DOI:

РАЗРАБОТКА МАТЕМАТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ВЫСОКОТЕХНОЛОГИЧНЫХ ЗДАНИЙ

Гребенюк Г.Г., Никишов С.М., Середа Л.А., Рощин А.А.
Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва, ул. Профсоюзная д.65
grebenuk@lab49.ru, nikishov@lab49.ru, sereda@lab49.ru, rochinaa@mail.ru

Аннотация: Для обеспечения безопасности жилых и нежилых высотных зданий, торговых центров, промышленных предприятий, оснащенных сложной инженерной инфраструктурой (системами тепло-, водо-, электроснабжения, вентиляции, IT-системами и др.) рассматриваются математические модели и алгоритмы взаимодействия сетевых инженерных систем при отказах или преднамеренных действиях злоумышленников. Особое внимание уделено распространению последствий отказа по инфраструктуре и поиску объектов, наиболее важных как для функционирования отдельных инженерных систем, так и для инфраструктуры в целом. Указанные модели апробированы на примере гетерогенной инженерной инфраструктуры здания научно-технического назначения, состоящей из трех инженерных систем. В процессе моделирования для каждого сценария рассчитан показатель влияния каждого узла. В результате проведенных расчетов найден критически важный объект для рассматриваемой инженерной инфраструктуры.

Ключевые слова: моделирование, безопасность, уязвимость, ущерб, критически важные элементы сетей.

Введение

Городская инфраструктура включает в себя большое количество различных объектов, таких как жилые и нежилые высотные здания, торговые центры, промышленные предприятия, стадионы и пр. Их функционирование обеспечивается сложными инженерными системами тепло-, водо-, электроснабжения, вентиляции, IT - системами и др. Рассматриваемые объекты характеризуются значительной стоимостью активов и высокой концентрацией людей, обеспечение безопасности которых является первоочередной задачей. Старение оборудования, отключения от внешних источников энергии, случайные отказы или действия злоумышленников представляют собой угрозы, реализация которых влияет на безопасность, сохранность материальных активов и др. При наличии угроз важно выполнить анализ уязвимостей системы по отношению к ним и затем оценку ущерба, если угроза была реализована. По ущербу и вероятности наступления инициирующих событий оценивается риск реализации угрозы.

Как правило, анализ уязвимостей инженерной инфраструктуры проводится для отдельных систем, без учета их взаимного влияния друг на друга. Однако, благодаря автоматизации процессов инженерного обеспечения, процессов управления, внедрению информационных технологий и т.д. взаимное влияние систем, входящих в инженерные инфраструктуры, все больше усиливается, и этот фактор нельзя не учитывать при анализе безопасности высокотехнологичных зданий.

1 Оценка взаимовлияния систем инфраструктуры от воздействия инициирующего события

Вследствие отказа переменные состояния систем, входящих в инфраструктуру, переходят от начального состояния $x_{11}^0, x_{21}^0, \dots x_{к1}^0$, $x_{12}^0, x_{22}^0, \dots x_{r2}^0, x_{1n}^0, x_{2n}^0, \dots x_{mn}^0$ в конечное состояние $x_{11}^1, x_{21}^1, \dots x_{к1}^1$, $x_{12}^1, x_{22}^1, \dots x_{r2}^1, x_{1n}^1, x_{2n}^1, \dots x_{mn}^1$, (где k, r, m – количество переменных состояния соответственно в 1-й, 2-й, n-ой системах). Если значения переменных в конечном состоянии выходят за допустимые пределы, то система оказывается функционально или физически уязвимой к инициирующему событию и становится неработоспособной [1].

Для получения точной оценки значений переменных состояния необходимо выполнить моделирование с использованием подробных математических моделей. Анализ результатов моделирования позволяет эксперту определить вид уязвимости (физический или функциональный), ожидаемое время восстановления и ущерб, нанесенный инициирующим событием.

На практике, при отсутствии точных математических моделей, описывающих процессы в сложных инфраструктурах, качественные оценки влияния инициирующих событий на элементы инженерных систем получают, используя топологические модели. В такой модели структура системы описывается матрицей смежности с логическими значениями 0 или 1 в зависимости от наличия или отсутствия связи между ее элементами, а неработоспособности узлов определяются из входо-выходной модели В. Леонтьева [2]:

$$(1)\ q = [I - A^T]^{-1} \cdot c,$$

где c – вектор сценариев размерности n x 1, с помощью которого задаются воздействия на систему ($c_i = 0$ для работоспособного i-го узла и $c_i = 1$ для инициирующего события с потерей работоспособности i-го узла); A – матрица смежности размерности $n\,x\,n$, отражающая взаимозависимости объектов системы, I – единичная матрица размерности $n\,x\,n$; q – вектор размерности $n\,x\,1$, являясь реакцией системы (1) на воздействия с, характеризует степень взаимовлияния узлов систем, входящих в инфраструктуру.

Для i-го узла q_i является показателем влияния отказа любого j-го узла инфраструктуры, задаваемого сценарием c_j=1. Значение показателя влияния характеризует критичность i-го узла, т.е. степень влияния события c_j=1 на i-ый узел (1).

Значения элементов матрицы A равны 0 либо 1. Если $a_{ij} = 0$, то это означает, что j-ый узел системы не зависит от i-го узла системы. Напротив, если $a_{ij} = 1$, то j-ый узел полностью зависит от i-го узла, и отказ i-го узла приведет к полной неработоспособности j-го узла.

Взаимосвязь систем обеспечивается через объекты, относящиеся одновременно к разным системам (далее «пограничные»).

В этой статье изменение работоспособности узла определяется по принадлежности к пути распространения последствий инициирующего события в графе инфраструктуры. Узел рассматривается как неработоспособный, если он находится на этом пути. Поиск траектории распространения и неработоспособных узлов выполняется в соответствии с разделом 2.

С использованием топологической модели представляет интерес оценить показатель влияния q вследствие взаимодействия систем разной природы. В «пограничных» узлах инженерной системы содержатся компоненты разной физической природы (электрические, гидравлические и др.), каждый из которых связан с соответствующей инженерной системой.

Топология инфраструктуры и место в ней начального события определяют траекторию распространения этого события и включаемые в нее «пограничные» узлы. Один или несколько нефункциональных компонентов появляются в узле, который является "пограничным", в зависимости от текущей траектории.

Появление на траектории одного и того же «пограничного» узла может быть разнесено во времени и вызываться различными взаимодействующими системами. Показатель влияния таких многокомпонентных узлов зависит от неработоспособности входящих в них компонент и должен увеличиваться с появлением новых неработоспособных компонент этого узла.

Увеличение показателя влияния происходит не только в «пограничных» узлах, но и в узлах внутри одной системы вследствие потери работоспособности смежных с ним узлов. Прямое применение указанной модели В. Леонтьева не позволяет выявить и визуализировать траекторию распространения последствий инициирующего события. Ниже рассмотрен подход, использующий поиск траектории распространения на графе инфраструктуры, сопровождающийся расчетом показателя влияния инфраструктуры. Применение входо-выходной модели В. Леонтьева с логической матрицей смежности всей инженерной инфраструктуры дает аналогичный результат при расчете вектора q.

2 Представление инженерной инфраструктуры в виде многослойной модели

В литературе [3 - 5] инженерные инфраструктуры, состоящие из нескольких инженерных систем, принято представлять в виде многослойной модели – “слоеного пирога”. При этом каждой инженерной системе соответствует слой, в котором располагаются ее объекты и коммуникации. Взаимосвязь систем обеспечивается через объекты, относящиеся одновременно к разным системам. Так сервер относится к IT-системе и одновременно к системе электроснабжения, будучи потребителем электроэнергии.

