Вестник Астраханского государственного технического университета.
Серия: Управление, вычислительная техника и информатика. 2024. № 3
Vestnik of Astrakhan State Technical University.
Series: Management, computer science and informatics. 2024. N. 3
ISSN 2072-9502 (Print), ISSN 2224-9761 (Online)

КОМПЬЮТЕРНОЕ ОБЕСПЕЧЕНИЕ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

COMPUTER ENGINEERING AND SOFTWARE

Научная статья
УДК 004.942
https://doi.org/10.24143/2072-9502-2024-3-56-64
EDN QUQAMG

Особенности оценки вредоносной активности в инфраструктуре Умного города на основе гранулирования информации и гранулярных моделей вычислений

Игорь Витальевич Котенко, Игорь Борисович Паращук ✉

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук,
Санкт-Петербург, Россия, shchuk@rambler.ru ✉

Аннотация. Объектом исследования является новый методологический подход к гранулированию информации, а также к построению и применению гранулярных моделей вычислений как к новому математическому и методологическому инструментарию повышения точности идентификации и оценки уровня вредоносной активности в инфраструктуре Умного города. Предложенный подход основан на практическом приложении элементов теории нечетких множеств в сочетании с элементами информационного гранулирования к задачам оценки признаков вредоносной активности. Произведен подробный анализ отличительных черт этого подхода, определяющих целесообразность и условия его применения для идентификации и оценки уровня вредоносной активности в инфраструктуре Умного города. Изучены и описаны теоретические аспекты применения гранулирования информации и гранулярных моделей вычислений в задачах оценки вредоносной активности, сочетающей различные признаки для различных категорий потенциальных угроз инфраструктуре и субъектам Умного города: категорий «кибератака», «вредоносная вирусная угроза» или «утечка (потеря) данных». Проведен анализ особенностей предложенного подхода, позволяющего учитывать мнения экспертов и устранять нечеткость, связанную с зашумленностью, неупорядоченностью и неформализованностью данных наблюдения, собираемых и предварительно обрабатываемых в интересах оценки угроз и последствий негативного проявления вредоносной активности. Выработана и детально изложена последовательность вычислений и аналитические выражения для расчета оценочных значений признаков наличия вредоносной активности для различных категорий потенциальных угроз инфраструктуре и субъектам Умного города. Подход предполагает практическую возможность оценки признаков вредоносной активности с использованием информационных гранул, образованных на основе учета минимального численного расстояния между значениями функций принадлежности, характеризующими нечетко заданные данные о наличии либо отсутствии наблюдаемых признаков (атрибутов) вредоносной активности, а также гранулярного суммирования и определения функции следа гранулярной суммы. При этом предложенный подход позволяет получать оценки признаков вредоносной активности, адекватные задачам мониторинга политики безопасности Умного города и в конечном итоге обеспечивает повышение достоверности проактивного контроля угроз и анализа возможных последствий негативного проявления подозрительной активности.

Ключевые слова: инфраструктура Умного города, вредоносная активность, оценка, угроза, признак, гранулирование информации, гранулярная модель вычислений

Благодарности: работа выполнена за счет гранта Санкт-Петербургского научного фонда № 23-РБ-01-09.

Для цитирования: *Котенко И. В., Паращук И. Б.* Особенности оценки вредоносной активности в инфраструктуре Умного города на основе гранулирования информации и гранулярных моделей вычислений // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2024. № 3. С. 56–64. https://doi.org/10.24143/2072-9502-2024-3-56-64. EDN QUQAMG.

Original article

Features of the assessment of malicious activity in the Smart City infrastructure based on information granulation and fuzzy granular calculations

Igor V. Kotenko, Igor B. Parashchuk✉

St. Petersburg Federal Research Center of the Russian Academy of Sciences,
Saint Petersburg, Russia, shchuk@rambler.ru✉

Abstract. The object of the research is a new methodological approach to information granulation and fuzzy granular calculations, as a mathematical and methodological tool for improving the reliability of assessing the level of information security of the Smart City infrastructure. The proposed approach is one of the options for the practical application of elements of the theory of fuzzy sets in the tasks of search, identification and current assessment of signs of time-bearing activity. A detailed analysis of the features of this approach has been carried out, determining the expediency and conditions of its application for assessing malicious activity in the infrastructure of a Smart City. The theoretical aspects of the application of information granulation and fuzzy granular computing to the assessment of malicious activity combining various signs for various categories of potential threats to the infrastructure and subjects of a Smart City - the categories “cyberattack”, “malicious virus threat” or “data leakage (loss)” are studied and described. The analysis of the features of the proposed approach is carried out, which allows taking into account the opinions of experts and eliminating the vagueness associated with noise, disorder and lack of formalization of surveillance data collected and pre-processed in the interests of assessing threats and consequences of negative manifestations of malicious activity. A sequence of calculations and analytical expressions for calculating the estimated values of signs of harmful activity for various categories of potential threats to the infrastructure and subjects of a Smart City has been developed and described in detail. The approach assumes the practical possibility of evaluating signs of malicious activity using information granules formed on the basis of a minimum numerical distance between the values of membership functions characterizing vaguely specified data on the presence or absence of observed signs (attributes) of malicious activity, as well as granular summation and determination of the trace function of the granular sum. At the same time, the proposed approach makes it possible to obtain estimates of signs of malicious activity that are adequate to the tasks of monitoring the Smart City security policy and, ultimately, provides increased reliability of proactive threat control and analysis of the possible consequences of a negative manifestation of suspicious activity.

