УДК 004.056.5:510.22

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ АТАКУЮЩЕЙ ПОВЕРХНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ОСНОВЕ ТЕОРИИ МНОЖЕСТВ И ