СИНТЕЗ МОДЕЛИ ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ДЛЯ БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ ТЕХНИЧЕСКОЙ СИСТЕМЫ В УСЛОВИЯХ ДЕСТРУКТИВНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ

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

Цель статьи: *повышение безопасности и устойчивости функционирования сложных технических систем, управляемых объектами критической информационной инфраструктуры в условиях деструктивного информационного воздействия, с использованием параметризованных эволюционных моделей.*

Методы: *синтез параметризованных эволюционных моделей значимых объектов критической информационной инфраструктуры на основе марковской теории оценивания многомерных диффузионных процессов.*

Полученный результат: *в рамках комплексного подхода к обеспечению безопасности сложных технических систем синтезирована параметризованная эволюционная модель объекта критической информационной инфраструктуры, функционирующего в условиях деструктивного информационного воздействия. Предложен подход к выработке рекомендаций по управлению сложной технической системой путем оперативной оценки основных характеристик функционирования объекта критической информационной инфраструктуры. Разработана последовательность выработки решений по эксплуатации сложной технической системы, основанная на оценке уровня воздействия и результатах оперативного вычисления основных характеристик функционирования объекта критической информационной инфраструктуры.*

Полученные результаты позволяют обоснованно сформировать технические требования к создаваемым или модернизируемым средствам обеспечения безопасности значимых объектов критической информационной инфраструктуры, осуществляющих управление сложными техническими системами.

Ключевые слова: *объект критической информационной инфраструктуры, уровень деструктивного воздействия, комплексный подход, набор функций безопасности, базовые решения, эволюционные модели, характеристики функционирования, векторный параметр.*

DOI: 10.681/2311-3456-2020-06-48-56

Введение

Развитая инфраструктура современного общества предполагает эксплуатацию значительного количества различного рода сложных технических систем (СТС), которые обеспечивают устойчивое функционирование государства, а также потребности общества и отдельного гражданина. В соответствии с Федеральным законом «О безопасности критической инфраструктуры Российской Федерации» к объектам критической информационной инфраструктуры (КИИ) Российской Федерации в том числе отнесены автоматизированные системы управления, обеспечивающие функционирование СТС, задействованных в сферах транспорта, связи, энергетики и в других сферах. Очевидно, что устойчивая работа указанных СТС служит залогом не только экономической стабильности, но и необходимого качества жизни общества.

Происходящий в настоящее время переход от индустриального общества к информационному наряду с несомненными преимуществами несет в себе и негативные факторы, обусловленные возможностью нанесения ущерба с использованием удаленного доступа к информационным и автоматизированным системам. Сейчас нет необходимости физически воздействовать на техническую систему с целью нарушения ее нормального функционирования. Гораздо проще, дешевле и безопаснее нарушить управление такой системой, что и осуществляется путем деструктивного информационного воздействия на объекты КИИ (далее – ОКИИ). Многочисленные примеры говорят об участившихся случаях компьютерных атак на ОКИИ, осуществляющих управление различными техническими системами обе-

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: lapsarap1958@mail.ru

3 Асютиков Александр Александрович, студент ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия. E-mail: alexander.asyutikov1306@gmail.com

спечения жизнедеятельности государства и общества[4]. Более того, в последнее время отмечается тенденция на повышение избирательности таких воздействий[5].

Среди всех возможных целей для компьютерных атак особое место занимают автоматизированные системы управления производственными и технологическими процессами, количество деструктивных информационных воздействий на них постоянно возрастает[6]. При этом опасность представляют не только компьютерные атаки со стороны злоумышленников, но и возможность дистанционного отключения или изменения режимов функционирования оборудования его поставщиками.

Именно поэтому вопросам защиты ОКИИ от деструктивного информационного воздействия уделяется большее внимание [1-7]. В научных изданиях рассматриваются отдельные аспекты обеспечения безопасности КИИ: организационные меры, вопросы учета событий, анализа количества воздействий и т.д. В рамках формализованного подхода применяются, как правило, методы экспертных оценок.

Нормативные правовые акты предусматривают применение для обеспечения безопасности ОКИИ сил и средств защиты от деструктивного воздействия. Состав средств обеспечения безопасности ОКИИ определяется исходя из их категории значимости. При этом определение необходимого состава и характеристик средств защиты от деструктивного воздействия требует применения формализованных подходов. Одна из важнейших составляющих систем обеспечения безопасности ОКИИ – это средства мониторинга безопасности, задача которых оценить состояние ОКИИ при деструктивном информационном воздействии, в том числе на некоторый последующий период времени, достаточный для нейтрализации воздействия и устранения его последствий. При исследовании проблемы обеспечения безопасности ОКИИ рассматривается не только способность противостоять компьютерным атакам, но и условия их функционирования, надежность, взаимодействие с внешней средой и смежными системами и другие [8-13].