Keywords*:* Smart City infrastructure, malicious activity, assessment, threat, feature, information granulation, fuzzy granularity calculation

Acknowledgment: the work was carried out at the expense of a grant from the St. Petersburg Scientific Foundation No. 23-RB-01-09.

For citation: Kotenko I. V., Parashchuk I. B. Features of the assessment of malicious activity in the Smart City infrastructure based on information granulation and fuzzy granular calculations. *Vestnik of Astrakhan State Technical University. Series: management, computer science and informatics*. 2024;3:56-64. (In Russ.). https://doi.org/10.24143/2072-9502-2024-3-56-64. EDN QUQAMG.

Введение

Инфраструктура Умного города представляет собой взаимоувязанный комплекс методов, форм, процедур, процессов, а также частных структур или объектов (зданий, сооружений, систем коммуникаций и т. п.), способных удовлетворять ежедневные и долгосрочные запросы субъектов Умного города с точки зрения обеспечения общей среды и факторов их существования, а также условий нормального естественного и эффективного функционирования экономической, социальной, экологической и иных областей жизнедеятельности Умного города, его совершенствования (развития) и воспроизводства [1–5]. По сути, это совокупность взаимосвязан-

ных и коррелированных структур, процессов и (или) объектов, составляющих и обеспечивающих основу функционирования Умного города [6–8].

Проблемы, обуславливаемые сложной физической сущностью, многогранным типажом, комплексным характером и высокой потенциальной опасностью существующих и предполагаемых эвентуальных угроз безопасности инфраструктуре Умного города, в последнее время ежедневно и повсеместно углубляются и расширяются. Это могут быть угрозы социокультурного плана, направленные на нарушение общественно-культурного уклада жизни в Умном городе, или компьютерные атаки, попытки кражи данных либо иные угрозы, предпосылками успешной реализации которых потенциальными нарушителями выступают признаки вредоносной информации.

При этом все эти типы угроз могут быть осуществлены нарушителями порознь или одновременно в разнообразных комбинациях. Многообразие типов и многогранность, комплексность потенциального воздействия угроз безопасности инфраструктуре Умного города как сложной киберфизической системе обусловлены разнообразием и изобилием видов субъектов и объектов, генерирующих эти угрозы. Это либо отдельные люди (либо группы хакеров) вне или внутри самого Умного города, либо организации и враждебные группы, реализующие целенаправленную политику недружественного нам государства. В последнем случае инфраструктуре Умного города противостоит значительно более существенный ресурс для реализации угроз в рамках информационного (или гибридного) противоборства между государствами, поставившими перед собой цель разрушить информационные либо иные критические инфраструктуры друг друга [9–11].

Таким образом, представляется значимым и актуальным создание продуктивных алгоритмов и математических методов оценки вредоносной активности (ВА) для упреждающей защиты информации, хранящейся, обрабатываемой и циркулирующей по каналам и трактам инфраструктуры такого класса. Решение подобных задач позволит максимально точно в отведенные сроки, полноценно выявить и идентифицировать угрозы, оценить степень рисков и потенциальный уровень защищенности инфраструктуры Умного города, а также упреждать действия субъектов угрозы и предпринимать превентивные меры защиты.

Анализ релевантных работ

Созданию способов построения аутентичных и продуктивных алгоритмов и математических методов оперативной и достоверной оценки ВА в инфраструктуре сложных организационно-технических объектов, функционирующих на многоуровневых аппаратно-программных платформах современных киберфизических систем, уделено достаточно много внимания в большом числе современных научно-исследовательских работ [9–21]. Эти работы в основном нацелены на теоретическую и практическую реализацию возможных подходов к поиску, идентификации и количественной (либо качественной) оценке ВА такого рода. Результаты этих исследований, безусловно, обладают новизной и иными достоинствами, но не всегда реализуемы в рамках практической деятельности должностных лиц, отвечающих за обеспечение политики безопасности. Более того, ряд предлагаемых в этих исследованиях подходов нередко несостоятельны с точки зрения реальных задач, решаемых в рамках оценки процессов такого рода с учетом неопределенности, нечеткости исходных данных.

Типовой мониторинг рисков кибербезопасности для объектов инфраструктуры Умного города и входящих в их состав промышленных подсистем автоматизации хорошо описан, например в работах [9–11], где исследуемые процедуры контроля потенциальной ВА предложено реализовать с учетом технологических особенностей таких сложных киберфизических систем и, в частности, особенностей современных беспроводных сенсорных сетей. Но практическая реализация таких методов связана с необходимостью создания сложной и дорогостоящей разветвленной сети сенсоров (датчиков) контроля параметров (количественных значений признаков) ВА.

Работы [12, 13] рассматривают понятийные аспекты ВА, под которой предложено понимать сетевую активность вредоносного программного обеспечения и потенциальных нарушителей. Кроме того, в этих работах исследованы подходы к анализу кибербезопасности с использованием комплексного контроля и «сшивания» сигналов от сенсоров (датчиков) контроля признаков ВА, причем особое внимание уделено получению выводов на основе моделирования. Но эти подходы неработоспособны без сбора статистики о потоках и группировании признаков ВА, что крайне негативно сказывается на оперативности оценки.

