УДК 004.052.31

В.Е. Гвоздев, М.Б. Гузаиров, А.С. Давлиева, Р.Р. Галимов

Оценка характеристик информационной безопасности радиосети MANET на основе анализа топологий связей

Топологические особенности распределенных инфокоммуникационных сетей относятся к ключевым факторам, определяющим их свойства: стабильность, надежность и устойчивость к отказам и атакам. Исследование влияния топологии связей в Mobile ad hoc network как составной части инфраструктуры вычислительно-коммуникационных систем относится к приоритетным задачам в рамках проблемы обеспечения эффективного и результативного сетецентрического управления. Показаны результаты исследования, целью которого было оценивание эффективности разных методов выявления характера тенденций в случае коротких временных рядов.

Ключевые слова: информационная безопасность, сетецентрическое управление, надежность, эффективность, тенденция, топология связей, компонент, статистические индексы.

DOI: 10.21293/1818-0442-2023-26-4-35-43

Результативность и эффективность сложных распределенных субъектоцентрических систем сетецентрического управления в значительной степени определяются функционированием объединений стационарных и мобильных информационных инфраструктур, производящих критически важные для потребителей продукты и услуги. Следствием сложных, часто не выявленных взаимосвязей явлений и процессов как внутри сложных систем, так и с внешней средой, отказов / сбоев аппаратных и программных компонентов, ошибок людей, дефектов в построении организационных систем, внешних злонамеренных воздействий является возникновение угроз и опасностей разной природы, возникновением в системах неожиданных уязвимостей [1–6]. Это стимулирует разработку и развитие методов повышения информационной безопасности систем информационной поддержки сетецентрического управления на основе разноаспектного рассмотрения свойств инфраструктурных компонент.

Mobile ad hoc network (MANET) есть совокупность двух либо более беспроводных устройств, способных взаимодействовать друг с другом в условиях отсутствия централизованного управления. Каждый из узлов в беспроводной ad hoc network является одновременно хостом и маршрутизатором. Топология сети в общем случае является динамической в силу изменчивости связей между узлами по причине мобильности узлов, покидания сети одними узлами и подключением к сети новых узлов. Узел можно рассматривать как абстрактную сущность, состоящую из маршрутизатора и набора связанных мобильных хостов. Узлы также способны реагировать на изменения в топологии и на сбои в аффилированных узлах посредством оперативного изменения маршрутов.

Топологические особенности распределенных инфокоммуникационных сетей относятся к ключевым факторам, определяющим их свойства: стабильность; надежность и устойчивость к отказам и атакам.

В силу отмеченных обстоятельств исследование влияния топологии связей в MANET как составной части инфраструктуры вычислительно-коммуникационных систем относится к приоритетным задачам в рамках проблемы обеспечения эффективного и результативного сетецентрического управления.

Особенности MANET как объекта информационной безопасности

Ad hoc NETwork (MANET) есть автономная система мобильных хостов, взаимодействующих через беспроводные связи, в совокупности формирующие коммуникационную сеть. Особенностями MANET являются следующие:

1. Все узлы способны перемещаться и могут образовывать без участия человека случайным образом динамические объединения (изменять топологию связей) как реакции на внешние и внутренние события.

2. В силу того, что связь является беспроводной, зоны распространения сигналов от узлов-отправителей ограничены. Поэтому возможна ситуация, когда узел назначения находится вне зоны непосредственного доступа узла-отправителя. В силу этого передача осуществляется через промежуточные узлы, т.е. по маршрутам. Особенностью маршрутизации в MANET является возможность присутствия в таблицах маршрутизации устаревшей информации, что обусловлено изменениями топологии сети вследствие перемещения узлов; возникновения новых связей / разрыва существующих связей.

3. Инфокоммуникационные компоненты MANET являются гетерогенными, что обусловлено составом и количеством ресурсов в разных узлах сети; асимметричностью связей между узлами; различиями в характеристиках связей передающих и принимающих узлов; изменением величины накладных расходов на обеспечение взаимодействия вследствие мобильности узлов.

4. Каждый из хостов способен производить, потреблять данные, направлять, отправлять и продвигать пакеты от других узлов, т.е. выполнять функции маршрутизатора. Узлы должны совместными усилиями создавать сети и управлять ими в условиях отсутствия централизованного органа управления.

5. Подходы к управлению состоянием MANET в отличие от стационарных сетей (infrastructure-based network) [7] зависят от текущих характеристик сети, в том числе от состояния источников питания (бата-

рей) узлов. Беспроводные каналы связи имеют значительно меньшую пропускную способность, чем сети с проводными соединениями. Реализованная пропускная способность беспроводной связи в условиях множественного доступа с учетом затухания, шумов и помех часто оказывается значительно ниже чем максимальная скорость передачи радиосигнала.

6. В силу динамического характера и заранее неопределенного состава сети к ней возможно подключение вредоносных узлов. Мобильные беспроводные сети обычно более подвержены физическим угрозам безопасности, чем стационарные кабельные сети. Возрастает возможность прослушивания и спуфинга (подмены), а также атак, следствием которых является отказ в обслуживании.

Характеристики надежности MANET

Надежность, наряду с устойчивостью, живучестью и уязвимостью, тесно связана с информационной безопасностью [8–10]. Надежность (reliability) является метрической характеристикой степени уверенности в том, что система реализует поставленную задачу [11]. Надежность является латентной системной характеристикой. Определение содержания этого понятия предполагает многоаспектное рассмотрение, во-первых, с точки зрения возможности обеспечения системой информационных потребностей пользователя. В рамках этой точки зрения предполагается соответствие свойств системы широкому диапазону требований пользователя. Во-вторых, с точки зрения возможности возникновения в системе отказов. В рамках этой точки зрения базовым вопросом является определение содержания понятия «отказ» на основе знаний о функциях системы.

