Инженерный вестник Дона, №11 (2024)
ivdon.ru/ru/magazine/archive/n11y2024/9656

Комплекс антропоморфических моделей поведенческого анализа процессов для обнаружения эффектов инфраструктурного деструктивизма

А.М. Русаков

МИРЭА - Российский технологический университет, Москва

Аннотация: В статье предложен комплекс антропоморфических моделей оценки рисков эффектов инфраструктурного деструктивизма. В основе данных моделей лежит один из подходов к оценке рисков инфраструктурного генеза, заключающийся в оценке эффекта инфраструктурного деструктивизма, состоящего в неконтролируемом саморазрушении информационной инфраструктуры. В отличие от уже имеющихся подходов к оценке показателей инфраструктурного деструктивизма, в статье предлагается использование моделей, учитывающих множественные поведенческие взаимодействия процессов на основе антропоморфического подхода. Антропоморфический подход предусматривает реализацию алгоритмов оценки межобъектного взаимодействия по принципам развития живой природы. Феномен инфраструктурного деструктивизма имеет практическое объяснение, связанное с тем, что при определённых условиях одновременная реализация деструктивных воздействий на объекты инфраструктуры от различных источников может привести как к катастрофическим изменениям (то есть к полному саморазрушению информационной инфраструктуры), так и к минимизации рисков инфраструктурного генеза. В статье вводится понятие метрики «здоровья» в системе мониторинга информационной безопасности инфраструктуры, которая отображает наличие «отрицательных» поведенческих активностей процессов и тем самым предсказывает увеличение вероятности появления эффектов инфраструктурного деструктивизма. Таким образом при применении предложенных моделей становится возможным повышение точности оценки рисков инфраструктурного генеза, следовательно, обеспечение достаточного уровня информационной безопасности.
Ключевые слова: инфраструктурный деструктивизм, деструктивные воздействия инфраструктурного генеза, антропоморфический подход, интеллектуальный анализ журналов событий, поведенческий анализ.

1. Введение

Стремительное применение цифровых технологий во всех сферах современной жизни сопровождается таким же стремительным и быстрым ростом компьютерных атак. Решение вопросов обеспечения безопасности объектов информатизации при этом сопровождается необходимостью учета постоянного усложнения и изменения архитектур информационных инфраструктур. В это же время, как показывает статистика, существенно увеличивается количество таргетированных кибератак на значимые объекты

информационной инфраструктуры [1-3]. Это приводит к повышению рисков информационной безопасности. Следовательно, к необходимости создания новых подходов по обеспечению их безопасности.

Отдельное внимание при управлении рисков информационной безопасности. должно быть уделено вопросам их динамики, что проявляется в условиях инфраструктурного деструктивизма и обуславливается специфичными для ИТ инфраструктуры признаками и свойствами [4, 5]. Таким образом, целью данной работы является повышение уровня информационной безопасности объектов инфраструктуры в следствии повышения точности оценки рисков инфраструктурного генеза.

Деструктивные воздействия инфраструктурного генеза рассматриваются сегодня в контексте инфраструктурного деструктивизма, под которым понимается «неспособность информационной инфраструктуры реализовывать свой функционал в полном объеме под воздействием рисков инфраструктурного генеза» [6, 7].

Тем не менее до сих пор остается ряд вопросов, связанных, в том числе, с качественной оценкой деструктивных эффектов от взаимодействия двух и более объектов информационной инфраструктуры, которые до сих пор не решены полностью и не позволяют адекватно оценить риски инфраструктурного генеза.

При этом, на практике возможна ситуация, когда один из объектов «нейтрализует» другой или возникает в системе эффект саморазрушения, усиливающийся при дополнительном воздействии кибератак. Обозначенное явление рассматривается в данном исследовании при моделировании объектов на базе антропоморфического подхода [8, 9]. В данной работе разработан комплекс антропоморфических моделей оценки поведенческой активности межобъектных взаимодействий инфраструктуры который

косвенно позволяет оценивать эффекты инфраструктурного деструктивизма, что особенно востребовано в сложившихся геополитических условиях.

2. Модель взаимодействия сервисов в информационной инфраструктуре

Рассмотрим случай, когда несколько сервисов взаимодействуют между собой и на каждый сервис отправляется запросы от клиентов, как представлено на рис.1.

