Научная статья
УДК 004.056.5; DOI: 10.61260/2218-13X-2025-1-94-108

ИССЛЕДОВАНИЕ АНТРОПОМОРФИЧЕСКИХ ВИДОВ ОРГАНИЗАЦИИ МЕЖОБЪЕКТНОГО ВЗАИМОДЕЙСТВИЯ НА УРОВНЕ СУБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

✉**Долженков Сергей Сергеевич;**
Максимова Елена Александровна.
МИРЭА – Российский технологический университет, Москва, Россия
✉***dolzhenkov@mirea.ru***

Аннотация. Представлены результаты исследования в области организации межобъектного взаимодействия на уровне субъекта критической информационной инфраструктуры с применением антропоморфического подхода. В качестве межобъектного взаимодействия рассмотрены уязвимости программного кода, обоснованы эффекты от межобъектного взаимодействия на уровне уязвимостей программного кода, возникающие в результате реализации поведенческих моделей. Они исследованы и обоснованы на основании антропоморфического подхода в формах: облигатного симбиоза, паразитизма, хищничества, аменсализма, аллелопатии, конкуренции, нейтрализма. Исследованы виды антропоморфизма в организации межобъектного взаимодействия на уровне критической информационной инфраструктуры. По результатам установлены новые закономерности в оценке рисков информационной безопасности. Взаимодействие уязвимостей программного кода может не только приводить к снижению работоспособности системы, но и возможны сценарии, при которых проявляется положительный эффект, то есть данную ситуацию можно использовать в качестве элемента системы защиты.

Ключевые слова: межобъектное взаимодействие, антропоморфический подход, критическая информационная инфраструктура, объект критической информационной инфраструктуры, моносубъектная система, уязвимости программного кода, динамика рисков

Для цитирования: Долженков С.С., Максимова Е.А. Исследование антропоморфических видов организации межобъектного взаимодействия на уровне субъекта критической информационной инфраструктуры // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2025. № 1. С. 94–108. DOI: 10.61260/2218-13X-2025-1-94-108.

Scientific article

STUDY OF ANTHROPOMORPHIC TYPES OF ORGANIZING INTER-OBJECT INTERACTION AT THE LEVEL OF THE SUBJECT OF CRITICAL INFORMATION INFRASTRUCTURE

✉**Dolzhenkov Sergey S.;**
Maksimova Elena A.
MIREA – Russian technological university, Moscow, Russia
✉***dolzhenkov@mirea.ru***

Abstract. The article presents the results of a study in the field of organizing inter-object interaction at the level of the subject of critical information infrastructure using the anthropomorphic approach. Vulnerabilities of program code are considered as inter-object interaction, the effects of inter-object interaction at the level of vulnerabilities of program code, arising as a result of the implementation of behavioral models, are substantiated. They are investigated and substantiated on the basis of the anthropomorphic approach in the form of: obligate symbiosis, parasitism, predation, amensalism, allelopathy, competition, neutralism. The types

of anthropomorphism in the organization of inter-object interaction at the level of critical information infrastructure are investigated. Based on the results, new patterns in the assessment of information security risks are established. The interaction of vulnerabilities of software code can lead not only to a decrease in the system's performance, but also scenarios are possible in which a positive effect is manifested, that is, this situation can be used as an element of the protection system.

Keywords: inter-object interaction, anthropomorphic approach, critical information infrastructure, object of critical information infrastructure, mono-subject system, vulnerabilities of software code, risk dynamics

For citation: Dolzhenkov S.S., Maksimova E.A. Study of anthropomorphic types of organization of inter-object interaction at the level of a subject of critical information infrastructure // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 1. P. 94–108. DOI: 10.61260/2218-13X-2025-1-94-108.

Введение

Современные тенденции развития информационных технологий предъявляют требования к процессу цифровизации компаниям реального сектора экономики, к которым, согласно Федеральному закону Российской Федерации от 2 июля 2013 г. № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях» [1], также относятся субъекты критической информационной инфраструктуры (СКИИ). Цифровизация процессов – сложный и многогранный процесс, составляющей частью которого является соблюдение политики информационной безопасности (ИБ), следовательно, это ключевой компонент поддержания целостности, работоспособности и отказоустойчивости информационных систем. Важно отметить, что прогнозируемо и безопасно осуществлять процессы цифровизации возможно принимая во внимание работу с уязвимостями на уровне программного кода объектов критической информационной инфраструктуры (ОКИИ) [2].

Организация межобъектного взаимодействия на уровне СКИИ играет важную роль в исполнении доктрины ИБ Российской Федерации. Следовательно, межобъектное взаимодействие является основой безопасности критической информационной инфраструктуры (КИИ) [3].

Отдельное внимание в процессах оптимизации информационных потоков на значимых объектах КИИ должно быть уделено динамике их поведения и угрозам на уровне программного обеспечения в разных типах взаимосвязей объектов. С этой целью будет использован антропоморфический подход [4]. Таким образом, целью данной работы является повышение уровня организации взаимодействия объектов КИИ за счёт использования антропоморфического эффекта от взаимодействия уязвимостей программного кода.

Для достижения поставленной цели необходимо рассмотреть организацию взаимодействия ОКИИ в рамках одного СКИИ, являющегося моносубъектной системой функционирования ОКИИ [5]. При этом необходимо учесть, что в границах одного СКИИ разные ОКИИ имеют различные типы связей: жесткие и гибкие, главные и второстепенные, внутренние и внешние, прямые, обратные и комбинированные связи, что приводит к радикально разным последствиям в результате их функционирующего взаимодействия.

Взаимодействие угроз

По результатам исследования [6–8] определены следующие виды связей межобъектного взаимодействия в СКИИ (рис. 1), основанные на антропоморфическом подходе (табл. 1).