Причинами, осложняющими определение понятия «отказ», являются следующие:

– содержание понятия в рамках исследования аппаратной инфраструктуры осложняется оценкой влияния нарушения работоспособности отдельных устройств на свойства сети в целом: нарушение работоспособности одного устройства может оказаться фатальным для системы; нарушение работоспособности другого приведет лишь к незначительной задержке в передаче сообщений;

– помимо точек зрения, ориентированных на исследование аппаратных компонентов, при оценке надежности инфокоммуникационных систем следует учитывать то, что ценность информационных сервисов с точки зрения пользователя в том числе определяется надежностью данных.

Динамическое изменение как внутреннего состояния MANET, так и внешней среды, в которой функционирует система, является не только причиной изменения содержания понятия «отказ», но и изменением состава и степени влияния разных факторов, приводящих к отказу аппаратных компонент и активизации латентных дефектов в программных продуктах, а также препятствующих доступности информации.

В [12] описан подход к оценке надежности сетевых структур на основе анализа топологии связей. Как упоминалось выше, надежность является системной характеристикой и, в зависимости от точки зрения на систему, допускает множество толкований (что является реализацией тезиса о множественности точек зрения на сложный объект, что соответствует архитектурному подходу, и предписывает учитывать многомерный характер отношений между компонентами сложной системы [13]).

В рамках сетецентрической концепции [14] повышение качества информационного взаимодействия между компонентами сети направлено в том числе на повышение плотности связности элементов, возможности интенсивного информационного обмена.

Связи в топологических структурах являются унифицированным инструментом описания физической и информационной областей сетецентрической среды, компонентой которой является MANET.

С формальной точки зрения MANET на *j*-м отрезке времени может быть поставлен в соответствие граф (V_j, O_j), где V_j – узлы графа; O_j – связи между узлами на *j*-м отрезке времени. В рамках архитектурного подхода к исследованию сложным систем [13] MANET может характеризоваться множеством графов $\{(V_j^{(k)}, O_j^{(k)})\}$, где k – идентификатор точки зрения на MANET.

Мобильные системы имеют возможность взаимодействовать с другими локальными информационными системами, а также с Internet. Считается, что в MANET в качестве точки сочленения в каждый момент времени выступает один из хостов. При этом сторонние информационные системы взаимодействуют со всеми хостами мобильной системы через хост, играющий роль точки сопряжения [15].

В настоящей работе постулируется положение о том, что надежность связей между хостами (при разном толковании содержания связей) определяет такие свойства безопасности мобильных систем, как доступность; уязвимость; доступность; конфиденциальность; устойчивость.

Следуя [12] в качестве метрики надежности, определяемой на основе топологии связей, используется

$$B = \frac{\sigma}{N(N-1)}, \qquad (1)$$

где N – количество узлов графа; σ рассчитывается по правилу

$$\sigma = \sum_{i=1}^{N} k_i,$$

где $k_i = 0$, если *i*-й узел является точкой сочленения, $k_i = p_i$ – степень *i*-го узла.

В [12] показано, что использование упомянутой метрики позволяет поставить сетевой структуре метрическую характеристику, значения которой лежат в диапазоне $B \in (0;1]$, причем наибольшее значение B соответствует полносвязным графам. Там же отмечается, что существует прямая зависимость между характеристикой надежности сети и её устойчивостью

к сбоям и отказам узловых компьютеров и каналов связи.

Квантификация свойств системы на основе анализа топологии связей является формальным аппаратом представления свойств MANET, определяемых влиянием различных факторов: наличием физических каналов приема-передачи сведений; протоколами маршрутизации; состоянием батарей; работоспособностью аппаратных компонент хостов; наличием и доступностью в разных хостах требуемых данных и информации; злонамеренных внешних воздействий и внутренних нарушителей [16] и т.д. Использование оценок надежности связей, имеющих в рамках разных точек зрения различное толкование, обеспечивает сопоставимость свойств, получаемых в рамках разных точек зрения на MANET. Это, в свою очередь, делает возможным использование для построения оценок интегральных характеристик безопасности известных методов выявления тенденций; аппарата порядковых статистик; статистических индексов; лингвистических переменных.

Оценка тенденций изменения информационной безопасности MANET на основе статистических индексов

Мониторинг состояния компьютерных сетей является одной из задач обнаружения и противодействия нарушениям и компьютерным атакам [16]. Результатом внешних и внутренних негативных воздействий является, например, уменьшение пропускной способности канала ниже допустимого уровня, что формально может быть представлено как разрушение связей между хостами. Своевременная идентификация негативных изменений состояния мобильных систем создает основу для реализации деятельности, направленной на обнаружение актуальных источников угроз безопасности информации.

Считается, что сокращение времени выявления негативных тенденций изменения информационной безопасности является критически важным фактором с точки зрения обеспечения своевременных реакций на причины, влияющие на состояние системы. Это обусловливает выделение областей применимости методов оценивания характера тенденций, в том числе при малом числе компонент временного ряда. В рамках настоящего исследования полагается, что в значениях показателей надежности связей помимо систематической (обусловленной актуальными источниками опасности) составляющей присутствуют случайные, обусловленные особенностями рельефа, отказами и восстановлением оборудования.