Рассмотрим пример гетерогенной инфраструктуры, состоящей из 16 узлов (рис. 1). Эта инфраструктура включает 3 инженерные системы: электроснабжения (обозначена штрих – пунктирными линиями), водоснабжения (обозначена пунктиром) и IT (обозначена сплошными линиями).

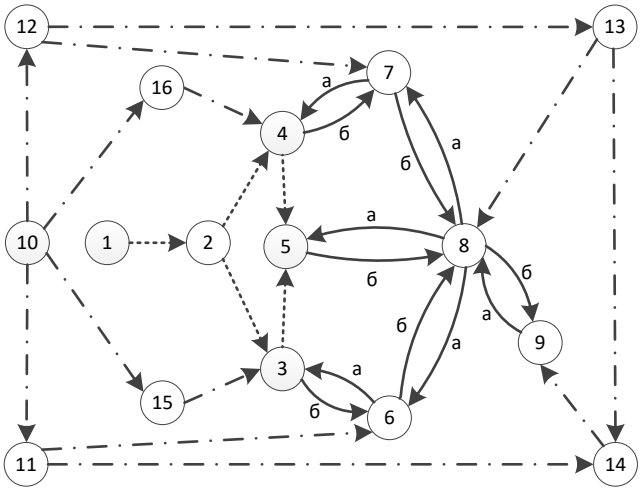

Рис. 1. Пример гетерогенной инфраструктуры

Изобразим данную инфраструктуру в виде многослойной модели. Каждой из 3 инженерных систем соответствует свой слой (рис. 2).