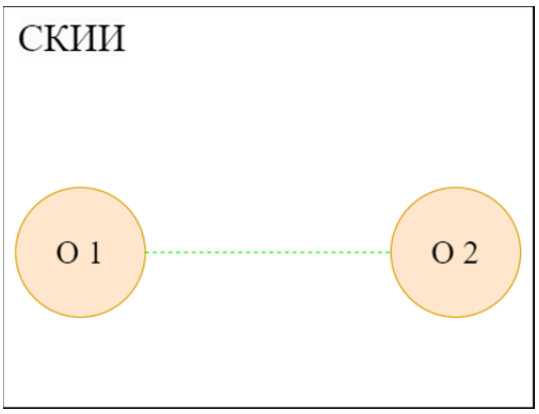

Рис. 1. **Базовая модель межобъектного взаимодействия на уровне СКИИ**

Таблица 1

Формы межобъектного взаимодействия на СКИИ

Симбиоз	Облигатный симбиоз	Взаимовыгода	Хотя бы один из объектов получает выгоду
	Паразитизм	Односторонняя выгода, продолжительное время нейтрально для второго объекта	
	Хищничество	Односторонняя выгода, уничтожение второго объекта	
Антибиоз	Аменсализм	Одностороннее отрицательное влияние, для второго объекта – нейтрально	Хотя бы один из объектов ограничивает возможности другого
	Аллелопатия	Двустороннее отрицательное влияние	
	Конкуренция	Взаимное уничтожение	
Нейтрализм		Объекты не оказывают взаимного влияния	

Применимо к СКИИ формы проявления симбиоза возможны в следующих случаях:

1. Облигатный симбиоз – взаимовыгодное существование объектов КИИ, при котором оба объекта взаимозависимы друг от друга, как следствие, образуется взаимовыгодная помощь.

2. Паразитизм – взаимодействие объектов СКИИ, при котором один из объектов не может существовать без частичного «поглощения» ресурсов второго, при этом второй объект может стабильно функционировать достаточно продолжительное время.

3. Хищничество – тип взаимодействия объектов СКИИ, при котором первый объект существует благодаря полному или частичному «поглощению» ресурсов второго, вплоть до его полного уничтожения. Существование первого объекта невозможно без «объекта-жертвы». Необходимо регулярное потребление ресурсов других объектов в рамках одного СКИИ [9].

Аналогично симбиотическим формам применимо к СКИИ рассмотрим возможные проявления антибиоза:

1. Аменсализм – форма антибиоза, при котором один объект СКИИ отрицательно влияет на другой, но сам не имеет ни положительных, ни отрицательных эффектов от оказанного влияния.

2. Аллелопатия – антибиотическое взаимодействие объектов СКИИ, при котором оба объекта получают отрицательный эффект от взаимодействия друг с другом, что обусловлено их функциональными параметрами.

3. Конкуренция – два объекта СКИИ являются инфраструктурными «врагами» по своей сути [10].

На основании вышеизложенного и табл. 1 выделены эффекты от видов связей межобъектного взаимодействия в СКИИ, основанные на антропоморфическом подходе для объектов Oi и Oj (табл. 2).

Таблица 2

Антропоморфические виды межобъектного взаимодействия на СКИИ*

Антропоморфические виды межобъектного взаимодействия на СКИИ	O_i	O_j
Облигатный симбиоз	+ / +	+ / +
Паразитизм	+ / -	- / +
Хищничество	+ / -	- / +
Аменсализм	0 / -	- / 0
Аллелопатия	- / -	- / -
Конкуренция	- / -	- / -
Нейтрализм	0	0

*В таблице «+» – положительный эффект; «+ / -» – положительный эффект у объекта O_i при отрицательном эффекте у объекта O_j; «- / +» – наличие отрицательного эффекта у объекта O_i при положительном эффекте у объекта O_j; «- / 0» – наличие отрицательного эффекта у объекта O_i, отсутствие эффекта у объекта O_j; «0 / -» – отсутствие эффекта у объекта O_i при отрицательном эффекте у объекта O_j; «-» – наличие отрицательного эффекта; «0» – отсутствие эффекта; «+ / 0» – положительный эффект у объекта O_i, отсутствие эффекта у объекта O_j; «0 / +» – отсутствие эффекта у объекта O_i, положительный эффект у объекта O_j [11].

Для формализации антропоморфических видов межобъектного взаимодействия введены обозначения:

V – уязвимость (от англ. Vulnerability);

T – наличие уязвимости или угрозы (от англ. Threat);

0 – отсутствие уязвимости или угрозы;

$T_X(T_Y)$ – использование для функционирования уязвимости X функционала уязвимости Y;

$\rightarrow$ – реализация угроз вследствие наличия уязвимостей;

$<,>, =$ – операции сравнения угроз по их возможному ущербу.

Таким образом, реализация обособленной угрозы N вследствие наличия в программном коде соответствующей уязвимости N может быть записана следующим образом:

$$V_N \rightarrow T_N.$$

Исключение из правил составляет случай, когда каждая уязвимость по отдельности не ведет к какой-либо угрозе (как будет показано далее, это верно для первого типа взаимодействий – облигатного симбиоза):

$$V_N \rightarrow 0.$$

Для визуализации межобъектного взаимодействия использованы следующие графические элементы: атака на ОКИИ с использованием уязвимости; уязвимость в ПО; угроза информации, реализуемая в результате атаки (рис. 2).

Рис. 2. **Графические элементы для визуализации взаимодействия уязвимостей**

Цвет стрелки, обозначающей угрозу, соответствует значимости последней. Так, белый цвет указывает на минимальный риск, зеленый означает низкий уровень риска проведения атаки с использованием уязвимостей, желтый – средний уровень риска, а красный – максимальный [12].

Каждый из эффектов межобъектного взаимодействия уязвимостей в межобъектном взаимодействии на уровне СКИИ представлен в формализованном виде.