Формальная постановка задачи

Имеются эмпирические исторические данные о наличии / отсутствии связей между хостами в различные моменты времени. По результатам оценки показателей надежности связей (например, характеризующих доступность информации), требуется оценить тенденцию изменения показателей. Дадим, следуя [16], содержательное толкование тенденциям разного вида.

Отрицательная тенденция сигнализирует о низком уровне защищенности системы, т.е. при появлении дополнительных угроз безопасности информации в отношении них не могут быть с высокой оперативностью приняты меры защиты информации, нейтрализующие эти угрозы.

Положительная тенденция соответствует высокому уровню защищенности, что означает: «…при появлении дополнительных угроз безопасности они с высокой степенью оперативности могут быть нейтрализованы…».

Отсутствие тенденции соответствует среднему уровню защищенности, что означает тому, что если в ходе эксплуатации информационной системы появились дополнительные угрозы безопасности информации, и в их отношении могут быть приняты меры защиты информации, нейтрализующие эти угрозы за время, приемлемое с точки зрения особенностей задач управления, поддерживаемых информационной системой.

Комплексный анализ информационной безопасности предполагает многоаспектное изучение свойств MANET. Каждой точке зрения ставится в соответствие топологическая структура. При этом единицы измерения разных характеристик различны.

Преобразование изначально несопоставимых характеристик к безразмерному виду на основании (1), постулируя взаимную независимость характеристик и полагая, что разные характеристики безопасности фиксируются в одни и те же интервалы времени, делает возможным формирование на основе временных рядов комплексных показателей информационной безопасности, например, в виде средних индексов.

Известны разные методы выявления тенденций, основанные на анализе качественных и количественных характеристик временных рядов. Особенностью задачи обеспечения информационной безопасности мобильных систем является необходимость оперативного реагирования на негативные изменения их состояния. Это обусловливает целесообразность использования методов, позволяющих объективно оценивать характер тенденции по малому числу измерений.

В ходе проведения исследований выполнялся следующий статистический эксперимент, целью которого было оценивание эффективности разных методов выявления характера тенденций в случае коротких временных рядов.

В случае оценки наличия отрицательной тенденции посредством датчиков случайных чисел в разных временных срезах генерировалось одно равномерно распределенное число

$$b(T_i) = 1 - a \cdot T_i, \quad (i = \overline{1;n}),$$

где T_i – значение временного ряда; a – характеристика скорости уменьшения показателя надежности.

Эксперимент повторялся 1 000 раз, причем в каждом из экспериментов оценивалась правильность идентификации наличия отрицательной тенденции, а также отсутствия тенденции. На рис. 1 показаны зависимости оценки эффективности разных методов в

виде доли правильных оценок характера тенденции от объема временного ряда *n* при различных *a*.

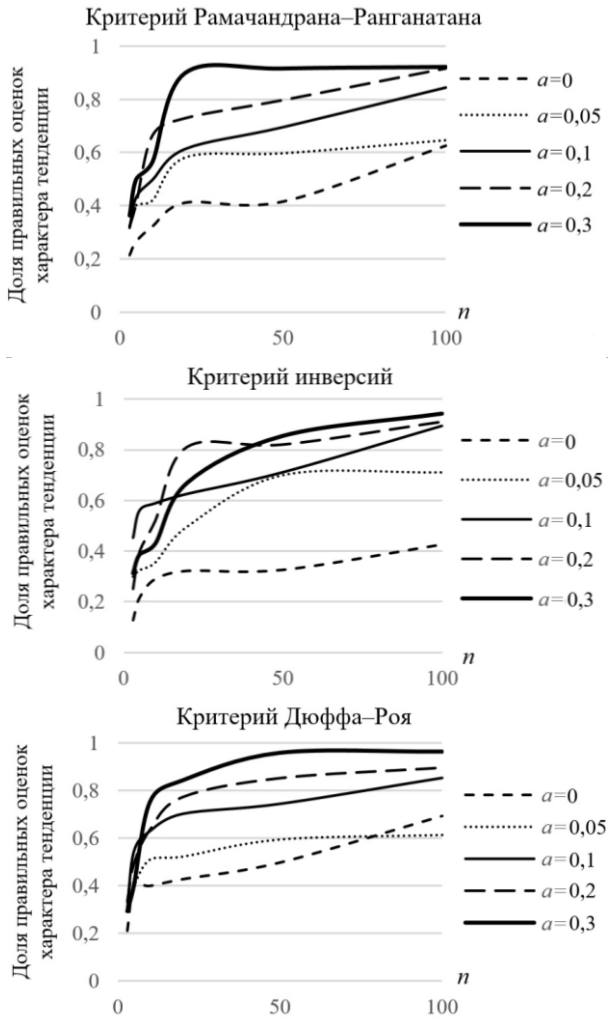

Рис. 1. Зависимости оценки эффективности разных методов в виде доли правильных оценок характера тенденции от объема временного ряда *n* при различных *a*

В работе рассматривались три критерия для выявления тенденции. Критерий Рамачандрана–Ранганатана является непараметрическим и учитывает не только количество серий временного ряда $T_1, T_2, .., T_n$, но и их длины, где одна серия – это ситуация $T_i \geq \tilde{T}$, а вторая – $T_i < \tilde{T}$. Особенность критерия состоит в том, что в случае больших объемах ряда гипотеза о случайности опровергается. Критерий инверсий предполагает наличие появления за значениями T_i временного ряда таких значений, являющихся меньшими по величине, т.е. $T_i > T_j$, где $i < j \leq n$. Статистикой данного критерия является общее число инверсий во временном ряде, принимающее целое число [17]. Критерий Дюффа–Роя является модификацией критерия автокорреляции. При предположении о справедливости гипотезы о случайности и отсутствии тренда распределение статистики Дюффа–Роя быстро сходится к стандартному нормальному закону [17].