Авторы предлагают комплексный подход к обеспечению работоспособности технических систем энергетики, топливно-энергетического комплекса, атомной энергии, оборонной, ракетно-космической, химической промышленности и других СТС, в рамках которого следует рассматривать безопасность ОКИИ с точки зрения выполнения объектом своих функций по оценке технического состояния названных систем и управлению ими. В данной работе под ОКИИ, обеспечивающими оценку состояния и управление названными выше СТС, понимаются автоматизированные системы управления. Поскольку качественная работа СТС зависит в основном от оптимальности принимаемых управленческих решений, то нормальное функционирование ОКИИ является необходимым условием эффективной эксплуатации технической системы. В связи с тем, что управление является важнейшим, но не единственным условием обеспечения функционирования СТС, безопасность ОКИИ необходимо рассматривать в широком смысле. То есть нормальное функционирование ОКИИ должно обеспечиваться не только его устойчивостью к деструктивным информационным воздействиям, но и общим техническим состоянием, определяемым показателями надежности и безотказности.

Неисправность ОКИИ может явиться следствием деструктивного информационного воздействия, старения и износа, реализации неоптимальных алгоритмов функционирования, других факторов. При этом следует учитывать, что неисправность ОКИИ как сложного объекта зачастую не приводит к потере его работоспособности, а только снижает качество функционирования [8,14,15]. Примером может служить формирование автоматизированной системой управления неоптимальных управляющих воздействий вследствие низкой точности измерения параметров функционирования при нештатной эксплуатации.

Очевидно, что снижение в допустимых пределах качества функционирования ОКИИ при деструктивном информационном воздействии позволяет продолжать нештатную эксплуатацию СТС в течение некоторого времени. Время нештатной эксплуатации используется для купирования деструктивного воздействия, устранения его последствий, задействования резервных систем или их составных частей, а также, при невозможности поддержания работоспособности СТС, для ее плановой остановки. Для оценки возможности и времени нештатной эксплуатации ОКИИ требуется смоделировать изменение его состояния с течением времени в условиях деструктивного информационного воздействия. Однако в настоящее время не существует достаточно адекватных моделей для решения этой задачи, несмотря на то, что проблемам безопасности КИИ уделяется все возрастающее внимание [3-7, 16-18].

Данная работа посвящена повышению безопасности СТС, функционирующей под управлением ОКИИ в условиях деструктивного воздействия с использованием комплексного подхода к синтезу параметризованной (зависящей от векторного вещественного параметра) модели объекта. Решение данной задачи предполагает анализ особенностей функционирования ОКИИ в различных условиях, разработку метода оперативной оценки интегральных характеристик функционирования объекта и выработку на этой основе рекомендаций по его дальнейшей эксплуатации. Для решения поставленной задачи следует обосновать требования к моделированию ОКИИ, а также разработать метод оценки основных показателей качества их функционирования.

4 90% российских компаний сталкивались с кибератаками, https://www.securitylab.ru/news/503725.php; Количество кибератак в России удвоилось, https://www.vedomosti.ru/technology/articles/2019/04/17/799417-kolichestvo-kiberatak

5 Киберпреступники бьют в цель, https://www.comnews.ru/information_security

6 Кибератаки на критически важные для РФ объекты участились в десятки раз, https://www.rbc.ru/ekb/13/02/2019/5c641f829a794756010d719d; Атаки на АСУ ТП, https://www.santi-malware.ru/threats/APCS-attack; Количество атак на АСУ продолжает расти: «Лаборатория Касперского», https://www.itbestsellers.ru/companies-analytics/detail.php?ID=40442; КИИ атаковали 4,3 млрд. раз за год, https://www.comnews.ru/content/116622/2018-12-12/kii-atakovali-43-mlrd-raz-za-god

Особенности функционирования объекта критической информационной инфраструктуры в условиях деструктивного воздействия и выбор модели оценки ее состояния

СТС, подвергающаяся деструктивному воздействию, должна сохранить работоспособность в течение некоторого времени, необходимого для компенсации (купирования) воздействия или для проведения его не аварийной остановки. Снижение качества выполнения СТС своих функций хотя и является негативным последствием нештатной эксплуатации, все же гораздо предпочтительней остановки объекта вследствие отказа. Объект КИИ, функционирующий в условиях деструктивного воздействия имеет особенности, связанные с решением комплексной задачи: с одной стороны требуется обеспечить максимально возможное время поддержания работоспособного состояния СТС, а с другой – не допустить прекращения ее функционирования вследствие аварии.

К основным особенностям функционирования ОКИИ в условиях деструктивного воздействия следует отнести:

1. Искажение исходной информации для принятия управленческих решений. Отдельные параметры функционирования СТС могут выходить за границы области допустимых значений, что приводит к неопределенности их оценки из-за ограниченности полосы пропускания используемых средств измерений и необходимости проведения контроля в быстроменяющихся условиях. Внешние и внутренние помехи, обусловленные деструктивным воздействием, приводят к существенному снижению точности из-за роста стохастической погрешности, а также появления ее систематической составляющей.

2. Возрастание ответственности за принятие управленческих решений. Неоптимальные или неправильные решения могут усугубить последствия деструктивного воздействия, привести к аварии или катастрофе.

3. Существенное повышение фактора времени. Несвоевременное принятие и реализация даже оптимальных управленческих решений приводят к углублению компьютерных инцидентов и развитию аварийной ситуации. Дефицит времени в условиях развития компьютерного инцидента приводит к снижению достоверности оценки состояния объекта и отличного от оптимального решения по выработке управляющих воздействий

4. Необходимость оценки последствий принятых решений с целью исключения развития нештатной ситуации предполагает оценку состояния объекта не только в текущем времени, но и его прогнозирование на некоторый период.

