УДК 65.012.123

О. Е. ФЕДОРОВИЧ[1], Н. В. ЕРЕМЕНКО[1], В. А. ПУЙДЕНКО[2]

[1] *Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина*
[2] *Харьковский радиотехнический техникум, Украина*

ИССЛЕДОВАНИЕ УГРОЗ И УЯЗВИМОСТЕЙ В КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЕ ТЕХНОГЕННЫХ ОБЪЕКТОВ И СИСТЕМ

Сформулирована и решена задача исследования угроз в критических инфраструктурах (КИ) технических объектов и систем (ТОС). Предложены методы: выбора рационального варианта проведения мероприятий по нейтрализации угроз, минимизации ущерба в случае возникновения угроз. Разработана структура агентной имитационной модели для исследования влияния угроз и уязвимостей в КИ ТОС. Предложенный подход позволяет исключить риски, связанные с воздействием агрессивных внешних воздействий на инфраструктуру техногенных объектов, чтобы обеспечить их нормальное функционирование в условиях морального и физического старения.

Ключевые слова: *критическая инфраструктура, техногенная система, угрозы и уязвимости, проведение мероприятий, моделирование угроз.*

Введение

Техногенные объекты и системы (аэрокосмическое производство, металлургия, энергоснабжение и т.д.) для своего нормального функционирования должны иметь достаточно надёжную инфраструктуру, с помощью которой, сырье, материалы, электроэнергия беспрерывно поступают в производство. Нарушение работы и сбои в критической инфраструктуре (КИ) могут приводить к остановкам техногенных объектов и систем (ТОС), а для ответственных (категорийных) объектов (электростанции, очистные сооружения и т.д.) к их деградации и возможному разрушению. К тому же, множество угроз, связанных с нарушением инфраструктуры и наличием уязвимостей в ТОС, за последние годы расширилось, путём добавления к традиционным (физические нарушения, отказы оборудования, сбои системы управления и др.) новых уязвимостей (террористические акты, блокировки, кибератаки и др.).

Поэтому актуальная тема предлагаемой публикации, в которой ставится и решается задача исследования влияния угроз и уязвимостей на функционирование критической инфраструктуры ТОС.

Постановка задачи исследования

Для решения задачи исследования выделены следующие основные этапы:

1. Выявление существующих факторов, влияющих на уязвимость критической инфраструктуры ТОС.

2. Выбор и обоснование рационального варианта превентивных мероприятий для уменьшения возможных ущербов в критической инфраструктуре ТОС.

3. Моделирование угроз и уязвимостей в критической инфраструктуре ТОС.

Решение задачи исследования

1. Выявление существенных факторов, влияющих на уязвимость критической инфраструктуры ТОС.

Для выделения существующих факторов, воспользуемся методом теории экспериментов, а точнее полнофакторным планированием (ПФЭ). Эксперты, специалисты по оценке угроз и уязвимостей, должны для конкретного техногенного объекта определить критическую инфраструктуру (КИ) и возможное множество факторов (угроз), влияющих на нормальное функционирование ТОС.

Далее необходимо сформировать план ПФЭ, в котором факторы принимают «два значения» $(+1,-1)$. Наличие «$+1$» в i-й строке плана будет означать наличие воздействия j-й угрозы на КИ ТОС. В противном случае, «-1» – означает отсутствие такой угрозы. Так как количество строк ПФЭ $N = 2^n$, (где n – количество возможных угроз), то в плане осуществляется полный перебор факторов и их комбинаций. При планировании возникновения угроз специалисты в области чрезвычайных ситуаций должны дать прогнозируемую оценку ущербов для каждой сроки ПФЭ и тем самым сформировать вектор-столбец значений ущербов КИ ТОС на угрозы.

Рассмотрим иллюстрированный пример. Пусть множество угроз соответствует трём факторам (блокировка железной дороги (ЖД), террористический акт, кибератака на систему управления ЖД). Сформулируем ПФЭ с $n = 3$ факторами и $N = 2^3 = 8$ откликами. Представим прогностические оценки экспертов ущербов от угроз в бальной шкале $(0 \div 10)$.

Пусть фактор x_1 соответствует блокировке ЖД, x_2 – теракт, x_3 – кибератака на систему управления ЖД. Соответствующий план ПФЭ с прогнозными оценками угроз представлен на рис. 1.

№	Факторы			Отклики			
	x_1	x_2	x_3	y	x_1x_2	x_1x_3	x_2x_3
1	-1	-1	-1	0	+1	+1	+1
2	-1	-1	+1	3	+1	-1	-1
3	-1	+1	-1	4	-1	+1	-1
4	-1	+1	+1	7	-1	-1	+1
5	+1	-1	-1	5	-1	-1	+1
6	+1	-1	+1	8	-1	+1	-1
7	+1	+1	-1	9	+1	-1	-1
8	+1	+1	+1	10	+1	+1	+1

Рис. 1. ПФЭ для трёх угроз

С помощью расчётных формул ПФЭ можно получить неполноквадратичную регрессионную модель вида:

$$\begin{aligned} y &= b_0 + b_1 \cdot x_1 + b_2 \cdot x_2 + b_3 \cdot x_3 + b_{12} \cdot x_1 \cdot x_2 + \\ &+ b_{13} \cdot x_1 \cdot x_3 + b_2 \cdot x_2 \cdot x_3 + b_{123} \cdot x_1 \cdot x_2 \cdot x_3 = \\ &= 5,75 + 2,25 \cdot x_1 + 1,75 \cdot x_2 + 1,25 \cdot x_3 - 0,25 \cdot x_1 \cdot x_2 - \\ &- 0,25 \cdot x_1 \cdot x_3 - 0,25 \cdot x_2 \cdot x_3 - 0,25 \cdot x_1 \cdot x_2 \cdot x_3. \end{aligned}$$

Выделим существующие факторы, обуславливающие уровень угроз. Самым существенным фактором в примере является x_1 – блокировка ЖД, на втором месте x_2 – теракт, и на третьем месте x_3 – кибератака на систему управления ЖД. Совместное воздействие факторов маловероятно по сравнению с основными факторами и оценивается в виде произведения факторов. Выбор существующих факторов позволит в дальнейшем обосновать мероприятия по уменьшению их влияния или возможную их нейтрализацию в КИ ТОС.

2. Выбор и обоснование рационального варианта превентивных мероприятий для уменьшения возможных ущербов в критической инфраструктуре ТОС. Выявленные на первом этапе существенные факторы угроз позволяют сосредоточиться на обосновании мероприятий, связанных с их нейтрализацией.

Для угрозы «блокировка ЖД», пусть такими мероприятиями (для примера) будут: политическое решение, проведение референдума, силовое решение. Возможны комбинации этих мероприятий. Тогда общее количество вариантов возможных вариантов мероприятий $N = 2^n$, где $n = 3$.

Сформируем набор показателей для оценки эффективности проведения возможных мероприятий по устранению угроз. Такими показателями могут быть: y_1 – возможный ущерб от угрозы; y_2 – затраты на проведение мероприятий по нейтрализации (уменьшению) угрозы; y_3 – время, затраченное на нейтрализацию угрозы; y_4 – риск выполнения мероприятий.

Представим значение показателей в виде значений лингвистических переменных (букв латинского алфавита):

$$y_1 = \begin{cases} A - \text{большой ущерб от угрозы;} \\ B - \text{средний ущерб;} \\ C - \text{минимальный ущерб.} \end{cases}$$

$$y_2 = \begin{cases} A - \text{малые затраты} \\ \text{на нейтрализацию угрозы;} \\ B - \text{средние затраты;} \\ C - \text{большие затраты.} \end{cases}$$

$$y_3 = \begin{cases} A - \text{небольшое время,} \\ \text{затраченное на нейтрализацию угрозы;} \\ B - \text{среднее время;} \\ C - \text{длительный срок.} \end{cases}$$

$$y_4 = \begin{cases} A - \text{незначительный риск,} \\ B - \text{средний риск;} \\ C - \text{очень большой риск.} \end{cases}$$

Для формирования вариантов проведения возможных мероприятий по устранению угроз в КИ ТОС воспользуемся значениями двоичного счётчика. Для примера $n = 3$, поэтому количество состояний счётчика $N = 2^3 = 8$. На рис. 2 представлена таблица полного множества вариантов мероприятий. Здесь «1» означает проведение мероприятия, а «0» – не проведение мероприятия.

Пусть эксперты, для примера, определили важность показателей для оценки возможных вариантов мероприятий по нейтрализации угроз в КИ ТОС в виде ряда по убыванию важности показателей: y_1, y_2, y_3, y_4. Тогда, для поиска компромиссного варианта проведения мероприятий по нейтрализации угроз, с учётом противоречивости показателей, вос-

пользуемся лексикографическим упорядочиванием вариантов.