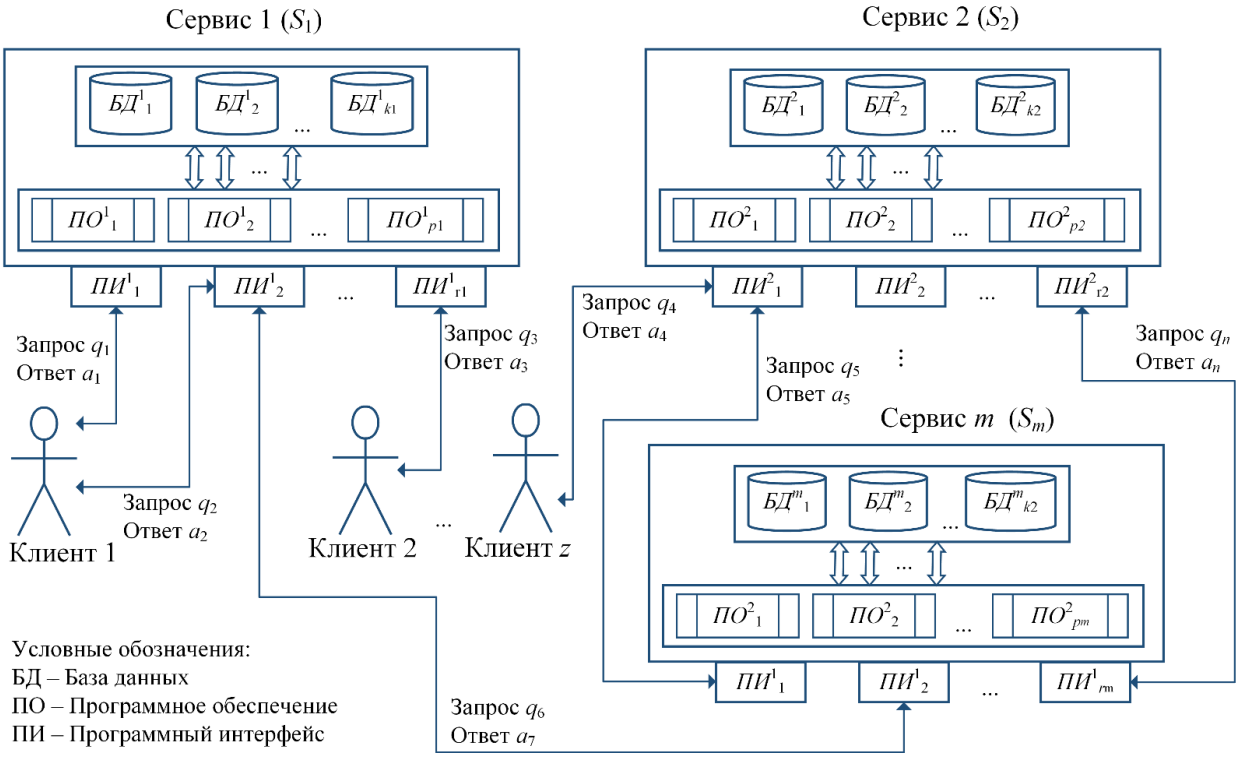

Рис. 1. – Пример взаимодействия сервисов в инфраструктуре

Пусть $S=\{S_1,S_2\ldots S_m\}$ – множество m взаимодействующих сервисов и z клиентов в инфраструктуре. Внутри каждого сервиса j, $j=\overline{1,m}$ находится комплект из p_j программного обеспечения (КПО): $КПО_j=ПО_1^j,ПО_2^j\ldots ПО_{p_j}^j$ и комплект из k_j баз данных $КБД_j=БД_1^j,БД_2^j\ldots БД_{k_j}^j$. Комплекты $КПО_j$ и $КБД_j$ между собой взаимодействуют. Сервисы S_j, $j=\overline{1,m}$ также

взаимодействуют между собой и с z клиентами через наборы программных интерфейсов (НПИ):

$НПИ_j = ПИ_1^j, ПИ_2^j \ldots ПИ_{r_j}^j$, где r_j – количество программных интерфейсов для каждого сервиса j. Общее число программных интерфейсов для каждого сервиса j, $j = \overline{1,m}$ составляет $r_1, r_2, ...r_m$. На каждый программных интерфейсов поступает последовательность запросов $Q_i^j = q_1^i, q_2^i \ldots q_{n_i}^i$, где $j = \overline{1,m}$, $i = \overline{1,r_j}$.

Каждый запрос в инфраструктуре имеет своё время обработки. Причем для одинаковых запросов время выполнения, может быть разным и зависит от внутреннего состояния и наличия свободных ресурсов инфраструктуре. Обозначим общее количество всех наблюдаемых запросов инфраструктуре как $Q_{all} = q_1, q_2, ...q_n$, где n – общее количество запросов инфраструктуре. Каждый из запросов q_i порождает процесс обработки этого запроса $Proc_i$, который обрабатывает сервис инфраструктуре, и по окончании обработки высылается ответ a_i.

Обозначим множество всех исследуемых процессов как $Proc_{all} = \{Proc_1, Proc_2, \ldots Proc_n\}$, где n – общее количество анализируемых процессов.

На рис.2 представлена временная диаграмма работы запроса q_i, который выполняет процесс $Proc_i$ с длительностью выполнения Tq_i.

Для каждого процесса $Proc_i$ существуют процессы, которые выполнялись до его начала, во время его работы и после его работы, а также частично до и после начала и окончания процесса $Proc_i$ за некоторый интервал времени $T_{набл}$. Обозначим данные процессы по отношению $Proc_i$ как показано на рисунке 3: $Proc_a$, $Proc_b$, $Proc_c$, $Proc_d$ и $Proc_e$. Указанные процессы $Proc_a$, $Proc_b$, $Proc_c$, $Proc_d$, $Proc_e$ и исследуемый процесс $Proc_i$

могут оказывать взаимное влияние приводящее к эффекту инфраструктурного деструктивизма.