Эффект 1. Облигатный симбиоз (+ / +)

Рассматриваемый эффект подразумевает необходимость совместного существования объектов.

На уровне СКИИ к данному типу могут быть отнесены уязвимости, которые превращаются в киберугрозы только посредством взаимодействия друг с другом.

Формализация представления взаимодействия вида «облигатный симбиоз» имеет следующий вид:

$$\begin{cases} V_1 \to 0 \\ V_2 \to 0 \\ V_1 + V_2 \to T_{12}. \end{cases}$$

Схема взаимодействия уязвимостей представлена на рис. 3.

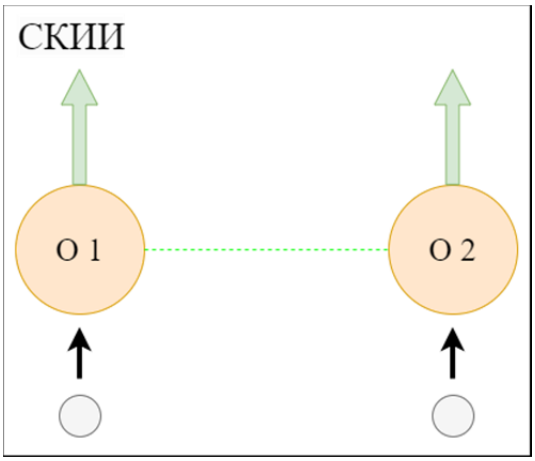

Рис. 3. **Схема реализации вида облигатного симбиоза уязвимостей (эффект 1)**

Облигатный симбиоз уязвимостей на уровне программного кода может возникнуть в результате «объединения» двух уязвимостей, где каждая отдельная уязвимость не представляет собой угрозу как таковую. Примером может служить угроза утечки данных по защищенным каналам связи между объектами в открытый злоумышленниками порт, где первая уязвимость – утечка данных, вторая – прослушивание порта.

Эффект 2. Паразитизм (+ / -)

Рассматриваемый эффект подразумевает одну из уязвимостей в качестве «паразита», а вторую – в качестве среды обитания для первой.

В СКИИ подобным примером могут служить уязвимости, где первая паразитирует на создаваемых информационных мощностях второй.

Формализация представления взаимодействия вида «паразитизм» имеет следующий вид:

$$\begin{cases} V_1 + V_2 \to T_1' + T_2' \\ T_1' = T_1 + D \\ T_2' = T_2 - D \end{cases},$$

где D – выгода, извлекаемая первой уязвимостью из второй.

Необходимо отметить, что угроза от второй уязвимости не всегда снижается пропорционально D; тем не менее такое упрощение не уменьшает общую корректность восприятия формулы.

Схема взаимодействия уязвимостей представлена на рис. 4.

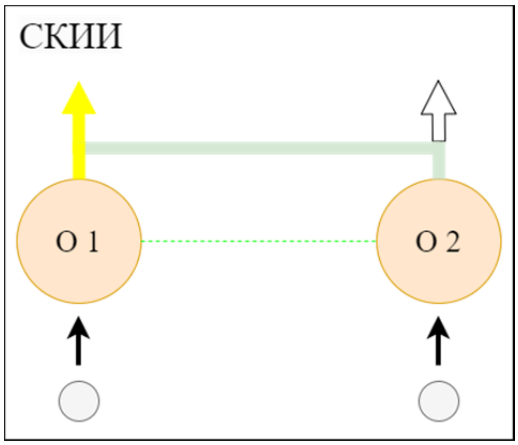

Рис. 4. **Схема реализации паразитического вида уязвимостей (эффект 2)**

В качестве примера паразитизма уязвимостей можно привести следующий сценарий: использование внутреннего алгоритма рассылки информации внутри защищенной сети для реализации внешних кибератак. В качестве организма-паразита выступает внешняя атака, например, DDoS, и в качестве маршрутизации использует алгоритм рассылки.

Эффект 3. Хищничество (+ / -)

Рассматриваемый эффект характеризуется тем, что одна уязвимость питается частями другой без симбиотических отношений.

Уязвимость оказывает агрессивное паразитирующее воздействие на другую путем подмены ее основного функционала на собственный.

Формализация представления взаимодействия вида «хищничество» имеет следующий вид:

$$\begin{cases} V_1 + V_2 \to T_1'(T_2) \\ T_1' > T_1. \end{cases}$$

Схема взаимодействия уязвимостей имеет следующий вид (рис. 5).

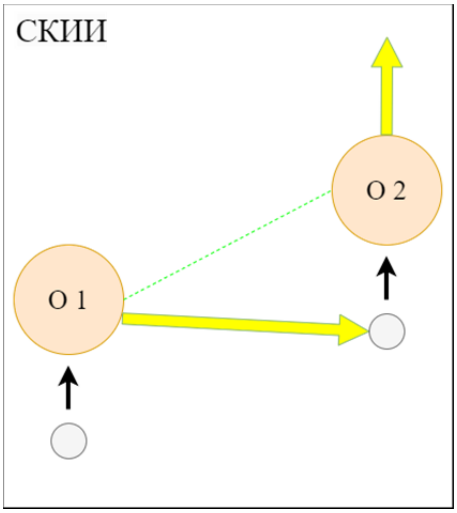

Рис. 5. **Схема реализации хищнического вида уязвимостей (эффект 3)**

Примером взаимодействия может быть усиление функционала уязвимостей для случая паразитизма: уязвимость 2 (из примера эффекта «паразитизм») начнет использовать алгоритм рассылки уязвимости 1, полностью подменив его ядро. Таким образом, уязвимость 2 полностью поглотит уязвимость 1 и будет существовать на ее ресурсах.

Эффект 4. Аменсализм (0 / -)

Рассматриваемый эффект характерен негативным воздействием первой уязвимости на вторую без обратного воздействия.