Названные выше особенности предъявляют дополнительные требования к формальному описанию (моделированию) состояния подвергшегося деструктивному воздействию ОКИИ, реализующего управление СТС.

Модель, используемая для решения задачи оценки состояния ОКИИ в условиях деструктивного воздействия, должна отвечать следующим основным требованиям:

1. Применение перспективного математического аппарата. Удобство формального описания параметров исследуемого процесса, минимизация ограничений при моделировании. Использование статистической информации, предварительного создания баз данных, простота использования вычислительной техники.

2. Процессы измерений, вычислений, обработки результатов при решении задач оценки состояния ОКИИ должны быть максимально удобны для выполнения их оператором, даже не имеющим специальных навыков, результаты должны быть обоснованы и не допускать неоднозначной трактовки.

3. Высокая оперативность, возможность получать результат в масштабе времени, близком к реальному, а также приемлемая точность и достоверность получения результата оценки состояния.

4. Универсальность синтезируемой модели, ее применение на однотипных ОКИИ не должно требовать существенных изменений и доработок. Модель призвана обеспечить как оценку состояния в заданный момент времени (прямая задача), так и оценку времени, по прошествии которого будет обеспечен заданный уровень качества объекта (обратная задача); оценка состояния должна осуществляться не только в вероятностном, но и в аналитическом виде.

5. Возможность получения достаточно надежной оценки состояния объекта в условиях неопределенности, ограниченности данных об исследуемом параметре, наличии случайных выбросов результатов измерений и различного рода возмущений.

6. Возможность корректировки модели и полученных результатов при поступлении дополнительной информации об исследуемом ОКИИ. Возможность использования дополнительных критериев для оценки объективности выбора параметров модели.

Синтез модели изменения состояния ОКИИ, обеспечивающего управление СТС, и использование результатов моделирования для организации квазиоптимального управления системой по аналогии с [8] предполагает выполнение следующих операций:

- оценку многомерной области Ω возможных значений параметров $\omega \in \Omega$, к которым могут относиться свойства внешнего деструктивного воздействия, а также параметры внешней среды, начальные и граничные условия исследуемых процессов и другие;
- получение параметризованных значений коэффициентов сноса и диффузии эволюционных уравнений, моделирующих исследуемый процесс изменения состояния ОКИИ, уточнение их по мере накопления статистической информации об исследуемом процессе для всех $\omega \in \Omega$;
- вычисление параметризованных характеристик законов распределения исследуемых процессов и их корректировку в процессе эксплуатации;
- формирование параметризованных эволюционных уравнений и их решение с заданной точностью для всех $\omega \in \Omega$;
- получение, хранение и использование базовых решений эволюционных уравнений, моделирующих исследуемый процесс измене-

ния состояния ОКИИ, в параметризованном виде;
- параметрическую оценку поведения исследуемого процесса на некоторое время, обусловленное вероятностью нахождения ОКИИ в работоспособном состоянии;
- оценку времени $T(x, \omega)$ нахождения ОКИИ в работоспособном состоянии с заданной вероятностью;
- выдачу результатов контроля и оценки состояния ОКИИ на некоторый период времени не только в виде аналитических выражений и характеристик, но и конкретных рекомендаций оператору, принимающему решение;
- высокую оперативность функционирования и получения результата оценки состояния, а также выработки управляющих воздействий в условиях нештатной ситуации, вызванной деструктивным воздействием;
- формирование квазиоптимального управления СТС на основе заданных критериев.

Наиболее полно предъявляемым требованиям удовлетворяют модели на основе эволюционных марковских процессов [14,15]. Они позволяют учитывать физическую сущность исследуемых процессов, начальные и граничные условия, параметры внешней среды и другие свойства ОКИИ, быстро и однозначно реагировать на их изменение, что обеспечивает адекватность модели исследуемому процессу. Поскольку в условиях деструктивного воздействия основным показателем качества ОКИИ является ее быстродействие, в работе [8] была предложена модель изменения его состояния в зависимости от векторного параметра ω, характеризующего свойства внешнего деструктивного информационного воздействия.

Обоснование объема функций безопасности, реализуемых объектом критической информационной инфраструктуры в условиях деструктивного воздействия

В нормальных условиях эксплуатации ОКИИ обеспечивает реализацию некоторого набора полезных функций $N(x, \omega, t)$ по управлению, который определяет качество и (экономические) показатели эффективности функционирования СТС в отсутствии деструктивного информационного воздействия $\omega=0$.

При этом ОКИИ реализует некоторый набор функций безопасности $B(x, \omega, t)$, требующий определенного объема расходования его ресурсов. Одним из показателей качества (эффективности) функционирования ОКИИ можно считать долю его ресурса, используемого на реализацию полезных (основных) функций предназначения $R|_{N(x,\omega,t)} - R|_{B(x,\omega,t)} = R|_{M(x,\omega,t)} \to \max$. В нормальных условиях при $\omega = 0$ это условие обеспечивается соотношением $B(x, \omega, t) = \min$, которое реализуется средствами, выполняющими минимально необходимый набор функций безопасности, например – только защиту от несанкционированного доступа.

В условиях деструктивного воздействия набор функций безопасности существенно расширяется за счет необходимости купирования возникающих угроз, следовательно, возрастает доля ресурса ОКИИ, расходуемого на реализацию функций безопасности $R|_{B(x,\omega,t)}$, соответственно уменьшается доля «полезного» ресурса $R|_{M(x,\omega,t)}$. При достижении некоторой минимально допустимой величины $R|_{M(x,\omega,t)} \geq R_{\text{доп}}|_{M(x,\omega,t)}$ продолжение эксплуатации ОКИИ становится нецелесообразным, требуется прекратить его эксплуатацию (произвести аварийную остановку) СТС.

По аналогии с [8] считаем, что ОКИИ является сложным объектом, поэтому деструктивное воздействие не сразу приводит к нарушению работоспособности, а только ухудшает характеристики (качество) его функционирования. В этом случае значение $R_{\text{доп}}|_{M(x,\omega,t)}$ может быть рассчитано на основе классического показателя «эффективность-стоимость» или получено методами экспертной оценки. Поскольку ОКИИ является техническим объектом, в качестве основы для определения $R_{\text{доп}}|_{M(x,\omega,t)}$ можно использовать вероятность сохранения его работоспособности в условиях деструктивного воздействия $P(x,\omega,t)$ в течение времени до наступления необратимых изменений в ОКИИ $T(x,\omega)$, приводящих к аварии СТС. При этом должны учитываться параметры деструктивного воздействия, уровень которых не должен превышать априори заданного допустимого значения $R_{\text{доп}}|_{M(x,\omega,t)} = F[P(x,\omega,t), T(x,\omega)] \ \forall \ \omega(t) < \omega_{\text{зад}}(t)$.

Для вычисления (оценки) названных выше характеристик функционирования ОКИИ воспользуемся эволюционной моделью, обоснование которой применительно к ОКИИ приведено в работе [8]. Рассмотрим функционирование ОКИИ в различных условиях с использованием названной модели, для чего разделим процесс его функционирования на два этапа: этап нормальной эксплуатации и этап нештатной эксплуатации, обусловленной деструктивным информационным воздействием.

Функционирование объекта критической информационной инфраструктуры на этапе нормальной эксплуатации

Изменение технического состояния объекта исследования по аналогии с широко распространенными моделями регрессии представим в виде стохастического дифференциального уравнения $\frac{dx(t)}{dt} = f(x,t) + g(x,t)n(t)$, где $f(x,t) \in R^r$, $g(x,t) \in R^r \times R^r$ – детерминированные гладкие неразрывные функции, $n(t) \in R^r$ – белый (гауссовский) шум с известными статистическими характеристиками [8,15]. Вид функций устанавливается на основе обработки измерительной информации.

Нештатные условия функционирования СТС приводят к однозначной зависимости состояния объекта исследования от параметров $\omega \in \Omega \subset R^m$. Значения параметров ω обусловлены начальными и граничными условиями, внешней средой, режимами функционирования объекта, различными воздействиями и другими.

Для решения задачи оценки состояния ОКИИ в условиях деструктивного информационного воздействия параметры ω характеризуют свойства этого воздействия: вид и структуру компьютерной атаки, ее интенсивность, время воздействия, а также значимость атакуемого ОКИИ и управляемых им систем и процессов. От названных параметров зависят значения коэффициентов сноса и диффузии исследуемого процесса, а также другие составляющие эволюционных уравнений. Выбор и оценка свойств деструктивного информационного воздействия производится специально предназначенным для этого устройством и используется для синтеза параметризованной модели ОКИИ.

Неисправностью ОКИИ считается дрейф даже одного параметра $x_i(\omega,t)$ за границу допустимой области $G_{\ddot{A},i} \subset R^1$ [13-15]. При этом работоспособность ОКИИ сохраняется, однако снижаются показатели качества (эффективности) ее функционирования. Безотказной работой при такой постановке считается вероятность того, что на интервале $t \in [s,T]$ ОКИИ не допустит выхода ни одного из параметров функционирования СТС за границы области допустимых значений, если до начала деструктивного воздействия все они находились внутри этой области $x(\omega,s) \in G_{\ddot{A}} : P(x,\omega,s) \equiv P\{x(\omega,t) \in G_{\ddot{A}}\}^r$.

Считаем, что на отрезке времени, в течение которого осуществляется деструктивное воздействие, состояние СТС полностью определяется свойствами ОКИИ: надежностью, безотказностью и быстродействием (оперативностью реагирования на инциденты).

В случае исследования отдельно взятого параметра функционирования вероятность безотказной работой ОКИИ подчиняется следующему соотношению

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

$$P(x_0,\omega,t_0) = 1,$$

а уравнение Фоккера-Планка-Колмогорова для плотности вероятности безотказной работой примет следующий вид [8,15]:

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

$$p(x,\omega,t_0) = p_0(x,\omega).$$

Соотношение (2) представляет собой параметризованную эволюционную модель функционирования ОКИИ, которая формируется в соответствующем блоке (блок 3) приведенной на рисунке схемы.

