Способ моделирования сетей связи, функционирующих при наличии множественных центров прямого и косвенного управления

Ю. И. Стародубцев[1], А. А. Бречко[2]
Военная академия связи им. С. М. Буденного
[1]prof.starodubtsev@gmail.com, [2]sashabreck27@gmail.com

М. А. Давлятова
Санкт-Петербургский политехнический университет Петра Великого
malika.davliatova@gmail.com

***Аннотация*. В статье представлен новый способ моделирования сетей связи, функционирующих в условиях множественных разнородных управляющих воздействий, в том числе опосредованных. Разработанный способ моделирования позволяет вычислить критическое количество реализуемых угроз безопасности, при котором обеспечивается реализация заданного количества и качества услуг связи.**

Ключевые слова: сеть связи; центр управления; угроза безопасности; нестационарность сети связи

Моделирование сложных систем является нетривиальной задачей. Сложные системы, которыми являются сети связи, имеют особенности, присущие, как сложным системам в целом, так и особенности специфические, характеризующие функционирование именно сетей связи.

Для эффективного управления сетью и принятия адекватных управленческих решений необходимо иметь информацию об особенностях функционирования сети в конкретных условиях. Проведение натурных экспериментов на сети не всегда возможно и целесообразно в силу возможного создания помех функционированию сети по назначению.

Моделирование сетей связи позволяет определить интересующие выходные параметры и характеристики, получить оценку показателей эффективности и качества, осуществить поиск оптимальной структуры и параметров сети. Моделирование применяется как для проектирования сетей связи, так и для исследования уже существующих сетей.

Сети связи, с увеличением масштаба и количества элементов, характеризуются сложной структурой, стохастичностью, нестационарностью, наличием множественных центров управления. Представляемый способ моделирования учитывает вышеописанные особенности сети и позволяет вычислить критическое количество реализуемых угроз безопасности, при котором обеспечивается реализация заданного количества и качества услуг.

Множественные центры управления, реализуя свои, зачастую стохастические воздействия, стохастически изменяют состояние сети связи. Центры прямого управления реализуют легитимное и целенаправленное управление сетью. Центрами косвенного управления могут являться различные сущности, в том числе реализующие преднамеренные деструктивные воздействия, приводящие к отказам элементов сети [1].

Существуют различные внешние воздействия, которые влияют на функционирование сети связи, и по причине возникновения воздействия делятся на непреднамеренные и преднамеренные. Основной причиной возникновения преднамеренных отказов вследствие внешних воздействий является реализация угроз безопасности. Угрозы безопасности информации – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Способ моделирования реализуется последовательностью действий, представленной на блок-схеме (рис. 1).

Предварительно формируют исходные данные для моделирования (рис. 1, блок 1), которые включают:

- исходный граф моделируемой сети связи, отражающий топологию и структуру сети связи в виде совокупности из N вершин и M ветвей;
- вероятности существования i-й вершины графа сети, где $i = 1, 2, ..., N$ – значения вероятности существования j-й ветви, соединяющей соответствующие вершины графа сети, где $j = 1, 2, ..., M$;
- совокупности из W возможных видов угроз безопасности, Z адекватных им средств защиты, причем каждому из видов угроз и средств защиты присваивают определенные численные индексы;
- число статистических экспериментов A;
- предварительно сформированные последовательности псевдослучайных чисел (ПСЧ)

и закон их распределения, которые соответствуют непреднамеренным отказам вершин и ветвей графа сети;

- предварительно сформированные ПСЧ и закон распределения случайных чисел, соответствующих появлению определенного вида угроз безопасности;
- требуемое значение среднего времени обслуживания абонентов;
- совокупность средств защиты от воздействия соответствующих видов угроз безопасности.

К наиболее часто реализуемым видам угроз безопасности можно отнести: анализ сетевого трафика, сканирование сети, подмену доверенного объекта сети и передачу по каналам связи сообщений от его имени с присвоением его прав доступа, навязывание ложного маршрута сети, внедрение ложного объекта сети.