Уязвимости оказывают сдерживающее действие: первая сдерживает вторую, благодаря чему риск использования последней снижается.

Формализация представления взаимодействия вида «аменсализм» имеет следующий вид:

$$\begin{cases} V_1 + V_2 \to T_1 + T_2' \\ T_2' < T_2. \end{cases}$$

Схема взаимодействия уязвимостей представлена на рис. 6.

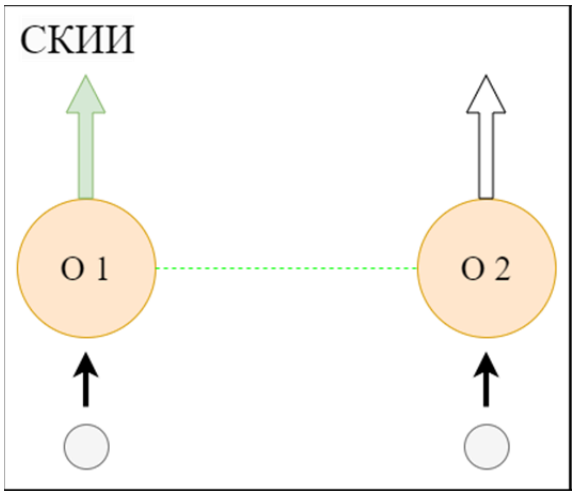

Рис. 6. **Схема реализации аменсалистического вида уязвимостей (эффект 4)**

Аменсализм уязвимостей ярко выражен в угрозах целостности информации. В качестве примера можно рассмотреть две уязвимости – первая из которых направлена на предоставление данных злоумышленникам, а вторая имеет цель заблокировать все данные к выводу в принципе. В таком сценарии первая уязвимость может перехватывать персональные данные людей, а вторая – предотвращать этот перехват.

Эффект 5. Аллелопатия (- / -)

Рассматриваемый эффект характеризуется взаимно-вредным влиянием уязвимостей программного кода.

Аллелопатический эффект от взаимодействия уязвимостей приводит к меньшему риску, чем сумма эффектов от их функционирования параллельно.

Формализация представления взаимодействия вида «аллелопатия» имеет следующий вид:

$$\begin{cases} V_1 + V_2 \to T_{12} \\ T_{12} < T_1 + T_2. \end{cases}$$

Схема взаимодействия уязвимостей представлена на рис. 7.

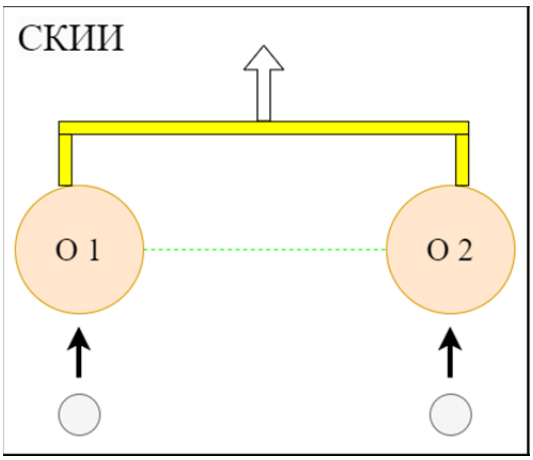

Рис. 7. **Схема аллелопатического вида уязвимостей (эффект 5)**

Аллелопатический эффект подобен эффекту амменсализма, однако первая уязвимость (из эффекта 4) должна быть существенно мощнее второй. В таком случае получим сценарий, когда одна уязвимость будет всеми способами пытаться создать утечку данных, а вторая противостоять этому инциденту. Однако в силу мощности первая уязвимость реализуется, однако существенно снизив свой потенциал из-за воздействия второй уязвимости.

Эффект 6. Конкуренция (- / -)

Отличительная особенность эффекта конкуренции – это общие ресурсы, за которые ведут борьбу уязвимости, тем самым происходит ограничение одной из уязвимостей, благодаря захвату большей части ресурсов другой уязвимостью.

При функционировании уязвимостей подразумевается использование ограниченных и общих ресурсов, например, оперативная память. В результате уязвимости начинают конфликтовать.

Формализация представления взаимодействия вида «конкуренция» имеет следующий вид:

$$\begin{cases} V_1 + V_2 \to T_1' + T_2' \\ \quad \begin{bmatrix} \begin{cases} T_1' \le T_1 \\ T_2' \ll T_2 \end{cases} \\ \begin{cases} T_1' \ll T_1 \\ T_2' \le T_2. \end{cases} \end{bmatrix} \end{cases}$$

Схема взаимодействия уязвимостей представлена на рис. 8.

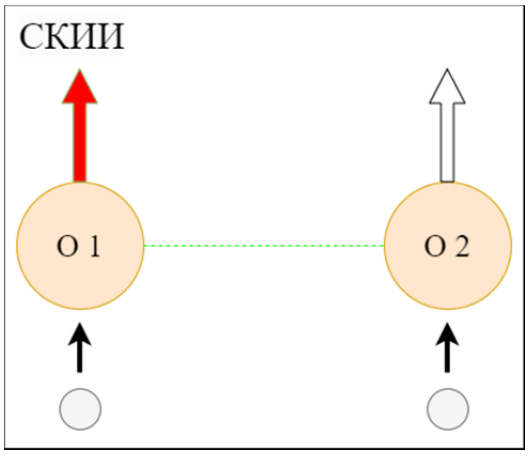

Рис. 8. **Схема конкуренческого вида уязвимостей (эффект 6)**

Конкуренция уязвимостей возникает в том случае, когда цель от реализации двух уязвимостей совпадает, а канал передачи данных во внешний периметр только один. Например, обе уязвимости вызывают раскрытие паролей пользователей и утечку этих данных по одному конкретному каналу связи. Работоспособной окажется та уязвимость, которая быстрее зарезервирует канал в сетевой библиотеке программы.