Решение уравнения (2) может быть представлено в виде

$$p(x,\omega,t) = \sum_{i=1}^{\infty} c_i(\omega)\gamma_i(x,t), \quad (3)$$

где $\{\gamma_k(x,t)\}$ – заданный базис.

В работе [8] показано, что решение уравнения (2) зависит от вида интерполирующей функции, используемой для определения коэффициентов $c_i(\omega)$. Вычисление базовых решений $p_n(x,\omega,t)$ производится заранее в узлах сетки, формируемой путем разбиения области определения параметра Ω на подобласти, в которых его значение квазипостоянно.

Решение (2) при использовании в качестве интерполирующей функции полинома Лагранжа $L_k(\omega) = \prod_{\substack{p=0 \\ p \neq k}}^{N} \frac{\omega - \omega_{(p)}}{\omega_{(k)} - \omega_{(p)}}$ выглядит следующим образом:

$$p_n(x,\omega,t) = \sum_{i=1}^{n}\sum_{k=1}^{N} c_{ni}(\omega_{(k)})L_k(\omega)\gamma_i(x,t), \quad (4)$$

При использовании классического степенного полинома решение (2) с учетом (3) будет таким:

$$p_n(x,\omega,t) = \sum_{i=1}^{n}\sum_{k=1}^{N} v_{ik}\omega^k\gamma_i(x,t), \quad (5)$$

Другие интерполирующие функции для получения базовых решений применять нецелесообразно вследствие их громоздкости, возрастания вычислительных сложностей, снижения точности приближенных вычислений из-за роста ошибки интерполяции.

Вычисленные базовые решения в нормальных условиях эксплуатации при отсутствии деструктивного воздействия хранятся в памяти управляющей системы объекта и корректируются по мере накопления статистической информации о самом ОКИИ и возможных характеристиках деструктивного воздействия, имевших место на других аналогичных объектах.

Этап нормальной эксплуатации может продолжаться сколь угодно долго до момента обнаружения деструктивного воздействия. Отметим, что после прекращения деструктивного воздействия и ликвидации его последствий нормальная эксплуатация восстанавливается и данный этап продолжается.

Функционирование объекта критической информационной инфраструктуры на этапе нештатной эксплуатации

Этап нештатного режима эксплуатации связан с началом деструктивного информационного воздействия на ОКИИ. Информация о деструктивном воздействии может быть получена от специально созданной для этого системы в составе ОКИИ или от системы высшего уровня.

Блок выявления признака деструктивного воздействия на ОКИИ, получив оценку его параметров, передает эти сведения для оперативной оценки характеристик функционирования объекта на основе имеющихся базовых решений. Базовые параметризованные решения эволюционного уравнения, хранящиеся в памяти ЭВМ, применяются для задачи оценки состояния ОКИИ с целью оперативного получения результата в условиях деструктивного воздействия.

Плотность распределения стохастического процесса является наиболее его информативным свойством [15], поэтому оценка (вычисление) основных характеристик ОКИИ производится сразу в аналитическом виде с использованием соотношений (4) или (5).

Как было указано ранее, для оценки возможности продолжения эксплуатации ОКИИ в условиях деструк-

тивного воздействия целесообразно использовать его параметрическую надежность в заданных точках интервала оценки состояния (в том числе и на некоторый последующий интервал времени), а также время достижения границ допустимой области отдельными составляющими вектора состояния объекта. Кроме того, вычисленные значения плотности вероятности эволюционного процесса, моделирующего поведение ОКИИ, позволяют назначить оптимальные допуски и ограничения на параметры его функционирования в условиях развития аварийной ситуации, вызванной деструктивным воздействием.

Если параметризованное решение эволюционного уравнения (2) представляет собой плотность вероятности непрерывного параметра $x(\omega,t)$, а параметр $x(\omega,t)$ характеризует техническое состояние ОКИИ, то на интервале $[g_{\min}, g_{\max}]$ функция распределения параметра равна $F(x,\omega,t)=\int_{g_{\min}}^{x} p(x,\omega,t)dx$, $x\in[g_{\min}, g_{\max}]$,

где $g_{\min}$ и $g_{\max}$ — нижняя и верхняя границы области допустимых значений параметра соответственно. Возможность выполнения ОКИИ своих функций по предназначению в каждый момент времени t определяется вероятностью нахождения его в работоспособном состоянии:

$$P(\omega,t)=\int_{g_{\min}}^{g_{\max}} p(x,\omega,t)dx. \quad (6)$$

Данная вероятность вычисляется при начальном условии $P(x,\omega,t_0)=1$ и границах области допустимых значений в виде поглощающих экранов [14]. Конкретное численное минимальное значение вероятности $P_{\min}(\omega,t)$, при котором продолжение эксплуатации ОКИИ нецелесообразно, определяется либо экспертными методами, либо рассчитывается на основе моделей регрессии.