№	Мероприятия			Показатели мероприятий			
	x_1	x_2	x_3	y_1	y_2	y_3	y_4
1	0	0	0	C	C	C	C
2	0	0	1	B	B	B	A
3	0	1	0	A	B	B	B
4	0	1	1	A	A	A	B
5	1	0	0	B	B	B	A
6	1	0	1	B	C	C	B
7	1	1	0	A	C	C	C
8	1	1	1	A	C	C	C

Рис. 2. Полное множество мероприятий для нейтрализации угроз в КИ ТОС

Исходное множество вариантов с учётом значений показателей (см. рис. 2) имеет вид:

1. C, C, C, C
2. B, B, B, A
3. A, B, B, B
4. A, A, A, B
5. B, B, B, A
6. B, C, C, B
7. A, C, C, C
8. A, C, C, C

После лексикографического упорядочивания вариантов получим:

4. A, A, A, B
3. A, B, B, B
7. A, C, C, C
8. A, C, C, C
2. B, B, B, A
5. B, B, B, A
6. B, C, C, B
1. C, C, C, C

Отбросим варианты с наихудшими значениями показателей (для примера это значения лингвистических переменных – C). Получим:

4. A, A, A, B
3. A, B, B, B

Таким образом, для проведения мероприятий, направленных на устранение (нейтрализацию) угроз целесообразно воспользоваться 4 или 3 вариантом проведения мероприятий. В случае большой размерности задачи (сложная КИ, большое количество угроз и уязвимостей) воспользуемся методом целочисленной линейной оптимизации с булевыми переменными.

Введём переменную x_{ij}, которая принимает два значения: $x_{ij} = 1$, если для i-й угрозы, для её нейтрализации выбрано j-е мероприятие, в противном случае $x_{ij} = 0$. При этом возникает следующее условие:

$$\sum_{j=1}^{n_i} x_{ij} = 1,$$

что означает обязательный выбор мероприятия для нейтрализации i-й угрозы, где n_i – количество возможных мероприятий. Тогда, показатели для оценивания эффективности мероприятий, связанных с угрозами в КИ ТОС будут выглядеть следующим образом:

$$y_1 = \sum_{i=1}^{n}\sum_{j=1}^{n_i} u_{ij}x_{ij},$$

$$y_2 = \sum_{i=1}^{n}\sum_{j=1}^{n_i} z_{ij}x_{ij},$$

$$y_3 = \sum_{i=1}^{n}\sum_{j=1}^{n_i} t_{ij}x_{ij},$$

$$y_4 = \sum_{i=1}^{n}\sum_{j=1}^{n_i} r_{ij}x_{ij},$$

где u_{ij} – остаточный ущерб, который связан с возникновением i-й угрозы, после проведения j-го мероприятия (в случае полной нейтрализации i-й угрозы с помощью j-го мероприятия $u_{ij} = 0$); z_{ij} – затраты, связанные с проведением j-го мероприятия по устранению i-й угрозы; t_{ij} – время, затраченное на проведение j-го мероприятия по устранению i-й угрозы; r_{ij} – риск выполнения j-го мероприятия по устранению i-й угрозы;

Пусть, в качестве целевой функции используется возможный остаточный ущерб, который возникает после проведения всех мероприятий по устранению множества угроз в КИ ТОС. В ходе оптимизации необходимо минимизировать ущерб:

$$\min\ y_1,\ y_1 = \sum_{i=1}^{n}\sum_{j=1}^{n_i} u_{ij}x_{ij},$$

с учётом выполнения следующих ограничений:

$$y_2 \le y_2^{'},\ y_2 = \sum_{i=1}^{n}\sum_{j=1}^{n_i} z_{ij}x_{ij},$$

$$y_3 \le y_3^{'},\ y_3 = \sum_{i=1}^{n}\sum_{j=1}^{n_i} t_{ij}x_{ij},$$

$$y_4 \le y_4^{'},\ y_4 = \sum_{i=1}^{n}\sum_{j=1}^{n_i} r_{ij}x_{ij},$$

$$\sum_{i=1}^{n_i} x_{ij} = 1,\ \sum_{i=1}^{n}\sum_{j=1}^{n_i} = n,$$

где $y_2^{'}$, $y_3^{'}$, $y_4^{'}$ – ограничения, связанные с затратами, временем (сроки) и рисками проведения мероприятий по нейтрализации угроз в КИ ТОС.