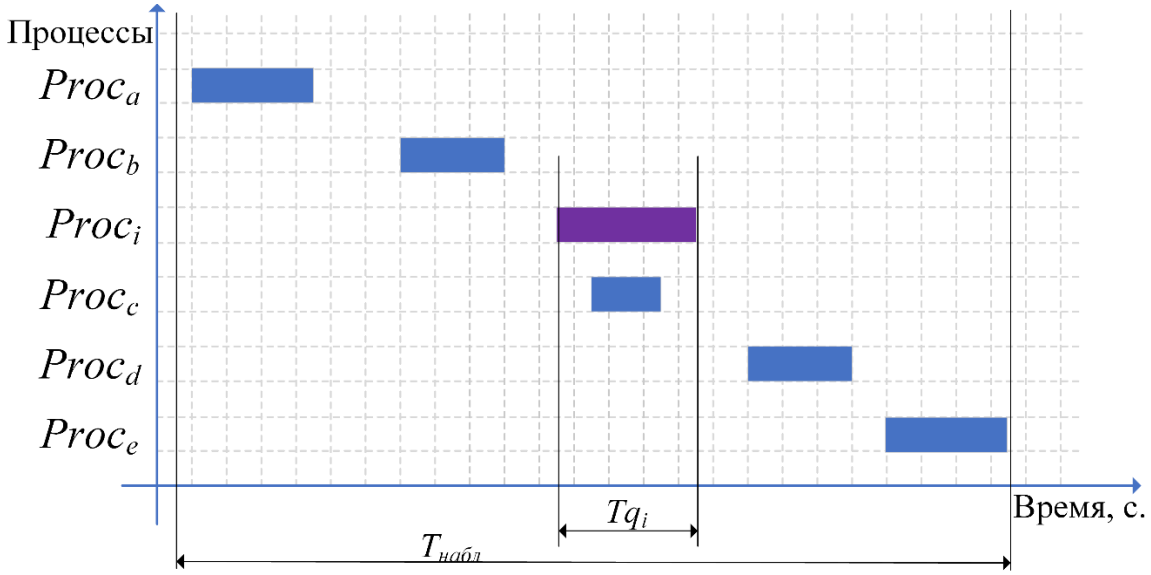

Рис. 2. – Временная диаграмма взаимодействующих процессов.

3. Комплекс антропоморфических моделей поведенческого анализа процессов информационных инфраструктур

Опишем поведенческие особенности взаимодействий сервисов на основе анализа наблюдаемых процессов. Поведение процессов предлагается оценить с помощью типов взаимодействия организмов живой природы – антропоморфических типов взаимодействия. Согласно широко распространенному в науке делению отношений живых организмов известны следующие типы их взаимодействий: симбиоз (облигатный и факультативный симбиоз, комменсализм, паразитизм, хищничество) – когда хотя бы один из организмов получает выгоду, антибиоз (аменсализм, аллелопатия, конкуренция) – когда один из организмов ограничивает возможности другого, и нейтрализм – сосуществования организмов без взаимного влияния.

На рис.3-11 представлены 9 временных диаграмм для основных антропоморфических типов взаимодействия процессов в инфраструктуре. Для этих временных диаграмм введем следующую систему обозначений:

- символ «+» и зеленый цвет стрелочки – процесс оказывает положительное влияние на другой процесс;
- символ «0» и желтый цвет стрелочки – процесс не оказывает влияние на другой процесс;

символ «–» и красный цвет стрелочки – оказывает отрицательное влияние на другой процесс.

Каждый тип взаимодействия процессов можно представить следующим образом.

Тип 1 Облигатный симбиоз (+|+). Данный тип характеризуется необходимостью совместного сосуществования организмов (рис.3).

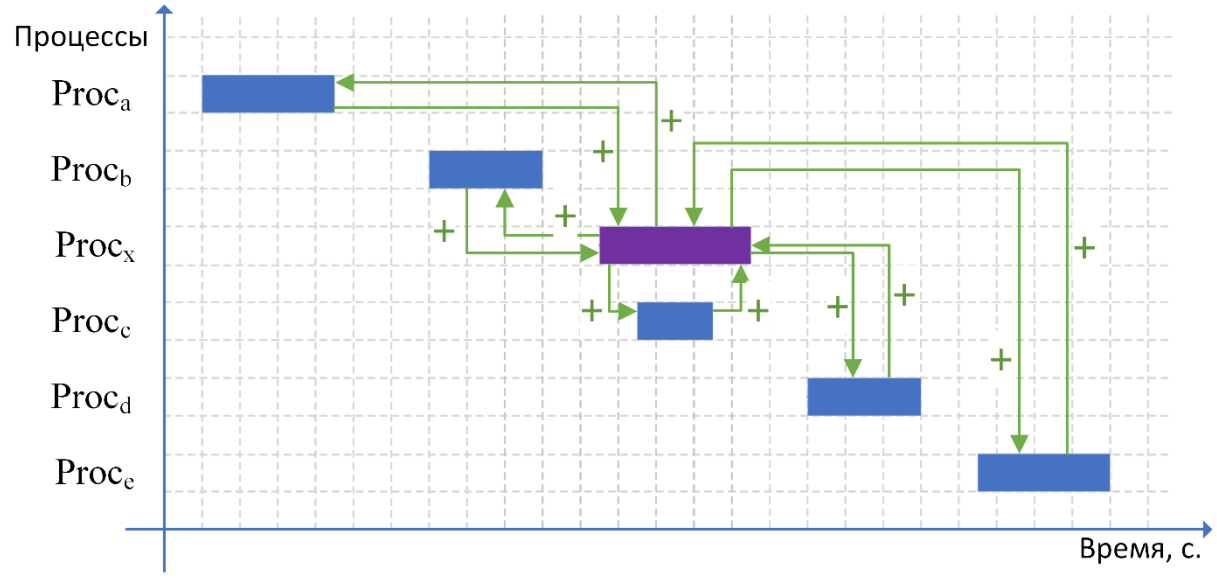

Рис. 3. – Временная диаграмма выполнения процессов тип 1 облигатный симбиоз

Тип 2 Факультативный симбиоз (+|+) – характеризуется взаимной выгодой от совместного сосуществования организмов, но без необходимости, как таковой (рис.4).