Если известна $f(x,\omega,t)$ — плотность вероятности времени достижения границы допустимой области $G_{\text{Д}}$, то появляется возможность определить моменты времени выхода процесса $x(\omega,t)$ на границы этой области

$$T_n(\omega)=\int_{0}^{\infty} t^n f(x,\omega,t)dt,\ n=1,2,... \quad (7)$$

Если уже найдено значение вероятности нахождения ОКИИ в работоспособном состоянии $P(\omega,t)$, то среднее время $T(\omega)$ достижения исследуемым параметром границ допустимой области можно определить путем численного решения уравнения

$$T(\omega)=\int_{0}^{\infty}\int_{g_{\min}}^{g_{\max}} p(x,\omega,t)dxdt. \quad (8)$$

Названные выше характеристики являются функциями не только от времени, но и от параметра ω, который характеризует свойства деструктивного воздействия. При условии нахождения параметра ω в пределах области Ω значения характеристик технического состояния ОКИИ будут находиться внутри «трубки», ограниченной максимальным значением вероятности для оптимистической оценки и минимальным – для пессимистической или гарантированной оценки.

Таким образом, на основе полученного с помощью разработанного метода параметризованного решения эволюционных уравнений, моделирующих поведение ОКИИ в различных условиях, можно отыскать в аналитическом виде значения основных характеристик исследуемого объекта. Важнейшим преимуществом предлагаемого подхода к оценке характеристик ОКИИ в нештатных условиях является его оперативность, которая обеспечивается использованием заранее полученных базовых решений эволюционных уравнений, моделирующих изменение состояния исследуемого объекта.

Полученные результаты позволяют синтезировать алгоритм (последовательность) функционирования ОКИИ в зависимости от уровня деструктивного информационного воздействия, обеспечивающий безопасность и минимизацию возможного ущерба.

Последовательность функционирования объекта критической информационной инфраструктуры в условиях деструктивного информационного воздействия

Для синтеза алгоритма функционирования ОКИИ в нештатных условиях, предварительно разобьем уровень (набор свойств) деструктивного информационного воздействия на три условных части. Здесь под уровнем следует понимать мощность (интенсивность) компьютерной атаки, а также другие характеристики воздействия, например его сложность.

А. Высокий уровень воздействия.

Уровень деструктивного воздействия, поступившего на вход ОКИИ, превышает допустимый

В этой ситуации ОКИИ отключается от сетей общего пользования, его функционирование приостанавливается, происходит принудительная остановка СТС. Далее проводятся работы по ликвидации последствий воздействия и восстановлению показателей функционирования ОКИИ.

Б. Низкий уровень воздействия.

Уровень деструктивного воздействия, поступившего на вход ОКИИ, менее заданного предельно допустимого $\omega(t)<\omega_{\text{çàä}}(t)$. Эксплуатация СТС под управлением ОКИИ продолжается, усиливается наблюдение за свойствами, воздействием и проводятся отдельные мероприятия по его купированию. В реальном масштабе времени проводится оценка основных характеристик ОКИИ для определения эффективности принимаемых мер.

В. Средний уровень воздействия.

Уровень деструктивного воздействия, поступившего на вход ОКИИ, находится в интервале $[\omega_{\text{äîï}}(t),\omega_{\text{çàä}}(t)]$, что позволяет, не прекращая функционирования ОКИИ, оценить возможность продолжения эксплуатации объекта в нештатных условиях, выработать меры по устранению деструктивного воздействия, а также оценить интервал времени, в течение которого возможна реализация выработанных рекомендаций по нейтрализации деструктивного воздействия.

На следующем шаге алгоритма (последовательности) с использованием базовых решений эволюционных уравнений вида (4) или (5) и оценки параметров воздействия $\omega(t) \in \Omega(t)$ определяются основные характеристики ОКИИ – вероятность нахождения его в работоспособном состоянии в соответствии с (6) и время нахождения исследуемых параметров в границах допустимой области в соответствии с (7) или (8).

Далее оценивается доля полезного ресурса $R|_{M(x,\omega,t)}$, используемого объектом для осуществления своих функций по предназначению. Условие $R|_{M(x,\omega,t)} \le R_{\text{äîï}}|_{M(x,\omega,t)}$ является обязательным для проведения мероприятия по восстановлению нормальной эксплуатации ОКИИ. При этом продолжается непрерывная оценка вероятности нахождения объекта в работоспособном состоянии и времени нахождения исследуемых параметров в границах допустимой области. На базе результатов текущих измерений $X(\omega,t)$ и полученных решений уравнений (6) – (8) формируется управляющее воздействие $U(x,\omega,t)$ для восстановления штатного режима эксплуатации ОКИИ, либо для минимизации ущерба от деструктивного воздействия.

Предложенный подход к оцениванию характеристик функционирования ОКИИ может быть положен в основу синтеза систем обеспечения безопасности объекта от деструктивного воздействия, функционирующих в масштабе времени, близкому к реальному.

Заключение

В настоящей работе обеспечение безопасности СТС, функционирующих под управлением ОКИИ, предложено реализовывать в рамках комплексного подхода, основанного на оперативной оценке состояния объекта после деструктивного информационного воздействия. В качестве важнейших показателей технического состояния ОКИИ выбраны основные параметры его функционирования: вероятность безотказной работы и время, в течение которого объект будет сохранять свою работоспособность. Оценка названных показателей производится на основе базовых параметризованных решений уравнений эволюции, моделирующих изменение состояния ОКИИ в условиях деструктивного воздействия. Параметризованная эволюционная модель, использование которой при решении задачи обеспечения безопасного функционирования объекта проиллюстрировано структурной схемой, положена в основу синтеза перспективных ОКИИ.

В ходе исследования выявлены особенности функционирования ОКИИ, реализующих управление СТС в условиях деструктивного информационного воздействия. Рассмотрены и обоснованы основные требования к возможным моделям ОКИИ, сформулированы основные задачи, решаемые объектами при реализации функций управления техническими системами. Предложена последовательность выработки рекомендаций по управлению СТС на основе оперативной оценки основных характеристик функционирования управляющего ОКИИ. Разработанная последовательность выработки решений на дальнейшую эксплуатацию СТС учитывает уровень деструктивного воздействия на ОКИИ.

Полученные в работе результаты позволяют обоснованно сформулировать технические требования к создаваемым или модернизируемым значимым ОКИИ, осуществляющим управление СТС. Предложенный подход к комплексной оценке безопасности функционирования ОКИИ в условиях угрозы деструктивного информационного воздействия может быть использован при проектировании систем обеспечения безопасности значимых объектов критической информационной инфраструктуры, осуществляющих управление СТС.

Литература

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. Кубарев А.В., Лапсарь А.П., Федорова Я.В. Повышение безопасности эксплуатации значимых объектов критической инфраструктуры с использованием параметрических моделей эволюции // Вопросы кибербезопасности. 2020. № 1. С. 8-17. DOI: 10.21681/2311-3456-2020-01-08-17.

9. Климов С.М., Астрахов А.В., Сычев М.П. Методические основы противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 2013. 110 с.
10. Антонов С.Г., Климов С.М. Методика оценки рисков нарушения устойчивости функционирования программно-аппаратных комплексов в условиях информационно-технических воздействий // Надежность. 2017. Том 17. № 1. С. 32-39.
11. Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организации противодействия / О.О. Андреев и др. Под ред. В.А. Васенина. – М.:МЦНМО, 2008. 398 с.
12. Минаев В.А., Королев И.Д., Зеленцова Е.В., Захарченко Р.И. Критическая информационная инфраструктура: оценка устойчивости функционирования // Радиопромышленность. 2018. Том № 28, № 4. С. 59–67.
13. Северцев Н.А., Бецков А.В. Системный анализ теории безопасности. – М.: Изд. МГУ «ТЕИС», 2009. 452 с.
14. Острейковский В.А., Сальников Н.Л. Вероятностное прогнозирование работоспособности ЯЭУ. – М.: Энергоатомиздат, 1990. 416 с.
15. Пугачев В.С., Синицын И.Н. Теория стохастических систем. – М.: Логос, 2000. 1000 с.
16. 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.
17. Астрахов А.В., Куликов Л.С., Минаев В.А. Моделирование угроз информационных воздействий манипулятивного характера // Вопросы радиоэлектроники. 2016. № 12. С. 63-69
18. Захарченко Р.И., Королев И.Д. Модель функционирования автоматизированной информационной системы в киберпространстве // Вопросы кибербезопасности. 2019. № 6. С. 69-78.

THE SYNTHESIS OF A CRITICAL INFRASTRUCTURE OBJECT MODEL FOR SAFE OPERATION OF A TECHNICAL SYSTEM UNDER THE CONDITIONS OF DESTRUCTIVE INFORMATION IMPACT

Kubarev A.[7], Lapsar' A.[8], Asyutikov A.[9]

The purpose *of the article: improving the security and stability of the functioning of complex technical systems managed by critical information infrastructure objects under the conditions of a destructive information impact, using parameterized evolutionary models.*

Methods: *synthesis of parametrized evolutionary models of significant objects of critical information infrastructure based on the Markov theory of estimation of multidimensional diffusion processes.*

The result*: within the framework of an integrated approach to ensuring the security of complex technical systems, a parametrized evolutionary model of an object of a critical information infrastructure operating under conditions of destructive information impact has been synthesized. An approach to the development of recommendations for managing a complex technical system by means of an operational assessment of the main characteristics of the functioning of a critical information infrastructure object is proposed. A sequence has been developed for developing solutions for the operation of a complex technical system, based on an assessment of the impact level and the results of an operational calculation of the main characteristics of the functioning of a critical information infrastructure object.*

The results obtained make it possible to reasonably formulate technical requirements for the created or modernized means of ensuring the security of significant objects of critical information infrastructure that manage complex technical systems.

Keywords: *critical information infrastructure object, level of destructive impact, integrated approach, set of security functions, basic solutions, evolutionary models, functioning characteristics, vector parameter.*

7 Aleksey Kubarev, lecturer at ANO DPO (autonomous non-profit organization of additional professional education) «Uchebnyy tsentr «Eshelon», Moscow, Russia. E-mail: mr.kubarev@gmail.com

8 Aleksey Lapsar', Ph. D., Associate Professor, Deputy Head of the Department of the FSTEK of Russia (Federal service for technical and export control) for the Southern and North Caucasian Federal Districts, Rostov-on-Don, Russia. E-mail: lapsarap1958@mail.ru

9 Alexander Asyutikov, student of the FGAOU VO (federal state autonomous educational institution of higher education) «National Research Nuclear University «MEPhI», Moscow, Russia. E- mail: alexander.asyutikov1306@gmail.com