Эффект 7. Нейтрализм (0 / 0)

Отсутствием каких-либо воздействий друг на друга.

Такие уязвимости, которые не влияют друг на друга, а функционируют параллельно.

Формализация представления взаимодействия вида «нейтрализм» имеет следующий вид:

$$V_1 + V_2 \rightarrow T_1 + T_2.$$

Схема взаимодействия уязвимостей представлена на рис. 9.

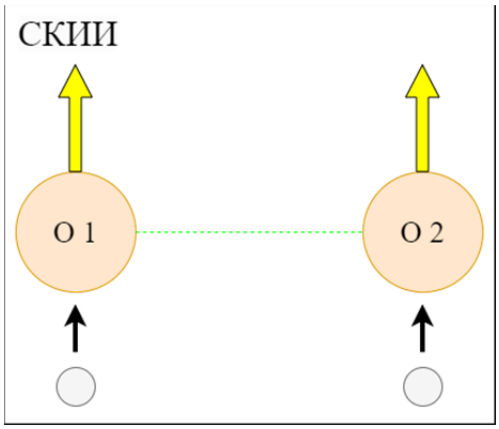

Рис. 9. **Схема нейтралитического вида уязвимостей (эффект 7)**

Подобный тип взаимодействия может возникнуть между любыми уязвимостями, по функциональному и целевому признаку не связанными друг с другом. Например, между встроенным в программу логином администратора и ошибками в криптографическом алгоритме хэша для проверки пароля.

По результатам исследований выделены семь наиболее популярных уязвимостей (топ-7) [13]:

У_1. SQL-инъекции позволяют злоумышленникам выполнять произвольные SQL-запросы к базе данных через уязвимые точки ввода данных.

У_2. Незащищенность API – неправильное управление аутентификацией и авторизацией, недостаточная валидация входных данных или отсутствие ограничения по частоте обращений могут быть использованы для атак.

У_3. Скриптинг – внедрение вредоносных скриптов на веб-страницы, которые могут повредить пользователям или украсть их данные.

У_4. Недостаточная аутентификация – уязвимости, связанные с незащищенным хранением паролей, несоответствующей политикой сложных паролей.

У_5. Устаревшее ПО. Его использование может привести к уязвимостям, если не производится регулярное обновление.

У_6. Уязвимости в маршрутизации – некорректная настройка межсетевых экранов и маршрутизаторов может привести к несанкционированному доступу к данным.

У_7. Некорректная работа с ошибками – код не обрабатывает ошибки корректно, могут раскрывать информацию о системе [13].

Далее составлена таблица взаимодействия уязвимостей программного кода, описанных выше (табл. 3). В ячейках указаны типы взаимодействий для соответствующих типов уязвимостей программного кода. Также в скобках указан эффект для первой уязвимости от взаимодействия со второй уязвимостью.

Таблица 3

Взаимодействие уязвимостей в межобъектном взаимодействии на уровне СКИИ

	У_1	У_2	У_3	У_4	У_5	У_6	У_7
У_1			В_1 (+)				
У_2					В_4 (-)		В_3 (+)
У_3	В_3 (+)			В_7 (0)			
У_4			В_7 (0)			В_5 (-)	
У_5		В_4 (0)					В_1 (+)
У_6				В_5(-)	В_2 (+)		
У_7		В_6 (-,-)					

Таким образом, можно утверждать, что определенной логики и закономерности в зависимости межобъектного взаимодействия не прослеживается. Заполнение значениями во всех ячейках требует работы экспертной группы или дополнительных исследований.

Метрика уязвимостей

В настоящее время метрик оценки программного кода, которые широко распространены и повсеместно используются, не обнаружено, кроме того, также не обнаружены метрики оценки программного кода с позиции функционирования уязвимостей в нем. Предложим собственную, основанную на антропоморфическом подходе взаимодействия угроз на уровне программного кода.

Метрика уязвимостей программного кода (Метрика) может быть записана следующим образом:

$$M = \begin{vmatrix} v_1 \\ \dots \\ v_N \end{vmatrix}, \quad (1)$$

где v_i – эффект от *i*-го типа уязвимости; N – количество рассматриваемых типов уязвимостей.

Рассмотрим случаи наличия программных кодов, в которых функционируют две и более уязвимостей. При наличии двух уязвимостей разных видов взаимодействия можно говорить о разных результатах для каждой уязвимости, что возможно отразить в формуле (1) при добавлении показателя M_1, который учитывает подобные разнообразные воздействия. Показатель M_1 является вектором такой же размерности, как и M. При этом каждый из элементов вектора должен зависеть от эффекта соответствующего типа уязвимости, а также от ее взаимодействия с остальными. Итоговая формула для M_1 имеет следующий вид:

$$M_1 = |v_1, \dots, v_N| \times \begin{vmatrix} I_{11} & \dots & I_{1N} \\ \vdots & \ddots & \vdots \\ I_{N1} & \dots & I_{NN} \end{vmatrix}, \quad (2)$$

где I_{ij} – коэффициент влияния взаимодействия *i*-го и *j*-го типа уязвимости на *i*-ю уязвимость.

В результате типы уязвимостей, которые не подразумевают взаимодействия, имеют коэффициент $I_{ij} \equiv 0$, в ситуации, когда вторая уязвимость усиливает первую: $I_{ij} > 0$, в обратном случае: – $I_{ij} < 0$. Аддитивный же эффект влияния всех типов уязвимостей на уязвимость данного типа определяется:

$$K_i = \sum_{j=1}^{N} V_j \times I_{ij} .$$

Предлагаемое решение

Предположим, что в рамках одного СКИИ взаимодействуют два ОКИИ посредством передачи данных: конфиденциальной информации из внутренней базы данных с использованием механизмов идентификации и аутентификации с целью разграничения прав доступа к базам данных разного уровня допуска. В таком сценарии вероятны нарушения конфиденциальности и сохранности данных: получение доступа к данным лицами, не имеющим таковых прав доступа. Как в большинстве случаев предполагаемая программа написана на языке программирования C# с базовым функционалом – запрос ввода логина и пароля, предоставление прав пользователю к соответствующим данным.