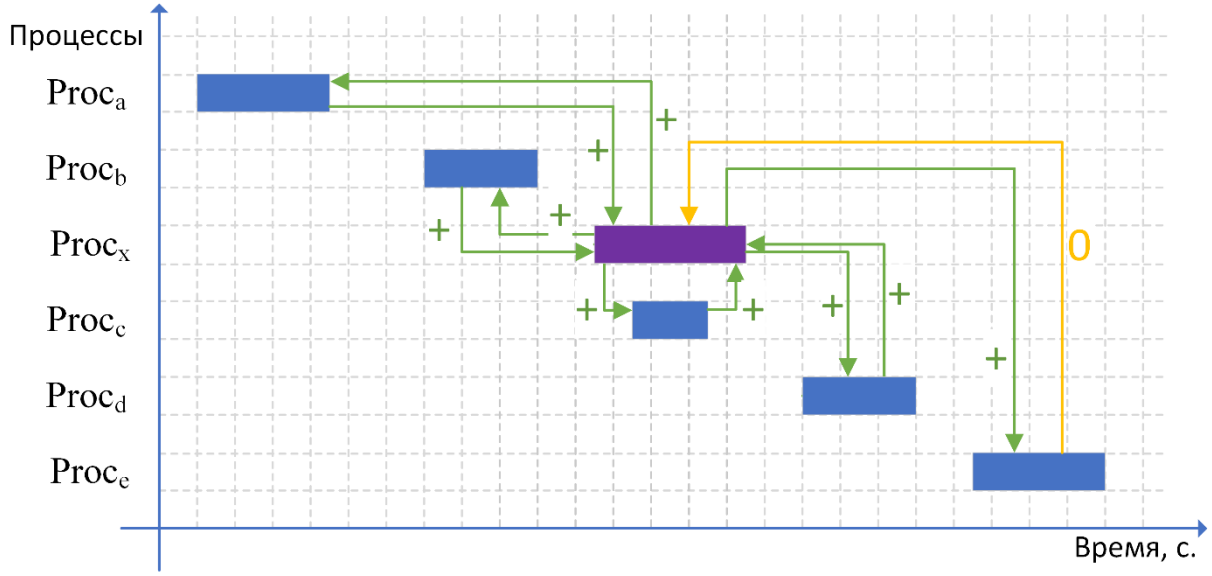

Рис. 4. – Временная диаграмма выполнения процессов тип 2 Факультативный симбиоз

Тип 3 Комменсализм (+|0). Данный тип характеризуется выгодой от существования одного организма при отсутствии какого-либо эффекта для другого (рис.5).

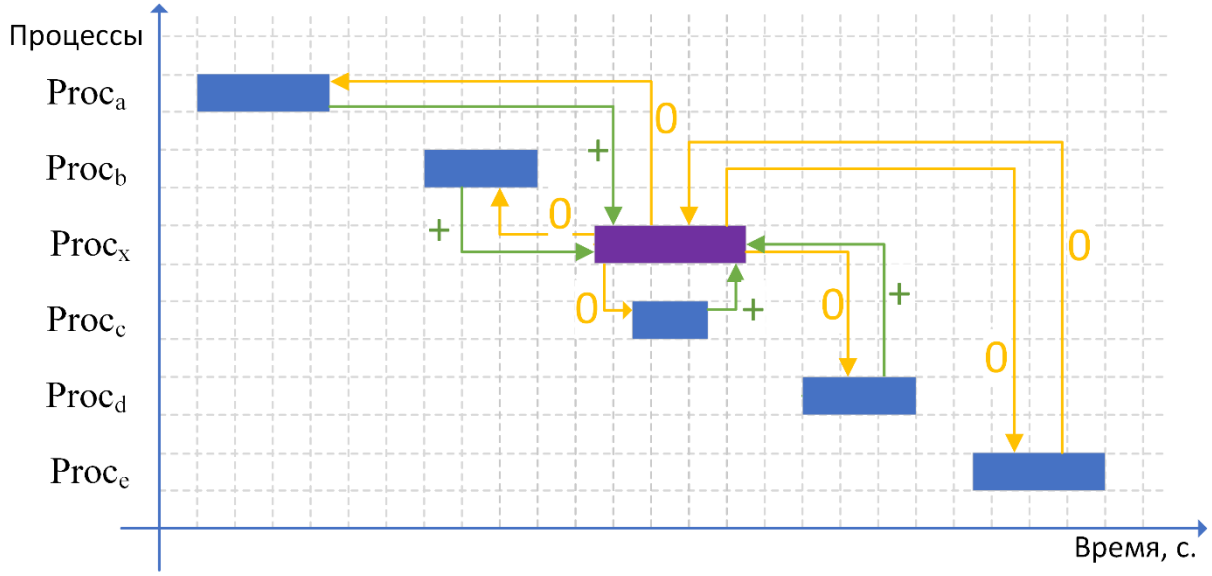

Рис. 5. – Временная диаграмма выполнения процессов тип 3 комменсализм

Тип 4 Паразитизм (+|–) – характеризуется извлечением выгоды от сосуществования одним организмом, используя при этом другого как источник питания, среду обитания и т.п., возлагая на него часть своих отношений с внешней средой (рис.6).