После задания исходных данных начинают процедуру моделирования сети связи. Первоначально имитируют процесс функционирования сети связи (рис. 1, блок 3) при наличии непреднамеренных отказов вершин и ветвей сети, входящих в исходный граф сети, структура которого рассматривается как совокупность двухполюсных систем. Полюсами в двухполюсных системах являются абоненты сети связи.

В результате действия непреднамеренных отказов происходит частичное разрушение начального графа. При этом информационное направление связи (ИНС) (абонент-абонент) считается работоспособным, если существует хотя бы один путь успешного функционирования (ПУФ) от одного абонента к другому [2]. Если существует хотя бы один ПУФ из существующих на исходном графе моделируемой сети связи, то ИНС (абонент 1-абонент 2) считается работоспособным и сеть связи для указанной группы абонентов выполняет свои функции. Для оценки уровня работоспособности, частично разрушенной под воздействием непреднамеренных отказов сети связи, измеряют ее номинальные характеристики $\overline{V}_H$, $\overline{K}_H$ (рис. 1, блок 4).

Существуют несколько видов характеристик функционирования сети связи, но наиболее простыми в измерении и существенно влияющими на среднее время обслуживания $\overline{t}_{обсл}$ характеристиками сети связи являются оперативно-технические характеристики [3, 4]. Поэтому были выбраны следующие характеристики: $\overline{V}_H$ – средняя скорость передачи сообщений; $\overline{K}_H$ – среднее количество ошибок в канале. При определении средней скорости передачи сообщений и количества ошибок в канале в сети связи необходимо учесть, что моделируемая сеть связи состоит из N узлов (вершин) и каждый узел имеет L^i каналов связи, т.е. среднее значение вычисляется по формулам:

$$\overline{V}_H = \frac{\sum_{i=1}^{N} \overline{V}_{iH}}{N}; \ \overline{K}_H = \frac{\sum_{i=1}^{N} \overline{K}_{iH}}{N}$$

где N – количество узлов (вершин) сети связи; $\overline{V}_{iH}$ – средняя номинальная скорость передачи сообщений на *i*-ом узле сети связи; $\overline{K}_{iH}$ – среднее номинальное число ошибок в каналах связи на *i*-ом узле сети связи;

$$\overline{V}_{iH} = \frac{\sum_{r=1}^{L^i} \overline{V}_r}{L}; \ \overline{K}_{iH} = \frac{\sum_{r=1}^{L^i} \overline{K}_r}{L},$$

где $\overline{V}_r$ – средняя скорость *r*-го канала *i*-го узла сети связи; L^i – количество каналов связи на *i*-ом узле; $\overline{K}_r$ – среднее количество ошибок в *r*-ом канале на *i*-ом узле сети связи.

После чего имитируют угрозы безопасности на сеть связи. При этом считают, что в дальнейшем процессе моделирования каких-либо нарушений работы сети из-за непреднамеренных отказов не происходит (т.е. установление стационарного режима – неизменность состояния сети связи). Данное условие возможно, учитывая, что средний промежуток времени между непреднамеренными отказами равен 51 часу (14 отказов в месяц), а средний промежуток времени между преднамеренными угрозами равен 15 минутам (4 реализации угроз безопасности в час).