Вероятность нахождения уязвимостей из топ-7 в гипотетическом межобъектном взаимодействии.

Мин. – минимальная, Ум. – умеренная, Выс. – высокая, Макс. – максимальная. Предлагаемая шкала вероятности будет иметь следующие пропорции: 0 (Мин.): 0,25 (Ум.): 0,75 (Выс.): 1 (Макс.) (рис. 10).

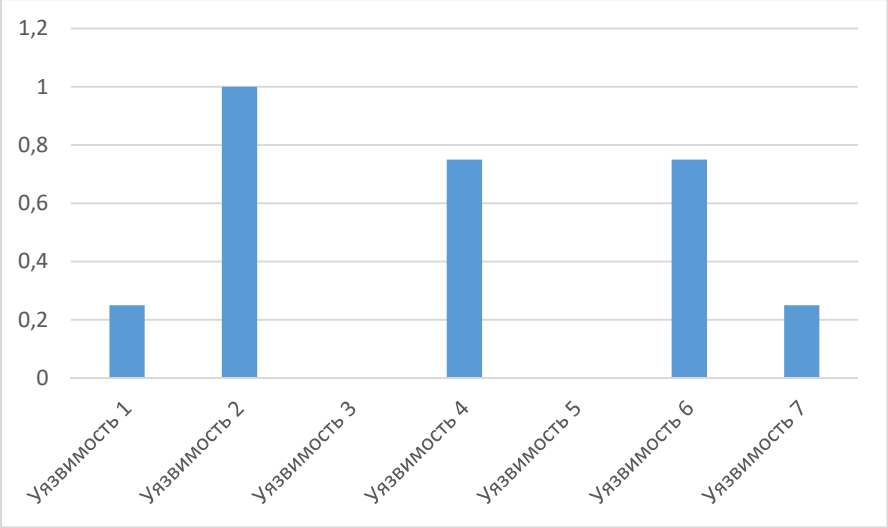

Рис. 10.

В результате Метрика представляется в следующем виде:

$$M = K_v \times \begin{vmatrix} 0.25 \\ 1 \\ 0 \\ 0.75 \\ 0 \\ 0.75 \\ 0.25 \end{vmatrix}, \quad (3)$$

где K_v – нормировочный коэффициент ($K_v \ll 1$).

Аналогично будем считать, что коэффициент влияния взаимодействия *i*-го и *j*-го типа уязвимости на *i*-ю уязвимость (I_{ij}) равен произведению K_I (нормировочный коэффициент) на эффект от взаимодействия: «0» – в случае отсутствия эффекта, «1» – для выгоды, «–1» – для ущерба; в случае нескольких эффектов, они суммируются.

Опираясь на формулу (2), а также следуя формуле (3) и табл. 3, вычислим корректирующий член на основании существующих взаимодействий уязвимостей:

$$M_1 = K_v \times |0.25, 1, 0, 0.75, 0, 0.75, 0.25| \times K_i \times M_1 =$$

$$= K_v \times K_i \times \begin{vmatrix} 0.25 \\ 1 \\ 0 \\ 0.75 \\ 0 \\ 0.75 \\ 0.25 \end{vmatrix},$$

где $M_1 =$

			+1				
					-1		+1
	+1			0			
			0			-1	
		0					+1
				-1	+1		
		-1–1					

.

Интерпретируя полученные результаты, можно говорить о возможности применения антропоморфического подхода в представленных уязвимостях: абсолютно всё взаимодействие разных уязвимостей показывает разный результат. Например, взаимодействие уязвимостей 2 и 4 никак не усиливает эффект друг от друга, однако результат взаимодействия двух уязвимостей совершенно непредсказуем: уязвимости могут усиливать друг друга, никак не влиять друг на друга и снижать эффект от взаимодействия, что, в свою очередь, может быть отражено в показателе оценки межобъектного взаимодействия на уровне СКИИ [14, 15].

Заключение

Представленное исследование подтверждает актуальность и востребованность применения антропоморфического подхода в оценке организации межобъектного взаимодействия на уровне СКИИ. Рассмотренные в работе примеры можно использовать в дальнейшем изучении вопросов взаимодействия уязвимостей на уровне программного кода ОКИИ.

Дополнительно возможно использование проведенного исследования в создании системы менеджмента ИБ организации с учетом инвестиционной составляющей: грамотное распределение ресурсов с целью исполнения политики ИБ путем отслеживания антропоморфических типов взаимодействия угроз, в которых возможны варианты взаимного уничтожения негативных последствий от их реализации. Принимая во внимание такие возможные сценарии, организации смогут выстроить гораздо более эффективную инвестиционную политику в области ИБ [16, 17].

Применение антропоморфизма для понимания взаимодействий оказалось достаточно удачным как для типизации, так и для их интерпретации человеком. Предложенная формализация показала свою жизнеспособность, хотя для полноценного математического аппарата необходимы дополнительные исследования и подходы, выходящие за рамки сферы ИБ.

Список источников

1. О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях: Федер. закон Рос. Федерации от 2 июля 2013 г. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Русаков А.М. Комплекс антропоморфических моделей поведенческого анализа процессов для обнаружения эффектов инфраструктурного деструктивизма // Инженерный вестник Дона. 2024. № 11 (119). С. 391–404. EDN DLHUZQ.