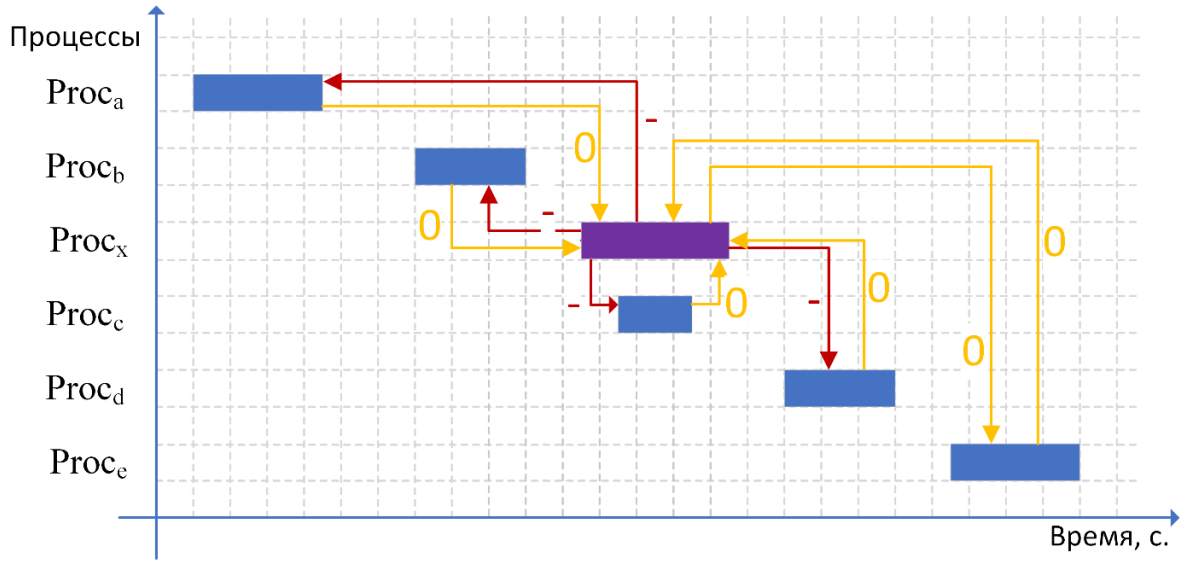

Рис. 6. – Временная диаграмма выполнения процессов тип 4 паразитизм

Тип 5 Хищничество (+|–). Данный тип характеризуется тем, что один организм питается частями другого при отсутствии каких-либо симбиотических (то есть взаимовыгодных) отношений и зачастую с умерщвлением первым второго (рис.7).

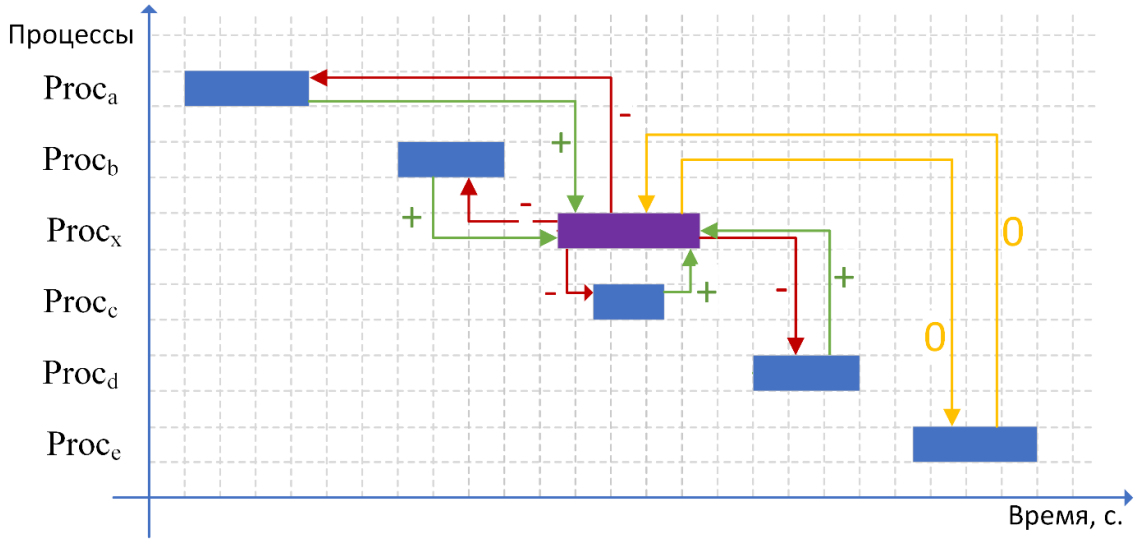

Рис. 7. – Временная диаграмма выполнения процессов тип 5 хищничество

Тип 6 Нейтрализм (0|0) – характеризуется отсутствием каких-либо воздействий друг на друга (рис.8).