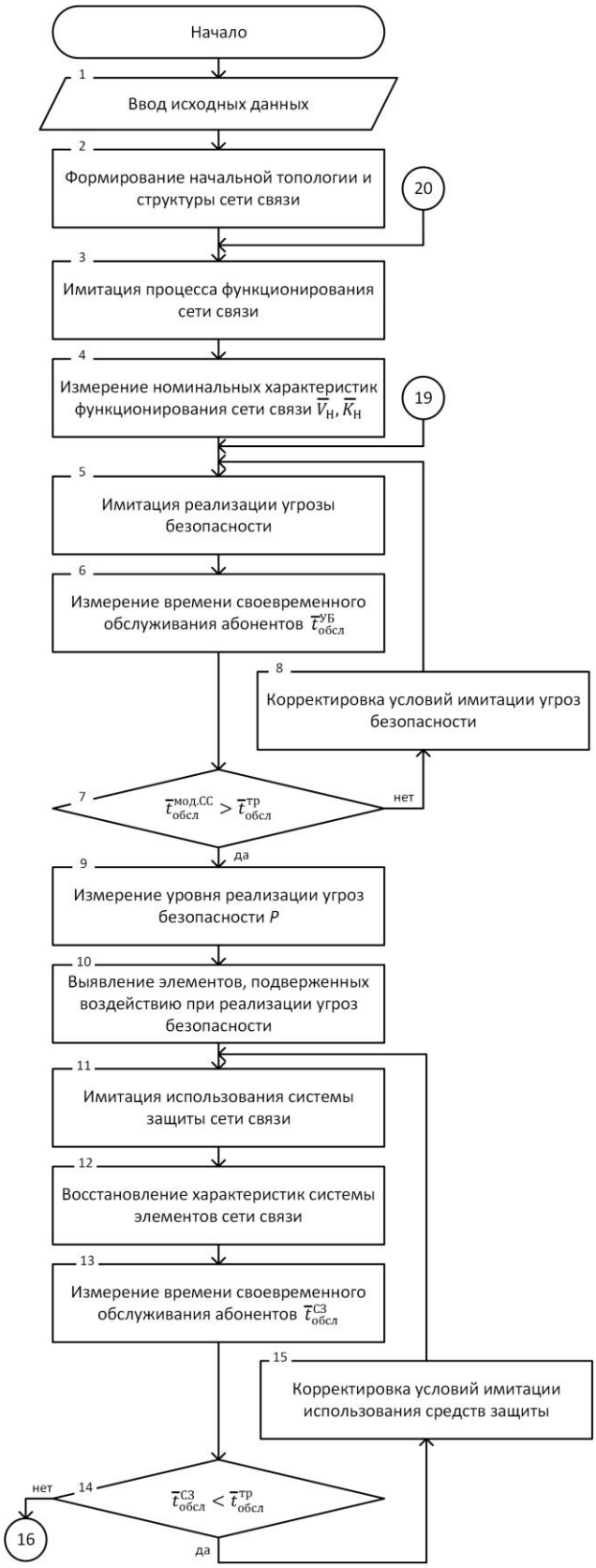
Имитацию угроз безопасности осуществляют путем воздействия угрозы, соответствующей сгенерированному случайным образом по предварительно заданному закону распределения численному индексу из ранее заданной совокупности угроз *W*. При этом считают, что последствия реализованной угрозы безопасности эквивалентны.

По результатам дополнительного воздействия угроз безопасности формируют второй промежуточный граф, включающий оставшиеся вершины и соединяющие их ветви после возникновения непреднамеренных отказов и реализации угрозы безопасности (рис. 1, блок 5). При этом используется заданный закон распределения ПСЧ для определения вершин сети отказавших при реализации угроз безопасности. После чего измеряют среднее значение времени обслуживания абонентов $\overline{t}_{обсл}$ и выполняют проверку соответствия времени обслуживания абонентов требуемому значению (рис. 1, блоки 6, 7).

Под временем обслуживания понимается время установления соединения, которое определяется с момента поступления заявки на узел связи до момента ответа абонента. При этом время обслуживания абонентов моделируемой сети связи определяют временем обслуживания на каждом узле. Причем, учитывая возможный разброс значений, время обслуживания вычисляют по формуле, характеризующей максимальное возможное время обслуживания на имеющихся узлах сети:

$$t_{обсл}^{\max} = \max\left\{t_{обсл}^{i}\right\}$$

где $t_{обсл}^{i}$ – значение времени обслуживания на *i*-м узле сети связи, $i = 1, 2, ..., N$.