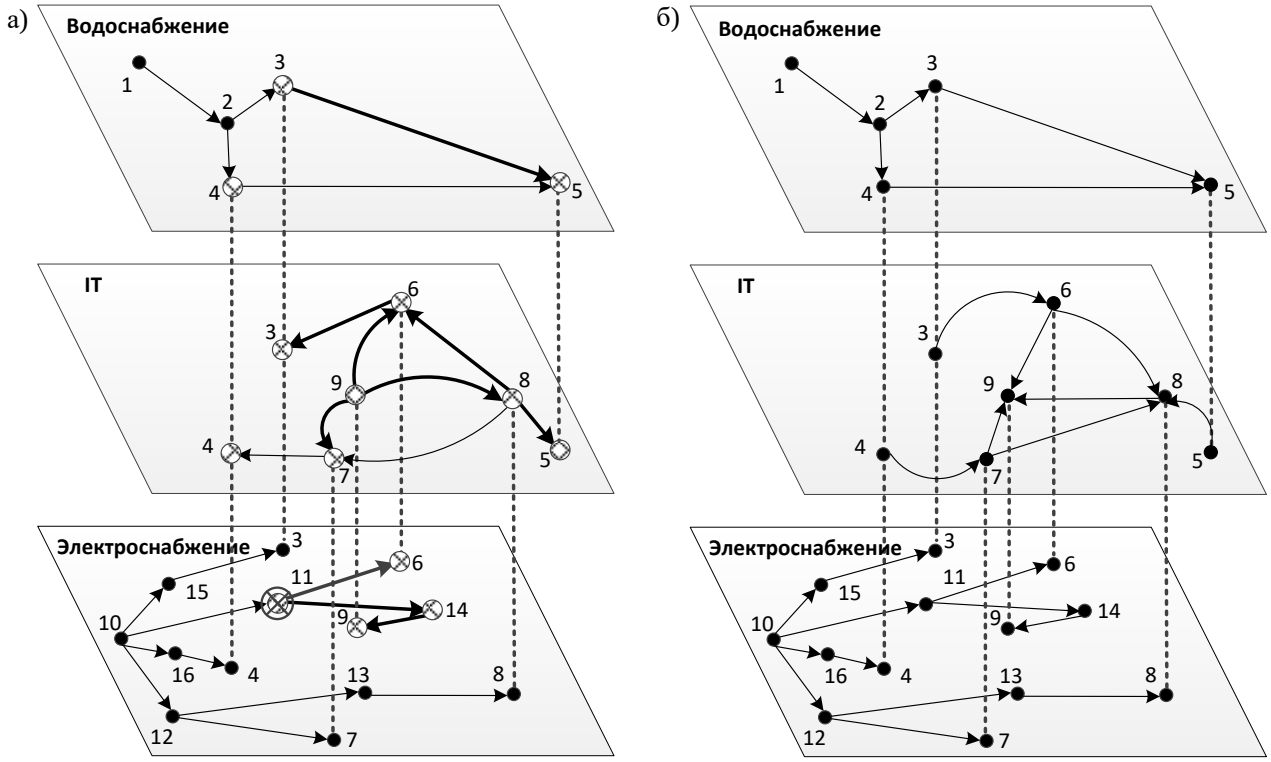

Рис. 2. Гетерогенная инженерная система в виде многослойной модели при различных режимах IT - системы: а) IT-система в режиме сбора данных, б) IT- система в режиме передачи управляющих команд

На слое электроснабжения размещены электрический ввод от внешней электрической сети (узел 10), «запитанные» от него электрические автоматы (узлы 11, 12, 13, 14, 15, 16) и подключенные к автоматам потребители электроэнергии: насосы (узлы 3, 4), коммутаторы (узлы 6, 7, 8), сервер (узел 9).

На слое водоснабжения располагается водонапорный бак (узел 1), вода из которого поступает в коллектор (узел 2) и доставляется потребителю (узел 5) насосами (узлы 3, 4).

IT-система расположена в одноименном слое, работает в двух режимах: режиме сбора данных (рис. 2а) и режиме передачи управляющих команд (рис. 2б). В первом режиме данные собираются с насосов (узлы 3,4) и потребителя (узел 5) и с помощью коммутаторов (узлы 6, 7, 8) передаются на сервер (узел 9). Во втором режиме сервер (узел 9) через коммутаторы (узлы 6, 7, 8) передает управляющие команды насосам (узлы 3,4) и потребителю (узел 5).

Через «пограничные» объекты, принадлежащие нескольким системам, осуществляются взаимодействия между ними. Например, насосы (узлы 3,4) являются одновременно потребителями в системе электроснабжения, основными узлами системы водоснабжения, источниками данных для IT-системы в режиме сбора данных и потребителями данных (команд управления) IT-системы в режиме передачи управляющих команд. На рис. 2 те объекты инфраструктуры, которые одновременно принадлежат нескольким взаимодействующим инженерным системам, соединены пунктирными линиями.

3 Модель распространения последствий отказа по инженерной инфраструктуре

Для распространения последствий отказа используется модель в виде ориентированного графа. Каждая система представляется как отдельный подграф этого графа, в котором выделяются три типа вершин: источники энергии и ресурса, сетевые узлы и потребители энергии и ресурса. Источниками в зданиях являются вводы от внешних сетей или автономные источники ресурсов.

В одном из известных подходов для решения задачи на многослойной модели необходимо записать матрицы смежности для каждого из слоев A_{el}, A_{IT}, A_w, а также матрицы, отражающие взаимозависимости между слоями $I_{el\to IT}$, $I_{IT\to w}$. Примеры матриц A_{el} и $I_{el\to IT}$ приведены на рис. 3.

а)

	3	4	6	7	8	9	10	11	12	13	14	15	16
3	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	1	1	0	0	1	1
11	0	0	1	0	0	0	0	0	0	0	1	0	0
12	0	0	0	1	0	0	0	0	0	1	0	0	0
13	0	0	0	0	1	0	0	0	0	0	0	0	0
14	0	0	0	0	0	1	0	0	0	0	0	0	0
15	1	0	0	0	0	0	0	0	0	0	0	0	0
16	0	1	0	0	0	0	0	0	0	0	0	0	0

б)

