasnosti kriticheskoj infrastruktury` // Voprosy` kiberbezopasnosti. 2019. №2. S. 42-49. DOI:10.21681/2311-3456-2019-2-42-49
3. Kolosok I.N., Gurina L.A., Povy`shenie kiberbezopasnosti intellektual`ny`x e`nergeticheskix sistem metodami ocenivaniya sostoyaniya // Voprosy` kiberbezopasnosti. 2018. №3. S. 63-69. DOI:10.21681/2311-3456-2018-3-63-69

5 Alexey V. Kubarev, lecturer of the Educational center «Echelon», Moscow, Russia. E-mail: kubarev@gmail.com

6 Alexey P. Lapsar, Ph.D., associate Professor, Deputy head of the Department of FSTEC of Russia in the southern and North Caucasus Federal districts, Rostov-on-Don, Russia. E-mail: lapsar1958@mail.ru

7 Yana V. Fedorova, the associate Professor of the Department «Information technologies and information protection» Department AT Rostov state economic University (RINH), Rostov-on-Don, Russia. E-mail: fyv21@mail.ru

4. Vasil`eva V.I., Kirillova A.D., Kuxarev S.N. Kiberbezopasnost` avtomatizirovanny`x sistem upravleniya promy`shlenny`x ob``ektov (sovremennoe sostoyanie, tendencii) // Vestnik UrFO. Bezopasnost` v informacionnoj sfere. 2018. № 4. S. 66-74.
5. Severcev N.A. Sistemny`j analiz i modelirovanie bezopasnosti. M.: Vy`sshaya shkola, 2018. 462 s.
6. Pugachev V.S., Sinicyn I.N. Teoriya stoxasticheskix sistem. M.: Logos, 2000. 1000 s.
7. Viktorova V. S., Stepanyancz. A.S. Modeli i metody` rascheta nadezhnosti texnicheskix sistem. M.: Lenand, 2014. 256 c.
8. Ostrejkovskij V.A. Teoriya nadezhnosti. M.: Vy`sshaya shkola, 2004. 462 s.
9. Danilyuk S.G., Murashko A.A. Primenenie veroyatnostno-lingvisticheskogo podxoda pri reshenii zadach ocenivaniya uyazvimosti sistem obespecheniya bezopasnosti e`kspluatacii vazhny`x texnicheskix ob``ektov // Izvestiya Instituta inzhenernoj fiziki, 2016 № 2. S. 5-10.
10. Gurina L.A., Zerkal`cev V.I., Kolosok I.N., Korkina I.S., Mokry`j I.V. Ocenivanie sostoyaniya e`lektroe`nergeticheskoj sistemy`: algoritmy` i primery` linearizovanny`x zadach. Irkutsk: ISE`M SO RAN, 2016. 37 s.
11. Lifshicz I.I., Fatkieva R.R. Model` integrirovannoj sistemy` menedzhmenta dlya obespecheniya bezopasnosti slozhny`x ob``ektov // Voprosy` kiberbezopasnosti. 2018. №1. S. 64-71. DOI:10.21681/2311-3456-2018-1-64-71
12. Chislo DDoS – atak v 2018 godu snizilos`, no oni stali slozhnee [E`lektronny`j resurs] https://www.itweek.ru/security/news-company/detail. php?ID=205254 (data obrashheniya k resursu: 14.03.2019 g.).
13. Bratchenko A.I., Butusov I.V., Kobelyan A.M., Romanov A.A. Primenenie metoda nechetkix mnozhestv k ocenke riskov narusheniya kriticheski vazhny`x svojstv zashhishhaemy`x resursov avtomatizirovanny`x sistem upravleniya // Voprosy` kiberbezopasnosti. 2019. №1. S. 18-24. DOI:10.21681/2311-3456-2019-1-18-24
14. Andryuxin E.V. , Ridli M.K., Pravikov D.I., Prognozirovanie sboev i otkazov v raspredelenny`x sistemax upravleniya na osnove modelej prognozirovaniya vremenny`x ryadov // Voprosy` kiberbezopasnosti. 2019. №3. S. 24-32. DOI:10.21681/2311-3456-2019-3-24-32
15. Pyatkova N.I., Beresneva N.M. Modelirovanie kriticheskix infrastruktur e`nergetiki s uchetom trebovanij e`nergeticheskoj bezopasnosti. // Informacionny`e i matematicheskie texnologii v nauke i upravlenii. 2017. № 3. S 54-65.
16. Tixonov V.I., Mironov M.A. Markovskie processy`. M.: Sovetskoe radio, 1977. 488s.
17. Kochnev S.V., Lapsar` A.P. Sintez izmeritel`no-upravlyayushhix sistem dlya potencial`no opasny`x slozhny`x texnicheskix ob``ektov na baze parametrizovanny`x markovskix modelej // Problemy` bezopasnosti i chrezvy`chajny`x situacij. 2014. №5. S. 77-85.
18. Kantorovich L.V., Akilov G.P. Funkcional`ny`j analiz. M.: SPb: BHV, 2017. 816 s.
19. Tanana V.P. Metody` resheniya operatorny`x uravnenij. M.: Nauka, 2015. 160 s.
20. Baxvalov N.S., Zhidkov N.P., Kobel`kov G.M. Chislenny`e metody`. M.: Binom, 2011. 640 s.
21. Samarskij A.A., Gulin A.V. Chislenny`e metody` matematicheskoj fiziki. M.: Al`yans, 2016. 432 s.
22. Grishko A.K., Ly`senko A.V., Moiseev S.A. Prognozirovanie i optimizaciya upravleniya processov proektirovaniya slozhny`x sistem v masshtabax real`nogo vremeni // Nadezhnost` i kachestvo slozhny`x sistem. 2018. №1. S. 40-45.
23. Kudinov Yu.I, Kelina A.Yu, Kudinov I.Yu., Pashhenko A.F. Nechetkie modeli i sistemy` upravleniya. M.: Lenard, 2017. 237 s.