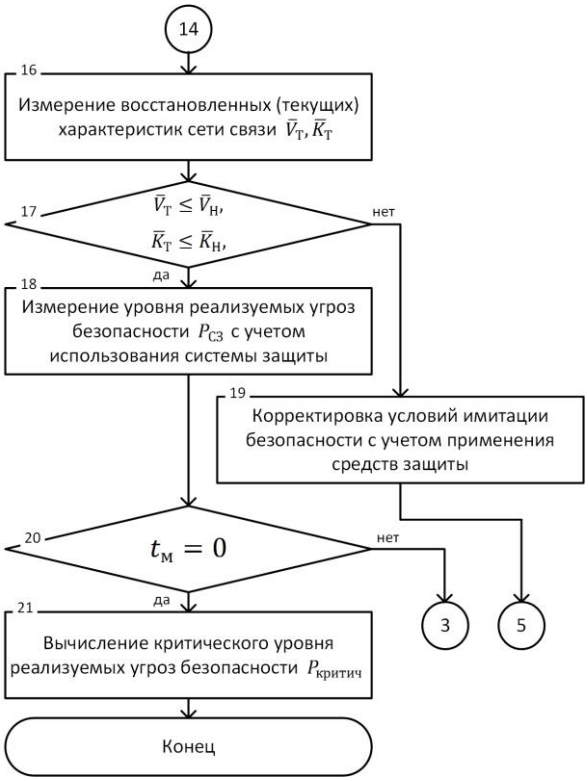


Рис. 1. Блок-схема способа моделирования сетей связи

Если требования по времени обслуживания абонентов выполняются, то осуществляют корректировку условий имитации угроз безопасности путем добавления еще одной угрозы безопасности, после чего повторно имитируют реализацию угроз безопасности с учетом добавленной угрозы (рис. 1, блок 8). Это позволяет определить уровень реализуемых угроз безопасности, воздействующих на моделируемую сеть связи и приводящих к нарушению ее функционирования, т.е. отсутствию необходимых информационных направлений связи. Если требования по времени обслуживания абонентов не выполняются, то измеряют уровень реализуемых угроз безопасности *P* путем определения количества угроз безопасности, использованных при имитации (рис. 1, блок 9), который является промежуточным и не учитывает использование средств защиты сети связи.

Затем выявляют вершины сети, которые были подвержены воздействию угрозам безопасности (рис. 1, блок 10) и имитируют (рис. 1, блок 11) использование средств защиты, для чего фиксируют одну из реализуемых угроз безопасности, выбирают из ранее заданной совокупности *Z* адекватное ей средство защиты.

После чего формируют (рис. 1, блок 12) итоговый граф, включающий восстановленные вершины и соединяющие их ветви, находящиеся на маршруте между исходящим и входящим узлами с учетом использованного средства защиты. При этом используют заданный закон распределения последовательности ПСЧ для определения вершин сети, восстановленных при использовании средств защиты.

Затем измеряют время обслуживания $t_{обсл}^{СЗ}$ абонентов для итогового графа (рис. 1, блок 13). Затем сравнивают (блок 14, рис. 2) время обслуживания $t_{обсл}^{СЗ}$ абонентов с учетом применения средств защиты с ранее заданным требуемым значением $t_{обсл}^{ТР}$. Если требования по времени обслуживания абонентов не выполняются, то корректируют условия имитации использования средств защиты путем добавления еще одного средства защиты (рис. 1, блок 15).

Это позволяет определить уровень (количество) реализуемых угроз безопасности, воздействующих на моделируемую сеть связи, которые могут быть устранены за счет использования средств защиты, т.е. возможности имеющихся средств защиты.