3. Доктрина информационной безопасности Российской Федерации: Указ Президента Рос. Федерации от 5 дек. 2016 г. № 646. Доступ из справ.-правовой системы «КонсультантПлюс».

4. Буйневич М.В., Израилов К.Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Часть 1. Типы взаимодействий // Защита информации. Инсайд. 2019. № 5 (89). С. 78–85. EDN OLLEYX.

5. Горин Д.С., Долженков С.С. Научно-методические основы управления качеством продукции на основе CALS-технологий // Вестник Академии права и управления. 2021. № 3 (64). С. 55–60. DOI: 10.47629/2074-9201_2021_3_55_60. EDN CUTDUR.

6. Максимова Е.А. Модели и методы оценки информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях инфраструктурного генеза: дис. ... д-ра техн. наук. СПб., 2022. 448 с. EDN OHDNPO.

7. Taneski V., Heričko M., Brumen B. Impact of security education on password change // 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). 2015. P. 1350–1355.

8. Marimuthu K., Gopinath M. Production of Sugarcane Forecasting using ARIMAX Model // Scopus. International Journal of Innovative Technology and Exploring Engineering. 2019. Vol. 8. Iss. 12-S.

9. Интеллектуальный анализ работы хранилища данных Greenplum на основе обработки лог-файлов / А.М. Русаков [и др.] // Современная наука: актуальные проблемы теории и практики. Сер.: Естественные и технические науки. 2023. № 6. С. 142–149. DOI: 10.37882/2223-2966.2023.06.31. EDN PIRKUE.

10. Долженков С.С., Максимова Е.А. Риск-менеджмент как средство реализации методологии поддержки процессов управления информационной безопасностью субъектов критической информационной инфраструктуры при деструктивных воздействиях инфраструктурного генеза // Актуальные проблемы прикладной математики, информатики и механики: сб. трудов Междунар. науч. конф. Воронеж: ООО «Вэлборн»; Изд-во «Научно-исследовательские публикации», 2024. С. 1538–1539. EDN DNWVWZ.

11. Буйневич М.В., Израилов К.Е. Аналитическое моделирование работы программного кода с уязвимостями // Вопросы кибербезопасности. 2020. № 3 (37). С. 2–12. DOI: 10.21681/2311-3456-2020-03-02-12. EDN CQFGPI.

12. Буйневич М.В., Израилов К.Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Часть 2. Метрика уязвимостей // Защита информации. Инсайд. 2019. № 6 (90). С. 61–65. EDN HLUDTX.

13. Modeling Software Vulnerabilities with Vulnerability Cause Graphs / D. Byers [et al.] // 22nd IEEE International Conference on Software Maintenance. 2006. P. 411–422.

14. Rinaldi S.M., Peerenboom J.P., Kelly T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies // IEEE control systems magazine. 2001. Vol. 21. № 6. P. 11–25.

15. Долженков С.С. Оптимизация системы менеджмента информационной безопасности объектов критической информационной инфраструктуры // Студенческая наука для развития информационного общества: материалы XV Всерос. науч.-техн. конф. с приглашением зарубежных ученых. Ставрополь: Северо-Кавказский федер. ун-т, 2024. С. 124–130. EDN EYGAVD.

16. Белов А.С., Добрышин М.М., Душкин А.В. Системный подход к проектированию систем обеспечения информационной безопасности. М.: Науч.-техн. изд-во «Горячая линия-Телеком», 2023. 232 с. ISBN 978-5-9912-1067-6. EDN DCSYJQ.

17. Castro J.L., Delgado M. Fuzzy systems with defuzzification are universal approximators // IEEE Transactions on Systems, Man and Cybernetics. Part B (Cybernetics). 1996. Vol. 26. Iss. 1. P. 149–152.

18. Долженков С.С., Максимова Е.А. Применение подходов риск-менеджмента в области информационной безопасности субъектов критической информационной инфраструктуры при деструктивных воздействиях инфраструктурного генеза // Кибернетика и информационная безопасность «КИБ-2023»: сб. науч. трудов Всерос. науч.-техн. конф. М.: Нац. исслед. ядерный ун-т «МИФИ», 2023. С. 100–101. EDN HSRMAM.

References

1. O vnesenii izmenenij v otdel'nye zakonodatel'nye akty Rossijskoj Federacii po voprosam zashchity intellektual'nyh prav v informacionno-telekommunikacionnyh setyah: Feder. zakon Ros. Federacii ot 2 iyulya 2013 g. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

2. Rusakov A.M. Kompleks antropomorficheskih modelej povedencheskogo analiza processov dlya obnaruzheniya effektov infrastrukturnogo destruktivizma // Inzhenernyj vestnik Dona. 2024. № 11 (119). S. 391–404. EDN DLHUZQ.

3. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii: Ukaz Prezidenta Ros. Federacii ot 5 dek. 2016 g. № 646. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus».

4. Bujnevich M.V., Izrailov K.E. Antropomorficheskij podhod k opisaniyu vzaimodejstviya uyazvimostej v programmnom kode. Chast' 1. Tipy vzaimodejstvij // Zashchita informacii. Insajd. 2019. № 5 (89). S. 78–85. EDN OLLEYX.

5. Gorin D.S., Dolzhenkov S.S. Nauchno-metodicheskie osnovy upravleniya kachestvom produkcii na osnove CALS-tekhnologij // Vestnik Akademii prava i upravleniya. 2021. № 3 (64). S. 55–60. DOI: 10.47629/2074-9201_2021_3_55_60. EDN CUTDUR.

6. Maksimova E.A. Modeli i metody ocenki informacionnoj bezopasnosti sub"ekta kriticheskoj informacionnoj infrastruktury pri destruktivnyh vozdejstviyah infrastrukturnogo geneza: dis. ... d-ra tekhn. nauk. SPb., 2022. 448 s. EDN OHDNPO.