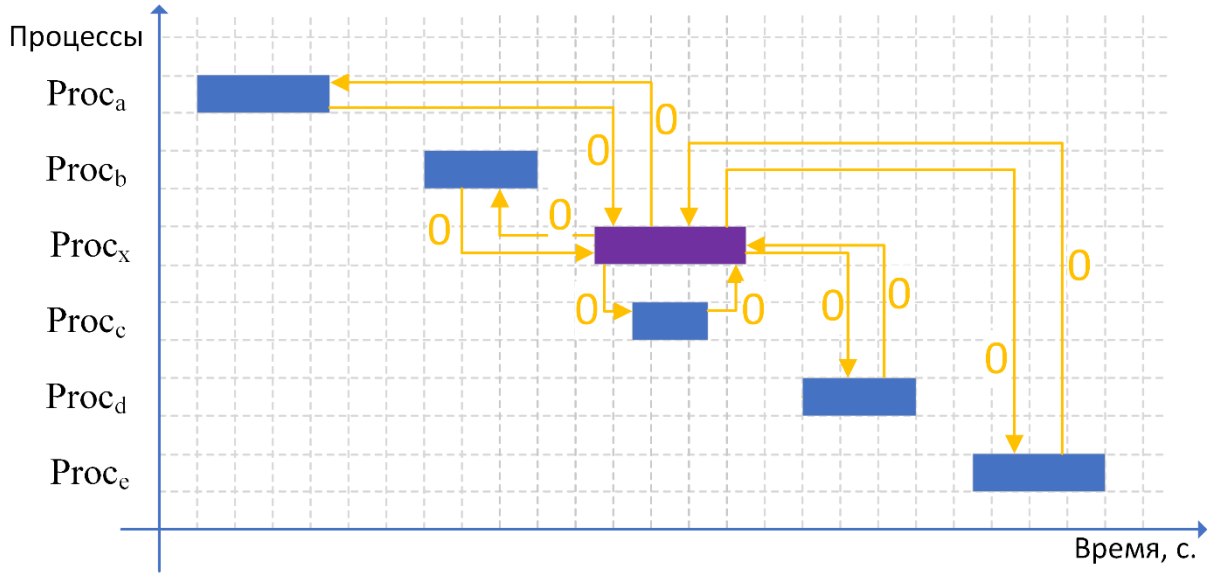

Рис. 8. – Временная диаграмма выполнения процессов тип 6 нейтрализм

Тип 7 Аменсализм (0|–). Данный тип характеризуется отрицательным влиянием одного организма на другого, не испытывая при этом какого-либо обратного влияния (рис.9).

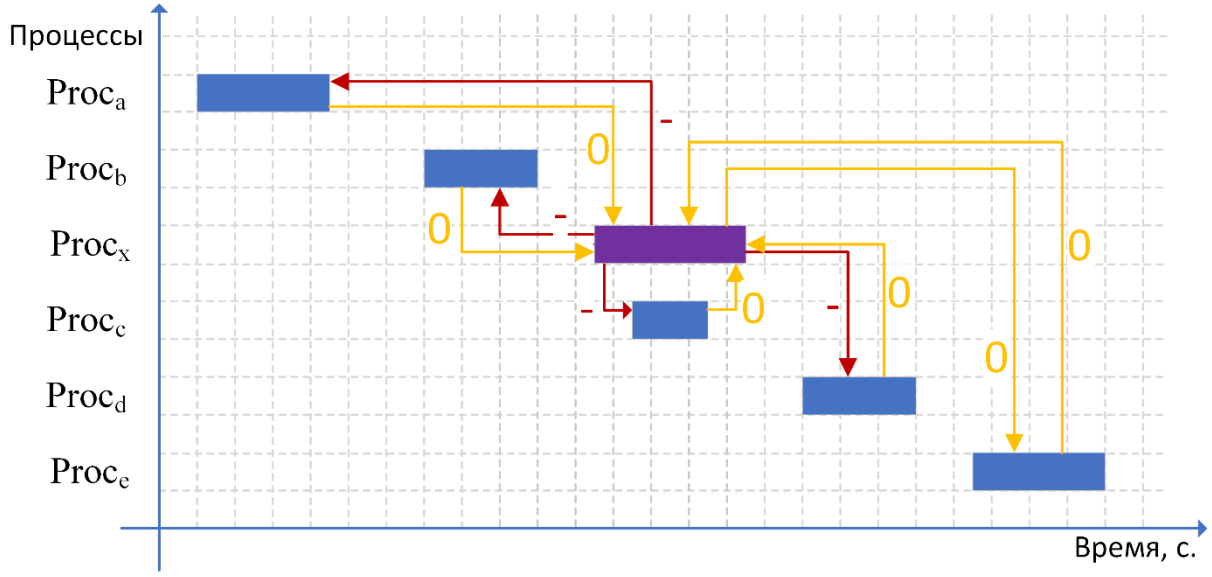

Рис. 9. – Временная диаграмма выполнения процессов тип 7 аменсализм

Тип 8 Аллелопатия (–|–) – характеризуется взаимно-вредным влиянием организмов друг на друга (рис.10).