Если требования по времени обслуживания абонентов не выполняются, то осуществляется измерение текущих характеристик сети связи $\overline{V}_T$, $\overline{K}_T$ с учетом восстановленных вершин за счет использованных средств защиты (рис. 1, блок 16). Для этого измеряют текущие скорости передачи сообщений и текущие количества ошибок в канале. По полученным измерениям вычисляют их средние значения по формулам:

$$\overline{V}_T = \frac{\sum_{i=1}^{N} \overline{V}_{iT}}{N};$$

$$\overline{K}_T = \frac{\sum_{i=1}^{N} \overline{K}_{iT}}{N},$$

где N – количество узлов (вершин) связи; $\overline{V}_{iT}$ – средняя текущая скорость передачи сообщений на i-узле сети связи; $\overline{K}_{iT}$ – среднее текущее количество ошибок в канале связи на i-ом узле сети связи.

Далее (рис. 1, блок 17) сравнивают средние текущие (восстановленные) значения характеристик сети связи $\overline{V}_T$, $\overline{K}_T$ с ранее заданными номинальными значениями данных характеристик сети связи $\overline{V}_H$, $\overline{K}_H$.

Если средние текущие значения характеристик сети связи равны номинальным, то осуществляется повторная корректировка условий имитации угроз безопасности с учетом применения средств защиты, путем добавления еще одной угрозы безопасности, после чего повторно имитируют реализацию угроз безопасности с учетом добавленной угрозы (рис. 1, блок 19).

Это позволяет определить уровень (количество) реализуемых угроз безопасности, воздействующих на моделируемую сеть связи, приводящих не только к невыполнению требований по времени обслуживания абонентов, но и к изменению (ухудшению) характеристик функционирования сети связи. В этом случае будет уточнен уровень реализуемых угроз безопасности P, который будет являться окончательным с учетом использования средств защиты сети связи.

Если текущие значения характеристик сети связи меньше номинальных, то производится измерение уровня реализуемых угроз безопасности $P_{СЗ}$ с учетом использованной средств защиты, путем определения количества реализованных угроз безопасности (рис. 1, блок 18).

Затем, после окончания моделирования, вычисляют критический уровень реализуемых угроз безопасности $P_{кр}$ по формуле: $P_{кр} = P - P_{СЗ}$ (рис. 1, блок 21).

Таким образом, имитация реализации угроз безопасности на сеть связи, существенно влияющих на параметры функционирования сети связи и приводящих к нарушению ее функционирования, путем определения критического уровня реализуемых угроз безопасности позволяет:

- осуществлять сравнительную оценку систем связи по уровню защищенности;
- определять необходимое количество сил (средств) защиты для обеспечения заданного количества и качества услуг связи;
- оптимизировать состав и структуру систем связи с учётом требований уровня защищенности.

Статья является развитием способа, на который получен патент РФ [5].

СПИСОК ЛИТЕРАТУРЫ

[1] Стародубцев Ю.И., Бегаев А.Н., Давлятова М.А. Управление качеством информационных услуг. / Под общ. ред. Ю.И. Стародубцева. СПб. : Изд-во Политехн. ун-та, 2017. 454 с.

[2] Иванов Е.В. Имитационное моделирование средств и комплексов связи и автоматизации. СПб. : ВАС, 1992. 347 с.

[3] Телекоммуникационные системы и сети: Учебное пособие. Том 1. Современные технологии. / Под ред. Профессора В. П. Шувалова. – М.: «Горячая линия», 2004. 249 с.

[4] Беликова И.С., Закалкин П.В., Стародубцев Ю.И., Сухорукова Е.В. Моделирование сетей связи с учетом топологических и структурных неоднородностей // Информационные системы и технологии. 2017. № 2 (100). С. 93-101.

[5] Пат. РФ № 2488165 / Д.А. Агеев, О.А. Баленко, В.В. Бухарин, Е.А. Жилков, А.В. Кирьянов, А.К. Сагдеев, Ю.И. Стародубцев. Способ моделирования сетей связи; Опубл. 20.07.2013.