7. Taneski V., Heričko M., Brumen B. Impact of security education on password change // 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). 2015. P. 1350–1355.

8. Marimuthu K., Gopinath M. Production of Sugarcane Forecasting using ARIMAX Model // Scopus. International Journal of Innovative Technology and Exploring Engineering. 2019. Vol. 8. Iss. 12-S.

9. Intellektual'nyj analiz raboty hranilishcha dannyh Greenplum na osnove obrabotki log-fajlov / A.M. Rusakov [i dr.] // Sovremennaya nauka: aktual'nye problemy teorii i praktiki. Ser.: Estestvennye i tekhnicheskie nauki. 2023. № 6. S. 142–149. DOI: 10.37882/2223-2966.2023.06.31. EDN PIRKUE.

10. Dolzhenkov S.S., Maksimova E.A. Risk-menedzhment kak sredstvo realizacii metodologii podderzhki processov upravleniya informacionnoj bezopasnost'yu sub"ektov kriticheskoj informacionnoj infrastruktury pri destruktivnyh vozdejstviyah infrastrukturnogo geneza // Aktual'nye problemy prikladnoj matematiki, informatiki i mekhaniki: sb. trudov Mezhdunar. nauch. konf. Voronezh: OOO «Velborn»; Izd-vo «Nauchno-issledovatel'skie publikacii», 2024. S. 1538–1539. EDN DNWVWZ.

11. Bujnevich M.V., Izrailov K.E. Analiticheskoe modelirovanie raboty programmnogo koda s uyazvimostyami // Voprosy kiberbezopasnosti. 2020. № 3 (37). S. 2–12. DOI: 10.21681/2311-3456-2020-03-02-12. EDN CQFGPI.

12. Bujnevich M.V., Izrailov K.E. Antropomorficheskij podhod k opisaniyu vzaimodejstviya uyazvimostej v programmnom kode. Chast' 2. Metrika uyazvimostej // Zashchita informacii. Insajd. 2019. № 6 (90). S. 61–65. EDN HLUDTX.

13. Modeling Software Vulnerabilities with Vulnerability Cause Graphs / D. Byers [et al.] // 22nd IEEE International Conference on Software Maintenance. 2006. P. 411–422.

14. Rinaldi S.M., Peerenboom J.P., Kelly T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies // IEEE control systems magazine. 2001. Vol. 21. № 6. P. 11–25.

15. Dolzhenkov S.S. Optimizaciya sistemy menedzhmenta informacionnoj bezopasnosti ob"ektov kriticheskoj informacionnoj infrastruktury // Studencheskaya nauka dlya razvitiya informacionnogo obshchestva: materialy XV Vseros. nauch.-tekhn. konf. s priglasheniem zarubezhnyh uchenyh. Stavropol': Severo-Kavkazskij feder. un-t, 2024. S. 124–130. EDN EYGAVD.

16. Belov A.S., Dobryshin M.M., Dushkin A.V. Sistemnyj podhod k proektirovaniyu sistem obespecheniya informacionnoj bezopasnosti. M.: Nauch.-tekhn. izd-vo «Goryachaya liniya-Telekom», 2023. 232 s. ISBN 978-5-9912-1067-6. EDN DCSYJQ.

17. Castro J.L., Delgado M. Fuzzy systems with defuzzification are universal approximators // IEEE Transactions on Systems, Man and Cybernetics. Part B (Cybernetics). 1996. Vol. 26. Iss. 1. P. 149–152.

18. Dolzhenkov S.S., Maksimova E.A. Primenenie podhodov risk-menedzhmenta v oblasti informacionnoj bezopasnosti sub"ektov kriticheskoj informacionnoj infrastruktury pri destruktivnyh vozdejstviyah infrastrukturnogo geneza // Kibernetika i informacionnaya bezopasnost' «KIB-2023»: sb. nauch. trudov Vseros. nauch.-tekhn. konf. M.: Nac. issled. yadernyj un-t «MIFI», 2023. S. 100–101. EDN HSRMAM.

Информация о статье:
Статья поступила в редакцию: 25.01.2025; одобрена после рецензирования: 20.02.2025;
принята к публикации: 22.02.2025
Information about the article:
The article was submitted to the editorial office: 25.01.2025; approved after review: 20.02.2025;
accepted for publication: 22.02.2025

Сведения об авторах:
Долженков Сергей Сергеевич, аспирант кафедры КБ-4 «Интеллектуальные системы информационной безопасности» Института кибербезопасности и цифровых технологий МИРЭА – Российского технологического университета (119454, Москва, пр. Вернадского, д. 78), e-mail: dolzhenkov@mirea.ru, https://orcid.org/0009-0004-8621-3994, SPIN-код: 1759-7373
Максимова Елена Александровна, заведующий кафедрой КБ-4 «Интеллектуальные системы информационной безопасности» Института кибербезопасности и цифровых технологий МИРЭА – Российского технологического университета (119454, Москва, пр. Вернадского, д. 78), доктор технических наук, доцент, e-mail: maksimova@mirea.ru, https://orcid.org/0000-0001-8788-4256, SPIN-код: 6876-5558

Information about the authors:
Dolzhenkov Sergey S., postgraduate student of the department KB-4 «Intelligent information security systems» of the Institute of cybersecurity and digital technologies of the MIREA – Russian technological university (119454, Moscow, Vernadsky ave., 78), e-mail: dolzhenkov@mirea.ru, https://orcid.org/0009-0004-8621-3994, SPIN: 1759-7373
Maksimova Elena A., head of the department KB-4 «Intelligent Information Security Systems» of the Institute of cybersecurity and digital technologies of the MIREA – Russian technological university (119454, Moscow, Vernadsky ave., 78), doctor of technical sciences, associate professor, e-mail: maksimova@mirea.ru, https://orcid.org/0000-0001-8788-4256, SPIN: 6876-5558