Таким образом, можно иметь более устойчивые результаты на уровне 70–80%, при условии, что чем сильнее тенденция, тем меньше данных необходимо, чтобы установить это.

Предлагаемый подход может составить основу принятия решений о периодичности контроля состояния MANET.

Оценка устойчивости информационной безопасности на основе аппарата статистических индексов

Анализ характера тенденций не позволяет оценить степень влияния разных факторов на изменение состояния системы. Поэтому в качестве самостоятельной задачи исследования, ориентированной на совершенствование свойств технических компонент информационной составляющей MANET, следует выделить задачи сопоставления характеристик информационной безопасности на основе данных, получаемых в разных условиях.

Ниже рассматривается использование аппарата статистических индексов для решения следующих задач:

а) оценка различия комплексных показателей информационной безопасности, полученных по результатам испытаний и данным эксплуатации;

б) оценка эффективности ресурсного обеспечения различных задач информационной безопасности;

в) оценка влияния структуры ресурсного обеспечения задач информационной безопасности на комплексный показатель информационной безопасности;

г) учета территориальных особенностей ситуаций, урегулирование которых обеспечивается мобильными системами различного состава и структуры.

Для решения выделенных задач используется аппарат статистических индексов, что позволяет сопоставлять свойства различных либо одинаковых по конструкции систем, соответствующих разным условиям исследования.

Рассмотрим способ обеспечения сопоставимости данных, получаемых в условиях динамично изменяющейся внешней среды. Изменчивость внешней среды проявляется как в различии длительности периодов наблюдения T_j, так и в числе регистрируемых значений разных характеристик информационной безопасности в течение *j*-го периода наблюдения T_j.

Основу формирования сопоставимых показателей составляет соотношение

$$Y_l(T_j) = \frac{1}{T_j} \int_{T_j} f(Y_l(t))dt,$$

где $f(Y_l(t))$ – оценка временной зависимости характеристики $Y_l(t)$, определяемая как кусочно-линейная аппроксимация по значениям узлов $\{t_q, Y_l(t_q)\}$, где t_q – упорядоченные по возрастанию отметки вре-

мени $t_q \in T_j$, в которых регистрируются значения *l*-х характеристик $Y_l(t)$.

Такое преобразование позволяет сформировать таблицу вида

$$< j, Y_l(T_j) >, \quad l = \overline{1;L}, \quad j = \overline{1;J},$$

где *l* – идентификатор характеристики информационной безопасности; *j* – идентификатор временного интервала, которому соответствует $Y_l(t)$.

Построенная таблица служит исходными данными для расчета частных статистических индексов.

Рассмотрим содержание выделенных выше задач а–г.

а. Оценка показателей качества компонент распределенных систем информационного обеспечения предприятием-производителем осуществляется по данным специально организованных испытаний. Однако получение объективных оценок на основе специально организованных испытаний осложняется тем, что при испытаниях невозможно в полной мере воспроизвести условия реальной эксплуатации [18, 19]. Это осложняет вынесение обоснованных заключений практической пригодности физических компонент информационной подсистемы сетецентрической системы управления, а также о структуре ресурсного обеспечения различных видов работ, связанных с созданием физических компонент.

Тестирование соответствия является важным этапом жизненного цикла сложных инфокоммуникационных сетей. Важной составляющей тестирования соответствия свойств коммуникационных протоколов их спецификациям, а также других характеристик распределенных инфокоммуникационных систем является разработка и исполнение тестов.

Технологии испытания коммуникационных протоколов в MANET основаны на эмуляции и / или симуляции. При этом результаты симуляционного тестирования в ряде случаев оказываются достаточно далеки от результатов, получаемых в условиях эксплуатации [18–20].

В качестве инструмента решения задачи оценки степени различия комплексных показателей информационной безопасности, полученных по результатам испытаний и данным эксплуатации, предлагается использовать *индекс переменного состава* I_{vc}.

Индекс переменного состава рассчитывается по формуле

$$I_{vc} = \left(\frac{\sum_{j=1}^{m} y_1^{(j)} \cdot a_1^{(j)}}{\sum_{j=1}^{m} a_1^{(j)}} \right) / \left(\frac{\sum_{i=1}^{k} y_0^{(i)} \cdot a_0^{(i)}}{\sum_{i=1}^{k} a_0^{(i)}} \right). \qquad (2)$$

Здесь $y_0^{(i)}$ – значения *i*-х показателей информационной безопасности, определяемые по результатам специально организованных испытаний (*i* = 1, ..., *k*); $y_1^{(j)}$ – значения *j*-х показателей информационной безопасности, определяемые в ходе эксплуатации (*j* = 1, …, *m*); $a_0^{(i)}, a_1^{(j)}$ – весовые характеристики *i*-х и *j*-х показателей информационной безопасности, определяемые на основе топологий связей этих характеристик.

По сути (2) является средним индексом.

б. В [21] отмечается, что несбалансированность структуры бюджета проекта с требованиями к программному продукту является причиной низких потребительских свойств последних. В многочисленных литературных источниках (в частности, в [22]) подчеркивается, что свойства MANET в значительной степени определяются особенностями коммуникационных протоколов. В связи с этим можно выделить задачу сопоставления различных подходов к распределению ресурсов по видам работ проекта (WBS) по результатам испытания альтернативных вариантов протоколов.