	3	4	6	7	8	9	10	11	12	13	14	15	16
3	1	0	0	0	0	0	0	0	0	0	0	0	0
4	0	1	0	0	0	0	0	0	0	0	0	0	0
6	0	0	1	0	0	0	0	0	0	0	0	0	0
7	0	0	0	1	0	0	0	0	0	0	0	0	0
8	0	0	0	0	1	0	0	0	0	0	0	0	0
9	0	0	0	0	0	1	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0

Рис. 3. Примеры матриц: а) матрица A_{el}, б) $I_{el\to IT}$

На первом шаге выбирается произвольный слой, содержащий хотя бы один узел, на который оказывает влияние вектор сценария c. Например, если поврежден узел 10, то – слой электроснабжения. Записывается вектор сценария c_{el}. Затем, по формуле (1) находится вектор повреждений q_{el}.

На втором шаге выбирается один из нерассмотренных слоев (в данном случае, IT). Рассчитывается вектор сценария влияния электроснабжения на IT

$$(2)\quad c_{el\to IT} = I_{el\to IT} \cdot q_{el} + c_w.$$

По формуле (1) вычисляется значение q_{IT}.

После рассмотрения всех слоев и учета всех зависимостей записывается финальный вектор q, элементы которого содержат максимальные значения повреждений из векторов для всех слоев.

Другим удобным способом описания каждого подграфа являются списки смежности. Сценарием задаются инициирующие события - отказы объектов систем (узлов графа). От отказавшего узла одной из систем в соответствии с ее списком смежности происходит распространение последствий отказа к другим узлам этой системы. Распространение вызывает появление новых отказов и доходит до «пограничных» узлов, которые принадлежат взаимодействующим системам.

Специальная программа-диспетчер формирует траекторию распространения последствий начального отказа в системе и при достижении ею «пограничного» узла дает команду на распространение воздействия по соседней системе вплоть до включения в траекторию следующего «пограничного» узла и так далее. В программе используется подход к построению траекторий распространения воздействий, изложенный в [6], который является эффективным для инфраструктуры, содержащей десятки и сотни потребителей в каждой инженерной системе. Этот подход использует свойства распределительных сетей, такие как разомкнутая структура электроснабжения, снабжение каждого потребителя от одного источника, в то время как один источник может снабжать энергией или ресурсами многих потребителей. Как правило, данные свойства выполняются для большинства распределительных сетей. Действие алгоритма, использующего указанные свойства распределительных сетей, создает безызбыточные сетевые конфигурации. Программа-диспетчер

получает данные от информационной учетной системы, которая содержит базу данных (БД), реестр объектов и их характеристик.

Рассмотрим один из сценариев распространения последствий отказа. На рис. 2а жирными линиями показано распространение отказа узла 11. Серыми заштрихованными кружками показаны узлы, на которые распространился отказ.

Вектор влияния будем обозначать через q. Для рассматриваемого сценария с отказом узла 11 примем $q_{11} = 1$. Воздействие от отказа узла 11 распространяется в системе электроснабжения, в результате чего отключаются от питания узел 14 ($q_{14} = q_{11} = 1$) и узел 6 ($q_6 = 1$). Воздействие отказа узла 14 распространяется на «пограничный» узел 9 ($q_9 = q_{14} = 1$). Затем отказ узла 9 распространяется по IT-системе на узел 8 ($q_8 = q_9 = 1$). Показатель влияния многокомпонентного узла 6 увеличивается, так как помимо потери питания от узла 11, происходит потеря работоспособности смежного с ним узла 8 в IT-системе ($q_6 = q_{11} + q_8 = 2$). Воздействие отказа узла 8 также распространяется на узел 7 ($q_7 = q_8 = 1$), а затем на узел 4 ($q_4 = q_7 = 1$). Показатель влияния узла 3 определяется в результате распространения отказа узла 6 ($q_3 = q_6 = 2$). Показатель влияния многокомпонентного узла 5 накапливается за счет прекращения подачи воды от смежных с ним узлов 3 и 4 в системе водоснабжения, а также отказа узла 8 в IT-системе ($q_5 = q_3 + q_4 + q_8 = 4$).