В работах [14, 15] много внимания уделено теоретическим и практическим инструментам повышения достоверности оценки потенциальных угроз кибербезопасности, реализацию которых может вызвать игнорирование признаков ВА. Но применяемый для этого критерий достоверности оценки угроз, математически интерпретируемый как дисперсия ошибки оценивания, почти непригоден для современных высокоточных систем оценки признаков ВА в инфраструктуре Умного города, где достоверность анализа признаков подозрительной ак-

тивности играет ключевую роль и учитывает неопределенность, нечеткость исходных данных.

Повышение достоверности оценки признаков ВА в инфраструктуре Умного города с учетом неопределенности данных мониторинга может быть реализовано, например, на основе использования нейронных сетей [16–18]. Такие математические и методологические приемы позволяют сглаживать, нивелировать, а в идеале – устранять неполноту и противоречивость исходных данных, но требуют дополнительных ресурсов (временных, вычислительных) на обучение нейронных сетей.

Применение методов адаптивной оптимальной фильтрации [19–21] позволяет частично снять проблему учета неопределенности. Но в условиях, когда априорная информация недоступна, необходимо обеспечить дополнительные, незашумленные, достоверные каналы наблюдения за параметрами (количественными значениями признаков) ВА в инфраструктуре Умного города.

Вместе с тем по-прежнему актуальной остается проблема учета при оценке признаков ВА в инфраструктуре Умного города нечетких наблюдаемых исходных данных об этих признаках и мнений экспертов об их потенциальной опасности. Эта проблема связана с нечеткостью, физически обусловленной зашумленностью, неупорядоченностью и, зачастую, неформализованностью процедур сбора, предобработки и окончательного формирования данных наблюдения в интересах оценки угроз и последствий негативного проявления ВА.

Учитывая вышеизложенное, можно утверждать, что результаты анализа релевантных работ позволяют говорить об актуальности и объективной потребности в теоретической и практической разработке методов и алгоритмов оценки ВА в инфраструктуре Умного города на случай учета нечетких наблюдаемых исходных данных и мнений специалистов – экспертов в вопросах кибербезопасности.

Математической и методологической основой разработки таких методов и алгоритмов оценки ВА могут служить постулаты гранулирования информации и построения гранулярных моделей вычислений [22–27].

Теоретические аспекты гранулирования информации и построения гранулярных моделей вычислений для задач оценки вредоносной активности

Известно, что ВА для различных категорий потенциальных угроз инфраструктуре и субъектам Умного города, например категорий «кибератака», «вредоносная вирусная угроза» или «утечка (потеря) данных», обладает рядом количественных или качественных признаков (атрибутов), характеризующих, соответственно, деятельность вредоносных программ, хакеров или набор характерных черт потенциальных компьютерных атак.

С помощью выявления определенных подобных ранних признаков ВА, достоверно и своевременно идентифицируя (обнаруживая, оценивая, распознавая) их, стремятся оценить степень рисков и повысить потенциальный уровень защищенности инфраструктуры Умного города [28, 29].

Оценку ВА следует производить, принимая во внимание динамику изменения во времени условий функционирования субъектов и объектов инфраструктуры Умного города, с учетом нечеткости исходных данных, требуемых для принятия решения по точной, однозначной идентификации угроз защищенности киберфизических систем такого класса [30]. Так, например, признаками (атрибутами) ВА с точки зрения угроз инфраструктуре Умного города из категории «кибератака» могут выступать нечеткие величины: $\tilde{\Im}_{\text{ск. тр}}$ – нечеткое множество признаков сканирования нарушителем информационного трафика инфраструктуры Умного города (входящего и исходящего) на наличие уязвимостей; $\tilde{\Im}_{\text{уч. дан}}$ – нечеткое множество признаков утечки, активного сбора или покупки в сети сторонними лицами (или ботами) информации о субъектах инфраструктуры, учетных данных персонала Умного города (комплексная проверка персонала, разведка организации Умного города, на которую нацелена кибератака); $\tilde{\Im}_{\text{ут. уязв}}$ – нечеткое множество признаков утечки, кражи, активного сбора или приобретения в сети сторонними лицами (или ботами) информации о потенциальных уязвимостях инфраструктуры Умного города – о скомпрометированных устройствах, уязвимостях программного обеспечения и т. п. [31].

Факты и анализ современных работ в данной области свидетельствуют о том, что помочь при решении задач идентификации подобных признаков (атрибутов) ВА могут и должны новые, инновационные практики, ориентированные, например, на математический аппарат гранулирования информации (ГрИ) и гранулярные модели вычислений (ГрМВ) в нечеткой среде [22–27].

Анализ работ [22–26], посвященных проблемам и потенциальным перспективам практического применения ГрИ и ГрМВ, показывает, что могут и должны быть использованы подходы, позволяющие на их основе математически корректно упорядочивать массивы нечетко заданных данных, соединяя, «сводя» их по принципу семантического и функционального сходства в специальные изолированные группы информационных структур (объектов, данных) – «информационные гранулы».

Алгоритмы ГрИ и расчеты, основанные на ГрМВ, в задачах интеллектуальной обработки данных в рамках оценки ВА в инфраструктуре Умного города включают две фазы вычислений.