В качестве инструмента решения задачи оценки эффективности ресурсного обеспечения решения разных классов задач информационной безопасности предлагается использовать *индекс постоянного состава* I_{fc}, характеризующий показатели информационной безопасности, полученные в результате испытаний, и соответствующие разным схемам распределения ресурсов. Рассчитывается по формуле

$$I_{fc} = \frac{\sum_{j=1}^{m} y_1^{(j)} \cdot a_1^{(j)}}{\sum_{j=1}^{m} y_0^{(j)} \cdot a_1^{(j)}}. \qquad (3)$$

Здесь $y_0^{(j)}$ – значения *j*-х показателей информационной безопасности в первом испытании (*j* = 1, ..., *m*); $y_1^{(j)}$ – значения тех же показателей информационной безопасности, определяемые во втором испытании при измененной схеме распределения ресурсов; $a_1^{(j)}$ – весовые характеристики *j*-х показателей информационной безопасности, определяемые на основе топологий связей этих характеристик.

в. Управление информационной безопасностью предполагает решение взаимосвязанного комплекса задач на организационном, методическом, технологическом уровнях. В рамках ограниченных объемов ресурсов важной задачей является формирование сбалансированной структуры затрат на обеспечение информационной безопасности. В связи с этим в качестве самостоятельной задачи следует выделить оценку влияния структуры ресурсного обеспечения задач информационной безопасности на комплексный показатель информационной безопасности. В качестве инструмента решения задачи оценки влияния структуры ресурсного обеспечения задач информационной безопасности на комплексный показатель информационной безопасности может использоваться *индекс структурных сдвигов* I_{ss}, рассчитываемый по формуле

$$I_{ss} = \left(\frac{\sum_{j=1}^{m} y_0^{(j)} \cdot a_1^{(j)}}{\sum_{j=1}^{m} y_0^{(j)} \cdot a_0^{(j)}} \right) \Bigg/ \left(\frac{\sum_{j=1}^{m} a_1^{(j)}}{\sum_{j=1}^{m} a_0^{(j)}} \right), \qquad (4)$$

где $y_0^{(j)}$ – значения j-х показателей информационной безопасности в первой схеме распределения ресурсов (j = 1, ..., m); $a_0^{(j)}, a_1^{(j)}$ – весовые характеристики j-х показателей информационной безопасности, определяемые на основе топологий связей этих характеристик при первой и второй схемах ресурсного обеспечения соответственно.

г. Устойчивость информационного сетевого взаимодействия в условиях динамически изменяющейся внешней среды является одним из базовых требований к системам информационного обеспечения сетецентрического управления [14]. MANET, при рассмотрении в рамках физической области, относится к классу технических систем с распределенными параметрами. В рамках этой точки зрения устойчивость является критически важным фактором безопасного функционирования MANET. Под устойчивостью понимается способность системы сопротивляться изменению своего состояния при различных воздействиях на нее [23, 24].

Особенностью сетецентрического управления является необходимость учета влияния территориальных особенностей ситуаций, урегулирование которых в том числе обеспечивается мобильными системами различного состава и структуры, при анализе информационной безопасности. Различие ситуаций и воздействий, испытываемых разными мобильными системами, находит отражение в топологических характеристиках показателей информационной безопасности. Для сопоставления уровней информационной безопасности, соответствующих разным участкам территории, могут использоваться индексы вида:

$$I_{A/B} = \frac{\sum_{j=1}^{m} y_1^{(j)} \cdot a_1^{(j)}}{\sum_{j=1}^{m} y_0^{(j)} \cdot a_1^{(j)}} \quad \text{и} \quad I_{fc} = \frac{\sum_{j=1}^{m} y_1^{(j)} \cdot a_0^{(j)}}{\sum_{j=1}^{m} y_0^{(j)} \cdot a_0^{(j)}}.$$

Здесь $I_{A/B}$ – индекс, в котором в качестве базы сравнения применяются данные за тот же период времени, соответствующие участку территории A; $I_{B/A}$ – индекс, используемый в качестве базы сравнения данных за тот же период времени соответствующие участку территории B; $y_0^{(j)}$ – значения j-х показателей информационной безопасности, определяемые на территории A; $y_1^{(j)}$ – значения j-х показателей информационной безопасности определяемые на территории B; $a_0^{(i)}, a_1^{(j)}$ – весовые характеристики показателей информационной безопасности, определяемые на основе топологий связей этих характеристик.

Пример использования индекса структурных сдвигов

В рамках проведения работ по обеспечению интероперабельности [25] инфокоммуникационных систем предложены две альтернативные архитектуры системы. В первой упор сделан на реактивный подход к обеспечению безопасности, основанный на выявлении и устранении латентных дефектов. Во второй – на превентивный подход, основанный на метафоре «Swiss Cheese Model» [26] и реализованный в рамках системной модели Anticipatory Failure Determination (AFD) [27].

По результатам испытания прототипов программных продуктов, в которых упор сделан на: эффективное восстановление работоспособности в случае проявления источников опасности (реактивный подход, AFD-1); предотвращение трансформации проявлений источника опасности в негативные последствия (превентивный подход, AFD-2), получены данные о характеристиках безопасности, соответствующие первой и второй архитектурам, при разном числе объектов в сети.

Требуется сформулировать предложения относительно направлений дальнейших работ по обеспечению функциональной безопасности программных компонент.

Заключение

В настоящей работе продемонстрировано использование аппарата статистических индексов применительно к задачам управления информационной безопасностью. Следует отметить, что идея использования статистических индексов в качестве интегральных характеристик сложных систем используется, например, в задачах экологической безопасности (индекс загрязнения атмосферы – ИЗА [28]; индекс загрязнения воды [29]). Ограничением рассмотренных выше формальных схем является линейная свертка индексов, соответствующих отдельным показателям информационной безопасности. Однако отмеченное ограничение не носит принципиального характера. В монографии [30] при описании метода обобщенного параметра приводится набор различных линейных и нелинейных сверток, предназначенных для формирования статистических индексов.

Литература

1. Baldwin K.J. Systems engineering guide for systems of systems. – Version 1.0. – Washington: Department of defense office of the deputy under secretary of defense for acquisition and technology, 2008. – 148 p.

2. Varshney U.S. Measuring the reliability and survivability of infrastructure-oriented wireless networks / U.S. Varshney, P.S. Andrew, A.D. Malloy // Local Computer Networks (LCN 2001), Florida, USA, 2001. – P. 611–618.

3. Bhaiji Y. Network security technologies and solutions // CCIE Professional Development, 2008. – 840 p.

4. Wireless local area network hits the public [Электронный ресурс]. – Режим доступа: http://www.touchbriefings.com/pdf/744/wire041_vis.pdf, свободный (дата обращения: 16.03.2011).

5. Westmark V.R. A definition for information system survivability // System Sciences. – 2004. – P. 1–10.

6. Сетецентрическое управление: современная парадигма развития систем управления в вооруженных силах ведущих держав мира / И.В. Сурма, В.И. Анненков, В.В. Карпов, А.В. Моисеев // Национальная безопасность. – 2014. – № 2(31). – С. 317–327.

7. Loo J. Mobile Ad hoc Networks: current status and future trends / J. Loo, J.L. Mauri, J.H. Ortiz // Auerbach publications, 2016. – 528 p.

8. ГОСТ 27.002–2015. Надежность в технике. Термины и определения. – 2016. – 23 с.

9. Ellison R.J. Survivable network systems: an emerging discipline / R.J. Ellison, D.A. Fisher, R.C. Linger, H.F. Lipson, T. Longstaff, N.R. Mead // Technical report CMU/SEI-97-TR-013. – 1997 [Электронный ресурс]. – Режим доступа: https://resources.sei.cmu.edu/asset_files/TechnicalReport/1998_005_001_16598.pdf, свободный (дата обращения: 15.09.2023).

10. Mohsin Y. Communication and computer networks simulator (NS2) // Computer communications (Networks). – 2014. – 17 p.

11. Randell B. System reliability and structuring // Computing Systems Reliability. – Cambridge University Press, New York, USA. – 1979. – P. 1–18.

12. Тимофеев А.В. Адаптивное управление и интеллектуальный анализ информационных потоков в компьютерных сетях. – СПб.: ООО «Анатолия», 2012. – 280 с.

13. IEEE 1471–2000. Recommended Practice for Architecture Description of Software-Intensive Systems [Электронный ресурс]. – Режим доступа: http://cabibbo.dia.uniroma3.it/ids/altrui/ieee1471.pdf, свободный (дата обращения: 18.05.2021).

14. Макаренко С.И. Подавление сетецентрических систем управления радиоэлектронными информационно-техническими воздействиями // Системы управления, связи и безопасности. – 2017. – № 4. – С. 15–59.

15. Cordeiro C. Ad hoc & sensor networks: Theory and Applications / C. Cordeiro, D. Agrawal // World Scientific Publishing Co. Pte, 2006. – 663 p.

16. Методика определения угроз безопасности информации в информационных системах: метод. документ // ФСТЭК России. – 2021. – 43 с.

17. Лемешко Б.Ю. Критерии проверки гипотез о случайности и отсутствии тренда. Рук-во по применению: учеб. пособие / Б.Ю. Лемешко, И.В. Веретельникова. – Новосибирск, 2021. – 215 с.

18. Maag S. Model-Based Testing for MANETs // Труды ИСП РАН. – 2014. – Т. 26, вып. 6. – С. 31–44.

19. Lu Z. Unlocking the power of OPNET modeler / Z. Lu, H. Yang. – Cambridge University Press, 2012. – 238 p.

20. Salem A. Mobile Ad-hoc Network simulators, a survey and comparisons / A. Salem, H. Awwad // International journal of P2P network trends and technology (IJPTT). – 2014. – Vol. 4, Iss. 3. – P. 22–26.

21. Макконнелл С. Сколько стоит программный проект. – М.: Русская редакция; СПб.: Питер, 2007. – 297 с.

22. Bekmezci I. Flying Ad-Hoc Networks (FANETs): a survey / I. Bekmezci, O. Sahingoz, S. Temel // Ad Hoc Networks. – 2013. – Vol. 11. – P. 1254–1270.

23. Колесников А.А. Проблемы теории аналитического конструирования нелинейных регуляторов и синергетический подход // Синергетика и проблемы управления. – М.: ФИЗМАТЛИТ, 2004. – С. 35–129.

24. Gvozdev V.E. Ensuring the functional safety of the distributed dynamic systems components in the conditions of uncertainty of the environment use / V.E. Gvozdev, M.B. Guzairov, O.Ya. Bezhaeva, A.S. Davlieva, R.R. Galimov // Proceedings – ICOECS–2020: 2020 International Conference on Electrotechnical Complexes and Systems. – 2020. – P. 1–6.

25. ГОСТ 55062–2021. Информационные технологии. Интероперабельность. Основные положения. – 2021. – 12 с.

26. Revisiting the «Swiss Cheese» Model of Accidents // European Organization for the Safety of Air Navigation. – 2006. – No. 13/06. – 25 p.

27. Renan Favarão Da Silva, Marco Aurélio De Carvalho. Anticipatory Failure Determination (AFD) for product reliability analysis: A comparison between AFD and Failure Mode and Effects Analysis (FMEA) for identifying potential failure modes // Federal Technological University of Paraná (UTFPR). – Curitiba, Brazil, 2019. – 24 p.

28. Руководящий документ РД 52.04.6672005. Документы о состоянии загрязнения атмосферы в городах для информирования государственных органов, общественности и населения. Общие требования к разработке, построению, изложению и содержанию. – М.: Метеоагентство Росгидромета, 2006. – 50 с.

29. Глотова Н.В. Мониторинг среды обитания: учеб. пособие к практ. занятиям. – Челябинск: Изд-во ЮУрГУ, 2006. – 22 с.

30. Гаскаров Д.В. Прогнозирование технического состояния и надежности радиоэлектронной аппаратуры / Д.В. Гаскаров, Т.А. Голинкевич, А.В. Мозгалевский. – М.: Советское радио, 1974. – 224 с.

Гвоздев Владимир Ефимович
Д-р техн. наук, проф. каф. технической кибернетики
Уфимского университета науки и технологий (УУНиТ)
К. Маркса ул., 12, г. Уфа, Россия, 450008
ORCID: 0009-0004-8557-3445
Тел.: +7-908-350-35-63
Эл. почта: wega55@mail.ru

Гузаиров Мурат Бакеевич
Д-р техн. наук, проф.каф. управления информационной безопасностью УУНиТ
З. Валиди ул., 32, г. Уфа, Россия, 450076
Тел.: +7 (347-2) 29-97-51
Эл. почта: guzairovmb@uust.ru

Давлиева Алия Салаватовна
Канд. техн. наук, доцент
каф. технической кибернетики УУНиТ
К. Маркса ул., 12, г. Уфа, Россия, 450008
ORCID: 0000-0002-7548-2134
Тел.: +7-908-350-35-63
Эл. почта: davlieva.as@ugatu.su

Галимов Роберт Ришатович
Аспирант каф. технической кибернетики УУНиТ
К. Маркса ул., 12, г. Уфа, Россия, 450008
Тел.: +7-908-350-35-63
Эл. почта: rrgalimov@gmail.com

Gvozdev V.E., Guzairov M.B., Davlieva A.S., Galimov R.R.
Evaluation of MANET information safety characteristics based on the analysis of link topologies

Topological features of distributed infocommunication networks are among the key factors that determine their properties: stability, reliability and resistance to failures and attacks. The study of the communications topology influence in the Wireless Mobile ad hoc network, as an integral part of the infrastructure

of computing and communication systems, is one of the priority tasks when it comes to ensure the effective and efficient network-centric control. The paper presents the results of a study aiming to evaluate the efficiency of various methods used to identify the nature of trends in the case short time series.

Keywords: information safety, network-centric control, reliability, efficiency, trend, link topology, component, statistical indices.

DOI: 10.21293/1818-0442-2023-26-4-35-43

References

1. Baldwin K.J. *Systems engineering guide for systems of systems. Version* 1.0. Washington. Department of defense office of the deputy undersecretary of defense for acquisition and technology, 2008, 148 p.

2. Varshney U.S. Andrew P.S., Malloy A.D. Measuring the reliability and survivability of infrastructure-oriented wireless networks, Florida, USA. *Local Computer Networks (LCN 2001)*, 2001, pp. 611–618.

3. Bhaiji Y. Network security technologies and solutions. *CCIE Professional Development*, 2008. 840 p.

4. Wireless local area network hits the public. Available at http://www.touchbriefings.com/pdf/744/wire041_vis.pdf, free. (Accessed: March 16, 2011).

5. Westmark V.R. A definition for information system survivability. *System Sciences*, 2004, pp. 1–10.

6. Surma I.V., Annenkov V.I., Karpov V.V., Moiseev A.V. *Setecentricheskoe upravlenie: sovremennaya paradigma razvitiya sistem upravleniya v vooruzhennyh silah vedushchih derzhav mira* [Network-centric control: a modern paradigm for the development of control systems in the armed forces of the leading powers of the world]. *National Security*, 2014, no. 2 (31), pp. 317–327. (In Russ.).

7. Loo J. Mauri J.L., Ortiz J.H. Mobile Ad hoc Networks: current status and future trends. *Auerbach publications*, 2016, 528 p.

8. GOST 27.002-2015 *Nadezhnost' v tekhnike. Terminy i opredeleniya* [Reliability in engineering. Terms and definitions], 2016. 23 p. (In Russ.).

9. Ellison R.J., Fisher D.A., Linger R.C., Lipson H.F., Longstaff T., Mead N.R. Survivable network systems: an emerging discipline. *Technical report CMU/SEI-97-TR-013* 1997 Available at: https://resources.sei.cmu.edu/asset_files/TechnicalReport/1998_005_001_16598.pdf, free (Accessed: May 15, 1999).

10. Mohsin Y. Communication and computer networks simulator (NS2). *Computer Communications (Networks)*, 2014. 17 p.

11. Randell B. System reliability and structuring. Cambridge University Press. New York, USA. *Computing Systems Reliability*, 1979, pp. 1–18.

12. Timofeev A.V. *Adaptivnoye upravleniye i intellektualnyy analiz informatsionnykh potokov v kompyuternykh setyakh* [Adaptive control and intelligent analysis of information flows in computer networks]. St. Petersburg, LLC «Anatolia», 2012, 280 p. (in Russ.).

13. IEEE 1471–2000. Recommended Practice for Architecture Description of Software-Intensive Systems. Available at: http://cabibbo.dia.uniroma3.it/ids/altrui/ieee1471.pdf, free (Accessed: May 18, 2021).