3. Моделирование угроз и уязвимостей в критической инфраструктуре ТОС. Для моделирования воздействия угроз воспользуемся методом агентного имитационного моделирования. Определим множество агентов в имитационной системе:

– «агент–КИ ТОС» – описывает состав и структуру КИ ТС;

– «агент–угроза», используется для инициации возможной угрозы; формируется в виде заявки по заданному закону распределения (возможно использовать статистику возникновения угроз для конкретных ТОС);

– «агент–уязвимость» – указывает на «слабое» место в ТОС при возникновении соответствующей угрозы (место указывается заранее в описании структуры ТОС);

– «агент–транспортировка» имитирует транспортировку грузов в КИ ТОС;

– «агент–складирование» имитирует складирование грузов в КИ ТОС;

– «агент–производство» имитирует производственный цикл в ТОС;

– «агент–ущерб» оценивает ущерб, возникающий в ходе реализации угроз в КИ ТОС;

– «агент–сценарий» описывает сценарий функционирования КИ ТОС в случае возникновения угроз;

– «агент–диспетчер» – управляет ходом событийного имитационного моделирования (системное время, список событий и т.д.);

– «агент–результаты» – используют для вывода промежуточных и окончательных результатов моделирования.

На рис. 3 представлена схема агентной имитационной модели для исследования КИ ТОС.

Выводы

Предложенный подход целесообразно использовать для исследования влияния угроз на критическую инфраструктуру техногенных объектов и систем. Это позволяет заблаговременно сформулировать и реализовать план превентивных мероприятий для уменьшения последствий реализуемых угроз в КИ ТОС, оценить возможные затраты, сроки, а также риски, связанные с выполнением комплекса предложенных мероприятий.

Литература

1. Геопространственные производственные системы. Часть 1. Анализ, моделирование, проектирование [Текст] : моногр. / О. Е. Федорович, В. М. Илюшко, О. Н. Замирец, Л. Д. Греков. – Х. : Нац. аэрокосм. ун-т «Харьк. авиац. ин-т», 2011. – 250 с.

2. Федорович, О. Е. Исследование логистики снабжения и сбыта в разнородной транспортной инфраструктуре грузоперевозок [Текст] : моногр. / О. Е. Федорович, Э. Е. Рубин, Н. В. Еременко. – Х. : Нац. аэрокосм. ун-т «Харьк. авиац. ин-т», 2016. – 198 с.

3. Федорович, О. Е. Модели и методы обеспечения качества в жизненном цикле и логистике высокотехнологического производства продукции развивающихся предприятий [Текст] : моногр. / О. Е. Федорович, Ю. Л. Прончаков, Ю. А. Лещенко. – Х. : ФОП Лысенко И. Б., 2017. – 255 с.

References

1. Fedorovich, O. E., Iljushko, V. M., Zamirec, O. N., Grekov, L. D. *Geoprostranstvennye proizvodstvennye sistemy. Chast' 1. Analiz, modelirovanie, proektirovanie* [Geospatial production systems. Part 1. Analysis, simulation, design]. Kharkov, Nac. ajero-kosm. un-t «Har'k. aviac. in-t», 2011. 250 p.

2. Fedorovich, O. E., Rubin, Je. E., Eremenko, N. V. *Issledovanie logistiki snabzhenija i sbyta v raznorodnoj transportnoj infrastructure gruzoperevozok* [Research of logistics of supply and sale in diverse transport infrastructure of a cargo transportation]. Kharkov, Nac. ajerokosm. un-t «Har'k. aviac. in-t», 2016. 198 p.

3. Fedorovich, O. E., Pronchakov, Ju. L. Leshchenko, Ju. A. *Modeli i metody obespechenija kachestva v zhiznennom cikle i logistike vysokotehnologicheskogo proizvodstva produkcii razvivajushhihsja predprijatij* [Models and methods of ensuring quality in life cycle and logistics of high-tech production of the developing enterprises]. Kharkov, FOP Lysenko I. B. Publ., 2017. 255 p.