Первая фаза алгоритма и расчетов, основанных на ГрМВ, применяемых в рамках оценки ВА в инфраструктуре Умного города, представляет собой реализацию процедуры собственно гранулирования информации. Ее сущность, физическая и математическая природа заключаются в группировании, соединении, «сведении» значительных массивов исходных данных о значениях признаков (атрибутов) ВА, заданных (наблюдаемых) нечетко, в информационные гранулы по принципу функционального сходства, в результате чего на основе алгоритма ГрИ определяется, к какому нечеткому множеству конкретное нечеткое число (исходные данные) математически «близко» и, как следствие, функционально «стремится». В итоге одна конкретная информационная гранула вмещает информационные объекты – нечеткие данные с наименьшим «расстоянием» между значениями их функций принадлежности.

$$\tilde{X}_{\tilde{\Im}_{\text{ск. тр}}} \text{ gran } X^{g}_{\tilde{\Im}_{\text{ск. тр}}} \Leftrightarrow (\min f_{\tilde{\Im}_{\text{ск. тр}}}(\mu_1^{(x)}, \ldots, \mu_m^{(x)}));$$

$$\tilde{Y}_{\tilde{\Im}_{\text{ск. тр}}} \text{ gran } Y^{g}_{\tilde{\Im}_{\text{ск. тр}}} \Leftrightarrow (\min f_{\tilde{\Im}_{\text{ск. тр}}}(\mu_1^{(y)}, \ldots, \mu_m^{(y)})),$$

где $\tilde{X}_{\tilde{\Im}_{\text{ск. тр}}}$ и $\tilde{Y}_{\tilde{\Im}_{\text{ск. тр}}}$ – нечеткие множества, сгруппированные в информационные гранулы $X^{g}_{\tilde{\Im}_{\text{ск. тр}}}$ и $Y^{g}_{\tilde{\Im}_{\text{ск. тр}}}$ и олицетворяющие мнения экспертов о наличии либо отсутствии наблюдаемых признаков ВА типа $\tilde{\Im}_{\text{ск. тр}}$; x и y – условное математическое обозначение элементов этих соответствующих нечетких множеств – конкретные признаки ВА из состава $\tilde{\Im}_{\text{ск. тр}}$, т. е., например, x – это признак сканирования нарушителем входящего информационного трафика инфраструктуры Умного города на наличие уязвимостей, а y – признак сканирования нарушителем исходящего трафика; gran – символ гранулирования.

Процедура реализации классических гранулярных вычислений составляет основу второй фазы алгоритма ГрИ и расчетов, основанных на ГрМВ, применяемых в рамках оценки ВА в инфраструктуре Умного города. Эта процедура позволяет последовательно вычислять гранулярную сумму, затем – функции следа гранулярной суммы. Сущность данной процедуры заключается в математической обработке суммы весов информационных гранул в интересах определения тенденции проявления признаков ВА и оценки уровня ВА в инфраструктуре Умного города.

Вторая фаза алгоритма ГрИ и расчетов, основанных на ГрМВ, применяемых в рамках оценки ВА в инфраструктуре Умного города, представляет собой реализацию собственно гранулярной модели вычислений. Данная процедура включает гранулярное суммирование и исчисление функции следа («трека») гранулярной суммы.

Методологические особенности процедур гранулирования информации и построения гранулярных моделей вычислений для получения оценок вредоносной активности

С учетом особенностей решаемой задачи в рамках первой фазы, например, две гранулы, образованные по принципу наименьшего «расстояния» между значениями функций принадлежности, определяющими нечеткие исходные данные о наличии либо отсутствии наблюдаемых признаков (атрибутов) ВА $\tilde{\Im}_{\text{ск. тр}}$ – признаков сканирования нарушителем информационного трафика на наличие уязвимостей в инфраструктуре Умного города (признаки ВА из категории «кибератака»), могут быть описаны на основе выражений

Гранулярное суммирование, осуществляемое в рамках этой фазы исследований, позволяет математически корректно реализовать «объединение» нескольких мнений специалистов о факте присутствия или отсутствия наблюдаемых признаков (атрибутов) ВА типа $\tilde{\Im}_{\text{ск. тр}}$ на основе дефаззификации и дальнейшего нечетко-гранулярного объединения нечетких множеств. Для нашего примера, для двух нечетких множеств $\tilde{X}_{\tilde{\Im}_{\text{ск. тр}}}$ и $\tilde{Y}_{\tilde{\Im}_{\text{ск. тр}}}$, элементы x и y которых характеризуют, соответственно, наблюдаемые признаки сканирования нарушителем входящего и исходящего трафика инфраструктуры Умного города на наличие уязвимостей

$$Q^{g(x,y)}_{\tilde{\Im}_{\text{ск. тр}}} = X^{g(x)}_{\tilde{\Im}_{\text{ск. тр}}} +_g Y^{g(y)}_{\tilde{\Im}_{\text{ск. тр}}},$$

где $\{+_g\}$ – условный математический признак гранулярного суммирования [23, 27].