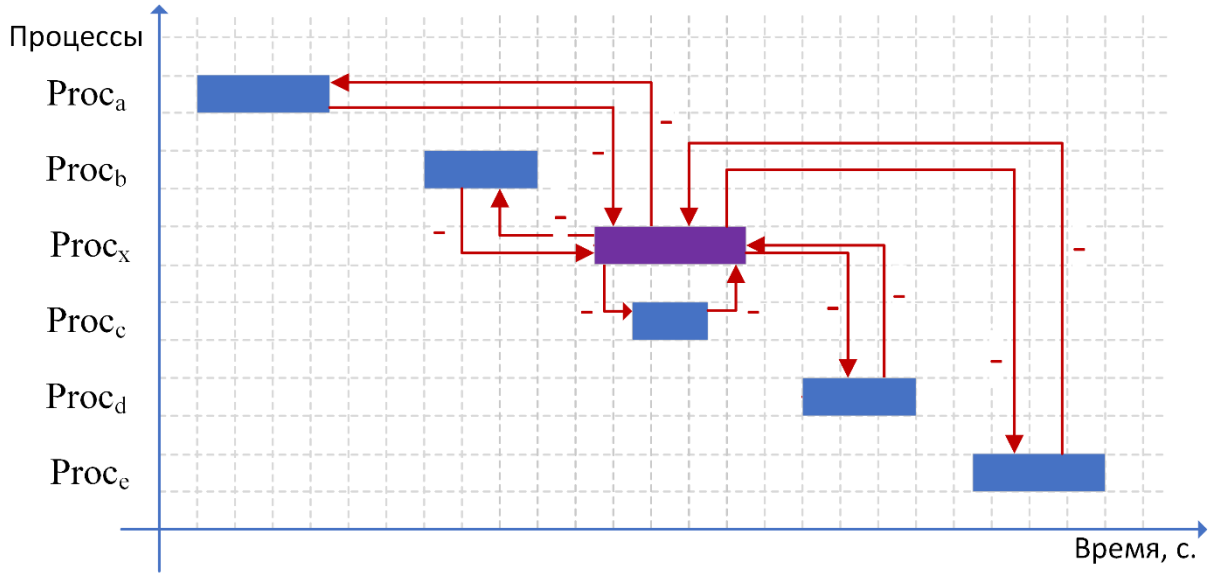

Рис. 10. – Временная диаграмма выполнения процессов тип 8 аллелопатия

Тип 9 Конкуренция (–|–). Данный тип характеризуется косвенным отрицательным влиянием организмов друг на друга по причине борьбы за общие ресурсы (рис.11).

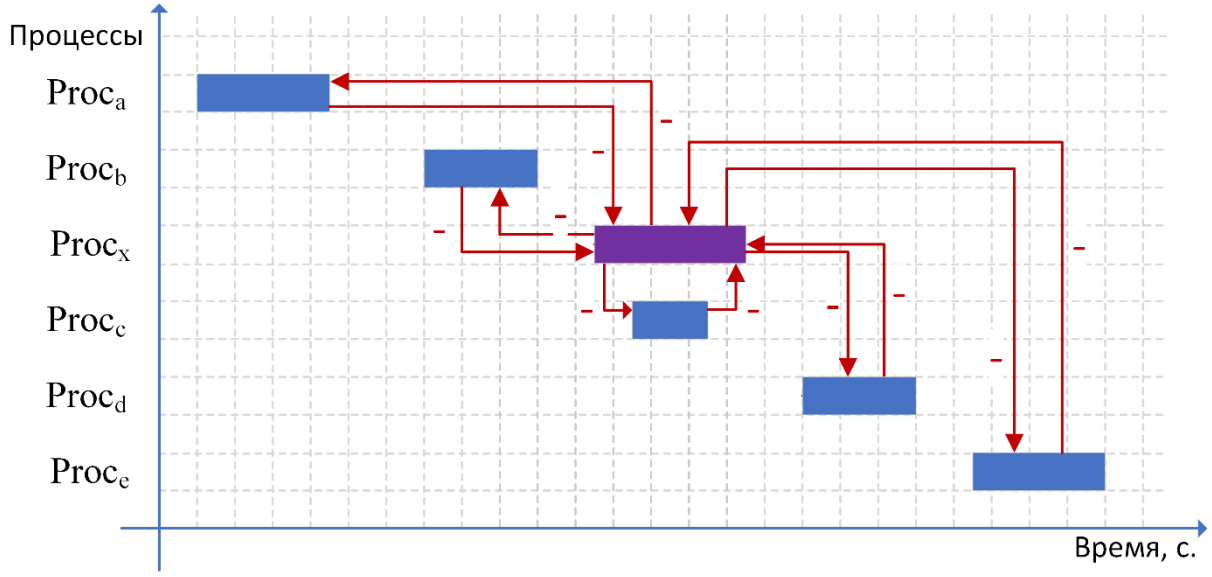

Рис. 11. – Временная диаграмма выполнения процессов тип 9 конкуренция

Временные диаграммы выполнения процессов (рис.3-11) выполнены с использованием элементов описания схем теории автоматического управления [10]. Временная последовательность выполнения процессов задается расположением процессов на диаграмме слева направо. На основе временных диаграмм выполнения процессов построен комплекс антропоморфических поведенческих моделей.

Разработанный комплекс антропоморфических поведенческих моделей процессов позволяет количественно оценить наличие определённых антропоморфических типов процессов в информационной инфраструктуре. Данный подход предлагается использовать как метрику «здоровья» инфраструктуры в системе мониторинга информационной безопасности.