References

1. Vasil'eva V.I., Kirillova A.D., Kuharev S.N. Kiberbezopasnost' avtomatizirovannyh sistem upravleniya promyshlennyh ob»ektov (sovremennoe sostoyanie, tendencii) // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2018. № 4. S. 66-74.
2. Zegzhda D.P., Vasil'ev YU.S., Poltavceva M.A., Kefeli I.F., Borovkov A.I. Kiberbezopasnost' progressivnyh proizvodstvennyh tekhnologij v epohu cifrovoj transformacii // Voprosy kiberbezopasnosti. 2018. № 2. S. 2-15. DOI: 10.21681/2311-3456-2018-2-2-15.
3. Lifshic I.I., Fatkieva R.R. Model' integrirovannoj sistemy menedzhmenta dlya obespecheniya bezopasnosti slozhnyh ob»ektov // Voprosy kiberbezopasnosti. 2018. № 1. S. 64-71. DOI: 10.21681/2311-3456-2018-1-64-71.
4. Gos'kova D.A., Massel' A.G. Tekhnologiya analiza kiberugroz i ocenka riskov kiberbezopasnosti kriticheskoj infrastruktury // Voprosy kiberbezopasnosti. 2019. № 2. S. 42-49. DOI: 10.21681/2311-3456-2019-2-42-49.
5. Kolosok I.N., Gurina L.A., Povyshenie kiberbezopasnosti intellektual'nyh energeticheskih sistem metodami ocenivaniya sostoyaniya // Voprosy kiberbezopasnosti. 2018. № 3. S. 63-69. DOI: 10.21681/2311-3456-2018-3-63-69.
6. Bratchenko A.I., Butusov I.V., Kobelyan A.M., Romanov A.A. Primenenie metoda nechetkih mnozhestv k ocenke riskov narusheniya kriticheski vazhnyh svojstv zashchishchaemyh resursov avtomatizirovannyh sistem upravleniya // Voprosy kiberbezopasnosti. 2019. № 1. S. 18-24. DOI: 10.21681/2311-3456-2019-1-18-24.
7. Andryuhin E.V. , Ridli M.K., Pravikov D.I., Prognozirovanie sboev i otkazov v raspredelennyh sistemah upravleniya na osnove modelej prognozirovaniya vremennyh ryadov // Voprosy kiberbezopasnosti. 2019. № 3. S. 24-32. DOI: 10.21681/2311-3456-2019-3-24-32.
8. Kubarev A.V., Lapsar' A.P., Fedorova YA.V. Povyshenie bezopasnosti ekspluatacii znachimyh ob»ektov kriticheskoj infrastruktury s ispol'zovaniem parametricheskih modelej evolyucii // Voprosy kiberbezopasnosti. 2020. № 1. S. 8-17. DOI: 10.21681/2311-3456-2020-01-08-17.
9. Klimov S.M., Astrahov A.V., Sychev M.P. Metodicheskie osnovy protivodejstviya komp'yuternym atakam. Elektronnoe uchebnoe izdanie. – M.: MGTU imeni N.E. Baumana, 2013. 110 s.
10. Antonov S.G., Klimov S.M. Metodika ocenki riskov narusheniya ustojchivosti funkcionirovaniya programmno-apparatnyh kompleksov v usloviyah informacionno-tekhnicheskih vozdejstvij // Nadezhnost'. 2017. Tom 17. № 1. S. 32-39.
11. Kriticheski vazhnye ob»ekty i kiberterrorizm. CHast' 1. Sistemnyj podhod k organizacii protivodejstviya / O.O. Andreev i dr. Pod red. V.A. Vasenina. – M.:MCNMO, 2008. 398 s.
12. Minaev V.A., Korolev I.D., Zelencova E.V., Zaharchenko R.I. Kriticheskaya informacionnaya infrastruktura: ocenka ustojchivosti funkcionirovaniya // Radiopromyshlennost'. 2018. Tom №28, № 4. S. 59–67.
13. Severcev N.A., Beckov A.V. Sistemnyj analiz teorii bezopasnosti. – M.: Izd. MGU «TEIS», 2009. 452 s.
14. Ostrejkovskij V.A., Sal'nikov N.L. Veroyatnostnoe prognozirovanie rabotosposobnosti YAEU. – M.: Energoatomizdat, 1990. 416 s.
15. Pugachev V.S., Sinicyn I.N. Teoriya stohasticheskih sistem. M.: Logos, 2000. 1000 s.
16. Pyatkova N.I., Beresneva N.M. Modelirovanie kriticheskih infrastruktur energetiki s uchetom trebovanij energeticheskoj bezopasnosti. // Informacionnye i matematicheskie tekhnologii v nauke i upravlenii. 2017. № 3. S 54-65.
17. Astrahov A.V., Kulikov L.S., Minaev V.A. Modelirovanie ugroz informacionnyh vozdejstvij manipulyativnogo haraktera // Voprosy radioelektroniki. 2016. № 12. S. 63-69
18. Zaharchenko R.I., Korolev I.D. Model' funkcionirovaniya avtomatizirovannoj informacionnoj sistemy v kiberprostranstve // Voprosy kiberbezopasnosti. 2019. № 6. S. 69-78.