Вслед за этим вычисляются функции следа («треки») гранулярной суммы для отдельных конкретных информационных гранул $X^{g}_{\tilde{\Im}_{\text{ск. тр}}}$ и $Y^{g}_{\tilde{\Im}_{\text{ск. тр}}}$. Например, для гранулы $X^{g(x)}_{\tilde{\Im}_{\text{ск. тр}}}$, входящей в состав $\tilde{\Im}_{\text{ск. тр}}$ и содержащей признаки (x) сканирования нарушителем входящего трафика, след («трек»)

гранулярной суммы определяется в соответствии с выражением

$$\text{tr}\ \tilde{\Im}^{(x)}_{\text{ск. тр}} = \left(\sum_{i=1}^{3} (\tilde{\Im}^{(x_i)}_{\text{ск. тр}})^2 + \mu_i^2 \right)^{\frac{1}{2}},$$

где $\text{tr}\ \tilde{\Im}^{(x)}_{\text{ск. тр}}$ – след («трек») гранулярной суммы для гранулы $X^{g(x)}_{\tilde{\Im}_{\text{ск. тр}}}$, хранящей, например, три элемента, три разноречивых, зачастую несовпадающих мнения экспертов об объективном существовании в наблюдаемых и контролируемых данных конкретного признака (x) – «симптома» сканирования нарушителем входящего информационного трафика инфраструктуры Умного города на наличие уязвимостей.

Далее осуществляется процедура поиска минимума в гранулах $X^{g(\mu)}_{\tilde{\Im}_{\text{ск. тр}}}$ и $Y^{g(\mu)}_{\tilde{\Im}_{\text{ск. тр}}}$, характеризующих, в этом случае, не нечеткие данные (мнения) о существовании в наблюдаемых и контролируемых данных конкретного признака ВА (x), а значения их функций принадлежности

$$Q^{g(\mu)}_{\tilde{\Im}_{\text{ск. тр}}} = \min\,(X^{g(\mu)}_{\tilde{\Im}_{\text{ск. тр}}},\ Y^{g(\mu)}_{\tilde{\Im}_{\text{ск. тр}}}).$$

В качестве итоговых расчетов определяют финальный, окончательный результат объединения нескольких мнений экспертов о наличии либо отсутствии наблюдаемых признаков ВА:

$$Q^{g}_{\tilde{\Im}_{\text{ск. тр}}} = [Q^{g(x,\,y)}_{\tilde{\Im}_{\text{ск. тр}}},\ Q^{g(\mu)}_{\tilde{\Im}_{\text{ск. тр}}}] = \begin{pmatrix} \tilde{\Im}^{(x_1)}_{\text{ск. тр}} & +_g\ \tilde{\Im}^{(y_1)}_{\text{ск. тр}} & \min\,(\mu_1^{(x)},\ \mu_1^{(y)}) \\ & \vdots\ \ \vdots\ \ \vdots & \\ \tilde{\Im}^{(x_m)}_{\text{ск. тр}} & +_g\ \tilde{\Im}^{(y_m)}_{\text{ск. тр}} & \min\,(\mu_m^{(x)},\ \mu_m^{(y)}) \end{pmatrix},$$

где $Q^{g}_{\tilde{\Im}_{\text{ск. тр}}}$ – множество, элементы которого характеризуют суммарные, обобщенные (на основе ГрИ и расчетов, основанных на ГрМВ), экспертные мнения о наличии либо отсутствии наблюдаемых признаков ВА типа $\tilde{\Im}_{\text{ск. тр}}$ в инфраструктуре Умного города.

В рамках нашего примера: если элементы множества $Q^{g}_{\tilde{\Im}_{\text{ск. тр}}}$ превышают предварительно заданные пороговые значения $\min\,(X^{g(\mu)}_{\tilde{\Im}_{\text{ск. тр}}},\ Y^{g(\mu)}_{\tilde{\Im}_{\text{ск. тр}}})$, например $\min\mu^{(x)}$ в сравнении с $\min\mu^{(y)}$ превышает величину 0,75 (т. е. $\min\mu^{(x)} \geq 0{,}75$), говорят о безусловном и однозначном наличии в данных наблюдения признаков ВА из состава $\tilde{\Im}_{\text{ск. тр}}$, т. е. об очевидном наличии x – признаков сканирования нарушителем входящего информационного трафика инфраструктуры Умного города на наличие уязвимостей.

В итоге результаты ГрИ и расчетов, основанных на ГрМВ для рассмотренных условий, численно характеризуют детализированные, конкретные значения элементов исходного нечеткого множества, содержащего информацию о наличии ВА для различных категорий потенциальных угроз инфраструктуре и субъектам Умного города, связанных с деятельностью вредоносных программ, хакеров или компьютерными атаками.

Заключение

Рассмотрены математические и методологические основы гранулирования информации, а также этапы реализации моделей и вычислительных алгоритмов нечетко-гранулярных вычислений применительно к задачам оценки вредоносной активности в инфраструктуре Умного города.

Предложенный подход позволяет повысить достоверность оценки наличия вредоносной активности в инфраструктуре Умного города за счет уточнения (верификации) нечетких наблюдаемых исходных данных о признаках такой активности и мнений специалистов. Его применение позволить минимизировать затраты на мониторинг в рамках обеспечения политики безопасности Умного города, учесть опыт специалистов для оценивания возможных негативных последствий реализации угроз Умному городу и расширить область применения относительно новых методов интеллектуального анализа данных – элементов теории нечетких множеств и информационного гранулирования, в рамках методологии преодоления неопределенности, нечеткости признаков подозрительной активности в трафике и иных объектах, субъектах и процессах Умного города.

Рассмотренные методы интеллектуального анализа данных позволяют устранить нечеткость, связанную с зашумленностью, неупорядоченностью и, зачастую, неформализованностью процедур формирования данных измерения и наблюдения в интересах оценки угроз и последствий негативного проявления вредоносной активности в инфраструктуре Умного города.