Суммарное значение показателя влияния всей инфраструктуры для сценария c_i рассчитывается по формуле:

$$(3)\ S_i = \sum_{j=1}^{n} q_j,$$

где n – общее количество узлов в инфраструктуре.

S_i указывает на степень влияния узла i на устойчивость функционирования инфраструктуры и, тем самым, определяет важность узла для инфраструктуры.

В таблице 1 представлены значения показателя влияния для сценариев с отказами всех узлов инженерной инфраструктуры рис. 1 при двух режимах IT - системы. Показатели влияния приведены в относительных единицах, по отношению к сумме максимальных значений показателя влияния.

Таблица 1. Показатели влияния инженерной инфраструктуры здания для двух режимов IT - системы

№ узла	Показатель влияния		№ узла	Показатель влияния	
	Режим 1	Режим 2		Режим 1	Режим 2
1	0.0480	0.1322	9	0.0720	0.0083
2	0.0400	0.1240	10	0.2720	0.2479
3	0.0160	0.0579	11	0.1120	0.0496
4	0.0160	0.0579	12	0.1040	0.0579
5	0.0080	0.0248	13	0.0720	0.0248
6	0.0240	0.0248	14	0.0800	0.0165
7	0.0240	0.0248	15	0.0240	0.0661
8	0.0640	0.0165	16	0.0240	0.0661

При построении графика (рис. 4) использовались максимальные значения показателя влияния среди двух режимов IT – системы.

Как видно из рис. 4, взаимные влияния в инженерной инфраструктуре наиболее значительны при реализации сценария с отказом узла 10, который является критически важным для рассматриваемой системы.

Рис. 4. График зависимости показателя влияния системы от отказов элементов инженерной инфраструктуры здания

4 Учет сложных зависимостей работоспособности узла от питающих сетей

В рассмотренном выше подходе отказ всегда распространяется через «пограничные» объекты, принадлежащие нескольким системам: если отказ в какой-либо системе достигает такого узла, программа-диспетчер автоматически продолжает траекторию распространения в других системах, содержащих этот же объект. В большинстве случаев это верно: насос системы водоснабжения, например, теряет работоспособность и при прекращении подачи воды, и при отключении от электричества, т. е. если воздействие достигнет его узла в любой из систем, к которым он принадлежит. Однако, существуют объекты, которые могут продолжать работать, даже если отказала часть из их «питающих» систем. Например, газомазутный котел в системе теплоснабжения может работать и на газе, и на мазуте, поэтому, если соответствующий ему узел графовой модели попал в траекторию распространения отказа в системе газоснабжения, отказ не должен распространяться на систему теплоснабжения до тех пор, пока воздействие не достигнет этого же узла и в системе снабжения мазутом. Если этого не случится, котел останется работоспособным, и не распространит воздействие на узлы в слое теплоснабжения. Однако, если к котлу прекратится подача воды, он потеряет работоспособность независимо от того, сохранилось ли его питание газом или мазутом, т. е. из слоя водоснабжения последствия отказа распространяются на слой теплоснабжения через «пограничный» узел котла всегда, без каких-либо дополнительных условий.

Для учета таких ситуаций целесообразно сопоставить каждому «пограничному» узлу логическую (булеву) функцию работоспособности, определяющую, при каких условиях он распространяет последствия отказа дальше. Входами этой функции служат признаки отсутствия воздействия на узел в каждой из систем, в которых он содержится, а выходом – признак работоспособности соответствующего объекта в целом, во всех системах. Такая функция может записываться с помощью операторов “И” и “ИЛИ” и должна храниться среди прочих характеристик объекта в информационной учетной системе, к которой обращается программа-диспетчер. Для узлов, не являющихся «пограничными», такая функция, очевидно, не требуется: они принадлежат только одному слою графовой модели и всегда распространяют отказ в своем слое.