Для прогнозирования рисков инфраструктурного деструктивизма исследуется динамика возникновения негативных поведенческих процессов. Для удобства отображения результатов предлагается объединить типы антропоморфического взаимодействия процессов в группы и классифицировать динамику взаимного влияния сервисов:

- «положительное»: тип 1 облигатный симбиоз, тип 2 факультативный симбиоз, тип 3 комменсализм;
- «нейтральное»: тип 4 нейтрализм;
- «отрицательное»: тип 5 паразитизм, тип 6 хищничество, тип 7 аменсализм, тип 8 аллелопатия, тип 9 конкуренция

Таким образом применив данную классификацию, повышается наблюдаемость поведенческой активности процессов сервисов инфраструктуры.

Заключение

В ходе исследования предложена модель взаимодействия сервисов в информационной инфраструктуре, на базе которой синтезирован комплекс

антропоморфических моделей поведенческого анализа процессов. Предложенные типы антропоморфических поведенческих взаимодействий проанализированы и из них выделены группы для описания взаимного влияния сервисов: «положительная», «отрицательная» и «нейтральная». Используя предложенные группы сформирована, метрика «здоровья» инфраструктуры, которую предлагается использовать в системе мониторинга информационной безопасности.

Благодаря наглядности представления метрики «здоровья» инфраструктуры появляется возможность оценивать тренды антропоморфических типов поведения процессов и прогнозировать появление критических «отрицательных» активностей и тем самым прогнозировать увеличение вероятности появления эффектов инфраструктурного деструктивизма. Данная метрика также детектирует нарушения в состоянии систем, подозрительную активность взаимодействия сервисов и осуществляет динамическую оценку угроз инфраструктурного деструктивизма и аномалий. Предложенное решение повышает эффективность работы центра обеспечения безопасности, позволяя своевременно выявлять признаки начинающегося саморазрушения информационной инфраструктуры.

Литература

1. Чибинев Н.Н., Ляшенко Н.В. Кибератака как новый вид чрезвычайных ситуаций // Инженерный вестник Дона, 2024, №7. URL: ivdon.ru/ru/magazine/archive/n7y2024/9323.

2. Головина Е. Ю., Журавлева А. В., Татарникова Л. И. Оценка состояния безопасности ИТ-инфраструктуры в организации // Молодежный вестник ИрГТУ. 2022. Т. 12, № 2. С. 266-272.

3. Курейчик В.М., Сахарова О.Н., Пирожков С.С. Угрозы в области хранения данных // Инженерный вестник Дона, 2021, №7. URL: ivdon.ru/ru/magazine/archive/n7y2021/7111.

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

5. Максимова Е. А. Оценка информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях. Волгоград: Волгоградский государственный университет, 2020. 95 с.

6. Maksimova E. A., Rusakov A. M., Lapina M. A.,. Lapin V. G. Anthropomorphic Model of States of Subjects of Critical Information Infrastructure Under Destructive Influences // Lecture Notes in Networks and Systems. 2022. V. 424. pp. 569-580.

7. Максимова Е. А., Буйневич М. В. Метод оценки инфраструктурной устойчивости субъектов критической информационной инфраструктуры // Вестник УрФО. Безопасность в информационной сфере. 2022. № 1(43). С. 50-63.

8. 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.

9. 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.

10. Knorn S., Varagnolo D. Automatic control: The natural approach for a quantitative-based personalized education // IFAC-PapersOnLine. 2020. V. 53. №2. pp. 17326-17331.

References

1. Chibinev N.N., Lyashenko N.V. Inzhenernyj vestnik Dona, 2024, №7. URL: ivdon.ru/ru/magazine/archive/n7y2024/9323.

2. Golovina E. Yu., Zhuravleva A. V., Tatarnikova L. I. Molodezhnyy vestnik IrGTU. 2022. V. 12, № 2. pp. 266-272.

3. Kureychik V.M., Sakharova O.N., Pirozhkov S.S. Inzhenernyj vestnik Dona, 2021, №7. URL: ivdon.ru/ru/magazine/archive/n7y2021/7111.

4. Rinaldi S. M., Peerenboom J. P., Kelly T. K. IEEE control systems magazine. 2001. V. 21. №. 6. pp. 11-25.

5. Maksimova E. A. Otsenka informatsionnoy bezopasnosti sub"ekta kriticheskoy informatsionnoy infrastruktury pri destruktivnykh vozdeystviyakh [Assessment of information security of the subject of critical information infrastructure under destructive influences]. Volgograd: Volgogradskiy gosudarstvennyy universitet, 2020. 95 p.

6. Maksimova E. A., Rusakov A. M., Lapina M. A., Lapin V. G. Lecture Notes in Networks and Systems. 2022. V. 424. pp. 569-580.

7. Maksimova E. A., Buynevich M. V. Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. 2022. № 1(43). pp. 50-63.

8. Buynevich M.V., Izrailov K.E. Zashchita informatsii. Insayd. 2019. № 5 (89). pp. 78-85.

9. Buynevich M.V., Izrailov K.E. Zashchita informatsii. Insayd. 2019. № 6(90). pp. 61-65.

10. Knorn S., Varagnolo D. IFAC-PapersOnLine. 2020. V. 53. №2. pp. 17326-17331.

Дата поступления: 23.10.2024

Дата публикации: 30.11.2024