Практическое применение предложенного подхода к оценке вредоносной активности в инфраструктуре Умного города предполагается не только в рамках научно-исследовательских и опытно-конструкторских работ по построению таких защищен-

ных аппаратно-программных платформ современных киберфизических систем, но и в модулях проактивного контроля информационной безопасности любых сложных информационно-технических систем. Направлением предстоящих исследований в данной области, на наш взгляд, должна быть разработка методов идентификации и прогнозной оценки уровня вредоносной активности, сочетающих гранулярные модели вычислений, нечеткие отношения предпочтения и алгоритмы сравнения нечетких доминирующих альтернатив.

Список источников

1. Chatterjee J. M., Jain V., Kumar V., Sharma B., Shrestha R. Smart City Infrastructure. The Blockchain Perspective. Beverly: John Wiley & Sons Limited, 2022. 380 p.

2. Kamara M. K. Securing Critical Infrastructures. Bloomington: Xlibris US, 2020. 385 p.

3. Mehmood R., See S., Katib I., Chlamtac I. Smart Infrastructure and Applications. Foundations for Smarter Cities and Societies. Cham: Springer Nature Switzerland AG, 2020. 655 p.

4. Suzuki L., Finkelstein A. Data as Infrastructure for Smart Cities. Stevenage: Institution of Engineering and Technology, 2019. 313 p.

5. Vacca J. Solving Urban Infrastructure Problems Using Smart City Technologies. Amsterdam: Elsevier, 2020. 820 p.

6. Паращук И. Б., Чечулин А. А. Нейро-нечеткий метод детектирования уязвимостей для контроля защищенности процессов и средств взаимодействия «человек – интеллектуальная система» в рамках концепции «Smart Transport» // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2023): сб. науч. ст. XII Междунар. науч.-техн. и науч.-метод. конф.: в 4 т. / под ред. С. И. Макаренко. СПб.: Изд-во СПбГУТ, 2023. Т. 1. С. 837–841.

7. Kotenko I. V., Parashchuk I. B. Interval Analysis of Security for Information and Telecommunication Resources of Critical Infrastructures // Society 5.0. Studies in Systems, Decision and Control. Cham: Springer Nature Switzerland AG, 2023. V. 437. P. 241–250.

8. Maheswaran M., Badidi E. Handbook of Smart Cities. Software Services and Cyber Infrastructure. Cham: Springer Nature Switzerland AG, 2018. 406 p.

9. Kotenko I. V., Parashchuk I. B. Analysis of Threats to Information Security of Industrial Automation Systems Using Euclidean and Hamming Distances between Fuzzy Sets // 2023 International Russian Automation Conference (RusAutoCon-2023) (Sochi, 10–16 September 2023). IEEE Xplore Digital Library: Browse Conferences, 2023. N. 10272922. P. 13–18.

10. Kanchan D. K., Kumhar D. Security Threats and Challenges in Smart Cities // Journal of Emerging Technologies and Innovative Research (JETIR). 2018. V. 5. Iss. 8. P. 205–209.

11. Kitchin R., Dodge M. The Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention // Journal of Urban Technology. 2019. V. 26. N. 2. P. 47–65.

12. Gambardella A., State B., Khan N., Tsourides L., Torr P., Baydin A. G. Detecting and Quantifying Malicious Activity with Simulation-based Inference // ICML workshop on Socially Responsible Machine Learning: 38-th International Conference on Machine Learning, 2021. P. 14–28.

13. Karabacak F., Ogras U., Ozev S. Malicious Activity Detection in Lightweight Wearable and IoT Devices Using Signal Stitching // Sensors. 2021. V. 21. N. 3408. P. 1–21.

14. Gabber H. The 2020 CyberSecurity & Cyber Law Guide. N. Y.: Independently published, 2020. 435 p.

15. Allodi L., Cremonini M., Massacci F., Shim W. Measuring the accuracy of software vulnerability assessments: experiments with students and professionals // Empirical Software Engineering. 2020. V. 25. P. 1063–1094.

16. Meeuwisse R. Cybersecurity Exposed: The Cyber House Rules. London: Cyber Simplicity Ltd, 2017. 175 p.

17. Desnitsky V. A., Kotenko I. V., Parashchuk I. B. Neural Network Based Classification of Attacks on Wireless Sensor Networks // 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (St. Petersburg and Moscow, 27–30 Jan. 2020). IEEE Xplore Digital Library, 2020. P. 284–287.

18. Паращук И. Б., Иванов Ю. Н., Романенко П. Г. Нейросетевые методы в задачах моделирования и анализа эффективности функционирования сетей связи. СПб.: ВАС, 2010. 104 с.

19. Haykin S. O. Adaptive Filter Theory. Upper Saddle River, New Jersey: Prentice Hall Inc., 2002. 920 p.

20. Lo J. T.-H. Synthetic approach to optimal filtering // IEEE Trans. Neural Networks. 1994. V. 5. P. 803–811.

21. Parlos A. G., Menon S. K., Atiya A. F. An algorithmic approach to adaptive state filtering using recurrent neural networks // IEEE Trans. Neural Networks. 2001. V. 12 (6). P. 1411–1432.

22. Liang J. Y., Qian Y. H. Information granules and entropy theory in information systems // Science in China Series F: Information Sciences. 2008. V. 51. N. 10. P. 1427–1444.

23. Yao Y. Y. Information granulation and rough set approximation // International Journal of Intelligent Systems. 2001. V. 16. N. 1. P. 87–104.

24. Mikhaylichenko A. V., Parashchuk I. B. Procedures for granular selection of analyzed parameters of technical reliability of modern disk storage systems // International Conference on Advanced InfoTelecommunications (ICAIT-2023). Saint Petersburg: SPbGUT, 2023. V. 1. P. 799–803.

25. Bargiela A., Pedrycz W. Granular Computing. An Introduction. N.Y.: Springer New York, 2012. V. 717. 452 p.

26. Liu H., Cocea M. Granular Computing Based Machine Learning. A Big Data Processing Approach. Cham: Springer International Publishing AG, 2018. 113 p.

27. Михайличенко А. В., Паращук И. Б. Элементы нечетко-гранулярных вычислений в приложении к задачам анализа технической надежности систем распределенной обработки данных // Прикаспийский журнал. Управление и высокие технологии. 2022. № 1 (57). С. 77–84.

28. Dobhal D. C., Sharma S., Purohit K. C., Nautiyal L., Singh K. Cyber Trafficking, Threat Behavior, and Malicious Activity Monitoring for Healthcare Organizations. Hershey: IGI Global, 2023. 206 p.

29. Desnitsky V. A., Kotenko I. V., Parashchuk I. B. Methods of Assessing the Effectiveness of Network Content

Processing Systems for Detecting Malicious Information Taking into Account the Elimination of Uncertainty in the Semantic Content of Information Objects // 2019 XXII International Conference on Soft Computing and Measurements (SCM) (St. Petersburg, 23–25 May 2019). IEEE Xplore Digital Library, 2019. P. 41–44.

30. Котенко И. В., Паращук И. Б. Верификация недостоверных параметров модели обнаружения вредоносной информации // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2019. № 2. С. 7–18.

31. Rid T., Buchanan B. Attributing Cyber Attacks // The Journal of Strategic Studies. 2015. V. 38. N. 1–2. P. 4–37.

References

1. Chatterjee J. M., Jain V., Kumar V., Sharma B., Shrestha R. *Smart City Infrastructure. The Blockchain Perspective*. Beverly, John Wiley & Sons Limited, 2022. 380 p.

2. Kamara M. K. *Securing Critical Infrastructures*. Bloomington, Xlibris US, 2020. 385 p.

3. Mehmood R., See S., Katib I., Chlamtac I. *Smart Infrastructure and Applications. Foundations for Smarter Cities and Societies*. Cham, Springer Nature Switzerland AG, 2020. 655 p.

4. Suzuki L., Finkelstein A. *Data as Infrastructure for Smart Cities*. Stevenage, Institution of Engineering and Technology, 2019. 313 p.

5. Vacca J. *Solving Urban Infrastructure Problems Using Smart City Technologies*. Amsterdam, Elsevier, 2020. 820 p.

6. Parashchuk I. B., Chechulin A. A. Neiro-nechetkii metod detektirovaniia uiazvimostei dlia kontrolia zashchishchennosti protsessov i sredstv vzaimodeistviia «chelovek – intellektual'naia sistema» v ramkakh kontseptsii Smart Transport [Neuro-fuzzy vulnerability detection method for monitoring the security of processes and means of interaction “human – intelligent system” within the framework of the Smart Transport concept]. *Aktual'nye problemy infotelekommunikatsii v nauke i obrazovanii (APINO-2023): sbornik nauchnykh statei XII Mezhdunarodnoi nauchno-tekhnicheskoi i nauchno-metodicheskoi konferentsii: v 4 t. Pod redaktsiei S. I. Makarenko*. Saint Petersburg, Izd-vo SPbGUT, 2023. Vol. 1. Pp. 837-841.

7. Kotenko I. V., Parashchuk I. B. *Interval Analysis of Security for Information and Telecommunication Resources of Critical Infrastructures. Society 5.0. Studies in Systems, Decision and Control*. Cham, Springer Nature Switzerland AG, 2023. Vol. 437. Pp. 241-250.

8. Maheswaran M., Badidi E. *Handbook of Smart Cities. Software Services and Cyber Infrastructure*. Cham, Springer Nature Switzerland AG, 2018. 406 p.

9. Kotenko I. V., Parashchuk I. B. Analysis of Threats to Information Security of Industrial Automation Systems Using Euclidean and Hamming Distances between Fuzzy Sets. *2023 International Russian Automation Conference (RusAutoCon-2023) (Sochi, 10-16 September 2023)*. IEEE Xplore Digital Library, Browse Conferences, 2023. No. 10272922. Pp. 13-18.

10. Kanchan D. K., Kumhar D. Security Threats and Challenges in Smart Cities. *Journal of Emerging Technologies and Innovative Research (JETIR)*, 2018, vol. 5, iss. 8, pp. 205-209.

11. Kitchin R., Dodge M. The Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*, 2019, vol. 26, no. 2, pp. 47-65.

12. Gambardella A., State B., Khan N., Tsourides L., Torr P., Baydin A. G. Detecting and Quantifying Malicious Activity with Simulation-based Inference. *ICML workshop on Socially Responsible Machine Learning: 38-th International Conference on Machine Learning*, 2021. Pp. 14-28.

13. Karabacak F., Ogras U., Ozev S. Malicious Activity Detection in Lightweight Wearable and IoT Devices Using Signal Stitching. *Sensors*, 2021, vol. 21, no. 3408, pp. 1-21.