Газомазутному котлу, который упоминался выше, будет соответствовать следующая функция:

$$(4)\ r_i = r_i^{\text{хв}} \wedge \left(r_i^{\text{газ}} \vee r_i^{\text{мазут}}\right),$$

где *i* – номер узла котла в графе инфраструктуры; r_i – признак работоспособности узла в целом; $r_i^{хв}$ – признак отсутствия воздействия на узел в системе водоснабжения; $r_i^{газ}$ – признак отсутствия воздействия на узел в системе газоснабжения; $r_i^{мазут}$ – признак отсутствия воздействия на узел в системе снабжения мазутом.

Эту функцию можно прочесть следующим образом: «котел работоспособен, если он подключен к водоснабжению, и при этом получает газ или мазут».

Для упрощения программы-диспетчера можно хранить функцию работоспособности узла в базе данных информационной учетной системы в виде КНФ (конъюнктивной нормальной формы). Фактически, достаточно хранить множество множеств номеров слоев модели инфраструктуры: узел будет считаться работоспособным, если среди всех хранимых для него множеств номеров слоев нет ни одного, в котором на узел оказывается воздействие во всех слоях этого множества. Для газомазутного котла в базе данных будет храниться множество множеств «{ {хв}, {газ, мазут} }».

В этом подходе программа-диспетчер, достигнув «пограничного» узла в процессе построения траектории распространения последствий отказа, вычисляет для него функцию работоспособности, и распространяет воздействие на соседнюю систему через этот узел только в том случае, если вычисленное значение ложно. При этом программе необходимо возвращаться к уже просмотренным слоям, поскольку здесь возможны «отложенные» последствия: при анализе системы газоснабжения котел, как «пограничный» узел, мог не распространить последствия отказа на систему теплоснабжения, поскольку снабжение мазутом на данный момент считается сохранившимся. Однако, первоначальный отказ может через несколько слоев распространиться и на систему снабжения мазутом, и в этот момент нужно вернуться к системе теплоснабжения и пересчитать функцию работоспособности для котла. Технически проще всего циклически перебирать слои инфраструктуры и пересчитывать функции работоспособности с изменившимися входами до тех пор, пока хотя бы в одном из слоев происходит распространение последствий отказа.

Заключение

Для повышения безопасности высокотехнологиченых зданий, оснащенных сложной инженерной инфраструктурой, разработано математическое и программное обеспечение, включающие комплекс моделей и алгоритмов, БД объектов и их характеристик.

Комплекс моделей и алгоритмов используется при сценарном моделировании последствий инициирующих событий для решения задач поиска и визуализации траекторий распространения последствий отказов, оценки показателя влияния элементов инфраструктуры, определения ее критически важных элементов.

Указанные модели и алгоритмы апробированы на фрагменте реальной инфраструктуры здания научно-технического назначения.

Литература

1. *Махутов Н.А., Резников Д.О.* Оценка уязвимости технических систем и ее место в процедуре анализа риска//Проблемы анализа риска. 2008. Том 5, № 3. — С. 76–89.
2. *Haimes Y.Y., Jiang P.* Leontief-Based Model of Risk in Complex Interconnected Infrastructures // Journal of Infrastructure Systems. - 2001, Vol. 7, No. 1, P. 23-27.
3. *Milanović J.V., Wentao Zhu* Cyber-physical system failure analysis based on Complex Network theory// IEEE EUROCON 2017 – 17th International Conference on Smart Technologies. Ohrid, Macedonia, 2017. https://ieeexplore.ieee.org/document/8011177.
4. *Kurant, M., & Thiran, P.* Layered complex networks. Physical Review Letters, 96(13), 138701-1-138701-4.
5. *Махутов Н.А., Резников Д.О., Петров В.П.* Особенности обеспечения безопасности критических инфраструктур// Безопасность в техносфере : науч.-метод. и информ. журнал. - 2014. - N 1. - С. 3-14.
6. *Grebenyuk G. G., Krygin A. A.* Limit graphs in structural optimization of modes in distribution networks // Automation and Remote Control. 2015. №76 (1). – P.120-132