14. Makarenko S.I. [Suppression of network-centric control systems by radio-electronic information and technical influences]. *Control Systems, Communications and Security*, 2017, no. 4, pp. 15–59 (in Russ.).

15. Cordeiro C. Agrawal D. Ad hoc & sensor networks: Theory and Applications. *World Scientific Publishing Co. Pte*, 2006, 663 p.

16. *Metodika opredeleniya ugroz bezopasnosti informatsii v informatsionnykh sistemakh: metodicheskiy dokument* [Methodology for determining information security threats in information systems: a methodological document]. FSTEC, Russia, 2021, 43 p. (in Russ.).

17. Lemeshko B.Yu., Veretelnikova I.V. *Kriterii proverki gipotez o sluchaynosti i otsutstvii trenda. Rukovodstvo po primeneniyu* [Criteria for testing hypotheses about randomness and the absence of a trend. Application guide: textbook]. Novosibirsk, 2021, 215 p. (in Russ.).

18. Maag S. Model-Based Testing for MANETs. *Russian Journal of Proceedings of the Institute for System Programming of the Russian Academy of Sciences*, 2014, vol. 26, iss. 6, pp. 31–44.

19. Lu Z., Yang H. Unlocking the power of OPNET modeler. *Cambridge University Press*, 2012, 238 p.

20. Salem A., Awwad H. Mobile Ad-hoc Network simulators, a survey and comparisons. *International journal of P2P network trends and technology (IJPTT)*, 2014, vol. 4, iss. 3, pp. 22–26.

21. McConnell C. *Skolko stoit programmnyy proyekt* [How much does a software project cost]. St. Petersburg: Peter, 2007, 297 p. (in Russ.).

22. Bekmezci I., Sahingoz O., Temel S. Flying Ad-Hoc Networks (FANETs): a survey. *Ad Hoc Networks*, 2013, vol. 11, pp. 1254–1270.

23. Kolesnikov A.A. *Problemy teorii analiticheskogo konstruirovaniya nelinejnyh regulyatorov i sinergeticheskij podhod* [Problems of the Theory of Analytical Design of Nonlinear Regulators and the Synergetic Approach]. *Synergetics and Control Problems*, 2004, pp. 35–129 (in Russ.).

24. Gvozdev V.E., Guzairov M.B., Bezhaeva O.Ya. Davlieva A.S., Galimov R.R. Ensuring the functional safety of the distributed dynamic systems components in the conditions of uncertainty of the environment use. *Proceedings – ICOECS 2020: 2020 International Conference on Electrotechnical Complexes and Systems*, 2020, pp. 1–6.

25. GOST 55062–202.1 *Informacionnye tekhnologii Interoperabel'nost'* [Osnovnye polozheniya Information technology Interoperability. Basic provisions], 2021, 12 p. (in Russ.).

26. Revisiting the «Swiss Cheese» Model of Accidents. *European Organization for the Safety of Air Navigation*, 2006, no. 13/06, pp. 1–25.

27. Renan Favarão Da Silva, Marco Aurélio De Carvalho. Anticipatory Failure Determination (AFD) for product reliability analysis: A comparison between AFD and Failure Mode and Effects Analysis (FMEA) for identifying potential failure modes. Curitiba, Brazil. *Federal Technological University of Paraná (UTFPR)*, 2019, 24 p.

28. Document RD 52.04.6672005. *Dokumenty o sostoyanii zagryazneniya atmosfery v gorodakh dlya informirovaniya gosudarstvennykh organov. obshchestvennosti i naseleniya. Obshchiye trebovaniya k razrabotke. postroyeniyu. izlozheniyu i soderzhaniyu* [Documents on the state of air pollution in cities to inform government agencies, the public and the population. General requirements for development, construction, presentation and content]. Meteo agency of Roshydromet, 2006, 50 p. (in Russ.)

29. Glotova N.V. *Monitoring sredy obitaniya* [Monitoring of the habitat: a textbook for practical exercises]. Chelyabinsk: Publishing house of YuUrGU, 2006, 22 p. (in Russ.).

30. Gaskarov D.V., Golinkevich T.A., Mozgalevsky A.V. *Prognozirovaniye tekhnicheskogo sostoyaniya i nadezhnosti radioelektronnoy apparatury* [Forecasting the technical condition and reliability of radio electronic equipment] Moscow. Soviet radio, 1974, 224 p. (in Russ.).

Vladimir E. Gvozdev
Doctor of Science in Engineering, Professor,
Department of Technical Cybernetics,
Ufa University of Science and Technology
12, K. Marx st., Ufa, Russia, 450008
ORCID: 0009-0004-8557-3445
Phone: +7-908-350-35-63
Email: wega55@mail.ru

Murat B. Guzairov
Doctor of Science in Engineering, Professor,
Department of Information Security Management
Ufa University of Science and Technology
12, K. Marx st., Ufa, Russia, 450008
Phone: +7 (347-2) 29-97-51
Email: guzairovmb@uust.ru

Aliya S. Davlieva
Candidate of Sciences in Engineering, Assistant Professor,
Department of Technical Cybernetics,
Ufa University of Science and Technology
32, Z. Validi st., Ufa, Russia, 450076
ORCID: 0000-0002-7548-2134
Phone: +7-908-350-35-63
Email: davlieva.as@ugatu.su

Robert R. Galimov
Postgraduate student, Department of Technical Cybernetics,
Ufa University of Science and Technology
12, K. Marx st., Ufa, Russia, 450008
Phone: +7-908-350-35-63
Email: rrgalimov@gmail.com