Поступила в редакцию 12.02.2016, рассмотрена на редколлегии 15.03.2017

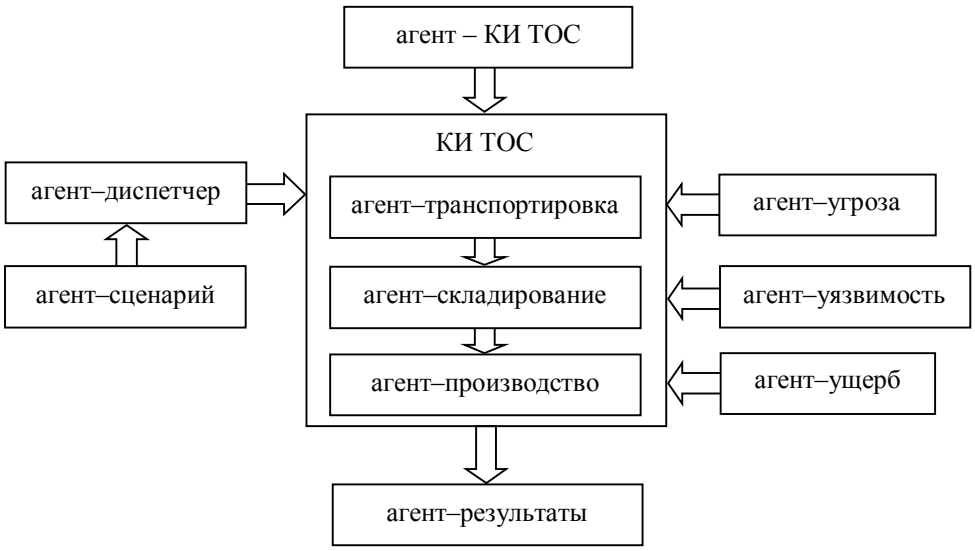

Рис. 3. Схема агентной имитационной модели для исследования угроз и уязвимостей в КИ ТОС

ДОСЛІДЖЕННЯ ЗАГРОЗ І ВРАЗЛИВОСТЕЙ У КРИТИЧНІЙ ІНФРАСТРУКТУРІ ТЕХНОГЕННИХ ОБ'ЄКТІВ І СИСТЕМ

О. Є. Федорович, Н. В. Єременко, В.О. Пуйденко

Сформульовано і вирішено задачу дослідження загроз у критичних інфраструктурах (КІ) технічних об'єктів і систем (ТОС). Запропоновано методи: вибору оптимального варіанта проведення методів по нейтралізації загроз, мінімізації збитку у разі виникнення загроз. Розроблено структуру агентної імітаційної моделі для дослідження впливу загроз і вразливостей в КІ ТОС. Запропонований підхід дозволяє виключити ризики, які пов'язано з впливом агресивних зовнішніх впливів на інфраструктуру техногенних об'єктів, щоб забезпечити їх нормальне функціонування в умовах морального та фізичного старіння.

Ключові слова: критична інфраструктура, техногенна система, загрози і вразливості, проведення заходів, моделювання загроз.

INVESTIGATION OF THREATS AND VULNERABILITY IN THE CRITICAL INFRASTRUCTURE OF TECHNOGENIC OBJECTS AND SYSTEMS

O. E. Fedorovich, N. V. Yeremenko, V. A. Puydenko

The problem of research of threats in critical infrastructures (CI) of technical objects and systems (TOS) is formulated and solved. The following methods are proposed: choosing an efficient option for carrying out the measures to neutralize the threats and minimize the damage in case of a threat. The structure of the agent simulation model to investigate the impact of threats and vulnerabilities in CI TOS is developed. The proposed approach allows eliminating the risks associated with the impact of aggressive external influences on the infrastructure of technogenic objects in order to ensure their normal functioning under conditions of moral and physical aging.

Keywords: critical infrastructure, technogenic system, threats and vulnerabilities, carrying out of measures, modeling of threats.

Федорович Олег Евгеньевич – д-р техн. наук, проф., зав. каф. информационных управляющих систем, Национальный аэрокосмический университет им. Н.Е. Жуковского «Харьковский авиационный институт», Харьков, Украина.

Еременко Наталия Валентиновна – канд. техн. наук, старший преподаватель каф. информационных управляющих систем, Национальный аэрокосмический университет им. Н.Е. Жуковского «Харьковский авиационный институт», Харьков, Украина.

Пуйденко Вадим Алексеевич– преподаватель компьютерных дисциплин, специалист первой категории, Харьковский радиотехнический техникум, Харьков, Украина.

Fedorovich Oleg Yevgenyevich – Doctor of Technical Sciences, Professor, Head of Information Management Systems Department, National Aerospace University «Kharkov Aviation Institute», Kharkov, Ukraine.

Yeremenko Nataliia Valentinovna– Candidate of Technical Science, the senior lecturer Department of Information Management Systems, National Aerospace University «Kharkov Aviation Institute, Kharkov», Ukraine.

Puydenko Vadim Alekseevich –Teacher of computer disciplines, Specialist of the first category, Kharkov Radio Technical School, Kharkov, Ukraine.