14. Gabber H. *The 2020 CyberSecurity & Cyber Law Guide*. New York, Independently published, 2020. 435 p.

15. Allodi L., Cremonini M., Massacci F., Shim W. Measuring the accuracy of software vulnerability assessments: ex-periments with students and professionals. *Empirical Software Engineering*, 2020, vol. 25, pp. 1063-1094.

16. Meeuwisse R. *Cybersecurity Exposed: The Cyber House Rules*. London, Cyber Simplicity Ltd, 2017. 175 p.

17. Desnitsky V. A., Kotenko I. V., Parashchuk I. B. Neural Network Based Classification of Attacks on Wireless Sensor Networks. *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (St. Petersburg and Moscow, 27-30 Jan. 2020)*. IEEE Xplore Digital Library, 2020. Pp. 284-287.

18. Parashchuk I. B., Ivanov Iu. N., Romanenko P. G. *Neirosetevye metody v zadachakh modelirovaniia i analiza effektivnosti funktsionirovaniia setei sviazi* [Neural network methods in the tasks of modeling and analyzing the effectiveness of communication networks]. Saint Petersburg, VAS Publ., 2010. 104 p.

19. Haykin S. O. *Adaptive Filter Theory*. Upper Saddle River, New Jersey, Prentice Hall Inc., 2002. 920 p.

20. Lo J. T.-H. Synthetic approach to optimal filtering. *IEEE Trans. Neural Networks*, 1994, vol. 5, pp. 803-811.

21. Parlos A. G., Menon S. K., Atiya A. F. An algorithmic approach to adaptive state filtering using recurrent neural networks. *IEEE Trans. Neural Networks*, 2001, vol. 12 (6), pp. 1411-1432.

22. Liang J. Y., Qian Y. H. Information granules and entropy theory in information systems. *Science in China Series F: Information Sciences*, 2008, vol. 51, no. 10, pp. 1427-1444.

23. Yao Y. Y. Information granulation and rough set approximation. *International Journal of Intelligent Systems*, 2001, vol. 16, no. 1, pp. 87-104.

24. Mikhaylichenko A. V., Rarashchuk I. B. Procedures for granular selection of analyzed parameters of technical reliability of modern disk storage systems. *International Conference on Advanced InfoTelecommunications (ICAIT-2023)*. Saint Petersburg, SPbGUT, 2023. Vol. 1. Pp. 799-803.

25. Bargiela A., Pedrycz W. *Granular Computing. An Introduction*. New York, Springer New York, 2012. Vol. 717. 452 p.

26. Liu H., Cocea M. *Granular Computing Based Machine Learning. A Big Data Processing Approach*. Cham, Springer International Publishing AG, 2018. 113 p.

27. Mikhailichenko A. V., Parashchuk I. B. Elementy nechetko-granuliarnykh vychislenii v prilozhenii k zadacham analiza tekhnicheskoi nadezhnosti sistem raspredelennoi

obrabotki dannykh [Elements of fuzzy-granular calculations in application to the tasks of analyzing the technical reliability of distributed data processing systems]. *Prikaspiiskii zhurnal. Upravlenie i vysokie tekhnologii*, 2022, no. 1 (57), pp. 77-84.

28. Dobhal D. C., Sharma S., Purohit K. C., Nautiyal L., Singh K. *Cyber Trafficking, Threat Behavior, and Malicious Activity Monitoring for Healthcare Organizations*. Hershey, IGI Global, 2023. 206 p.

29. Desnitsky V. A., Kotenko I. V., Parashchuk I. B. Methods of Assessing the Effectiveness of Network Content Processing Systems for Detecting Malicious Information Taking into Account the Elimination of Uncertainty in the Semantic Content of Information Objects. *2019 XXII International Conference on Soft Computing and Measurements (SCM) (St. Petersburg, 23-25 May 2019)*. IEEE Xplore Digital Library, 2019. Pp. 41-44.

30. Kotenko I. V., Parashchuk I. B. Verifikatsiia nedostovernykh parametrov modeli obnaruzheniia vredonosnoi informatsii [Verification of invalid parameters of the malicious information detection model]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2019, no. 2, pp. 7-18.

31. Rid T., Buchanan B. Attributing Cyber Attacks. *The Journal of Strategic Studies*, 2015, vol. 38, no. 1-2, pp. 4-37.

Статья поступила в редакцию 20.03.2024; одобрена после рецензирования 15.05.2024; принята к публикации 11.07.2024
The article was submitted 20.03.2024; approved after reviewing 15.05.2024; accepted for publication 11.07.2024

Информация об авторах / Information about the authors

Игорь Витальевич Котенко – доктор технических наук, профессор; главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности; Санкт-Петербургский Федеральный исследовательский центр Российской академии наук; ivkote@comsec.spb.ru

Игорь Борисович Паращук – доктор технических наук, профессор; ведущий научный сотрудник лаборатории проблем компьютерной безопасности; Санкт-Петербургский Федеральный исследовательский центр Российской академии наук; shchuk@rambler.ru

Igor V. Kotenko – Doctor of Technical Sciences, Professor; Head Researcher and Chief Scientist of the Laboratory of Computer Security Problems; St. Petersburg Federal Research Center of the Russian Academy of Sciences; ivkote@comsec.spb.ru

Igor B. Parashchuk – Doctor of Technical Sciences, Professor; Leading Researcher of the Laboratory of Computer Security Problems; St. Petersburg Federal Research Center of the Russian Academy of Sciences; shchuk@rambler.ru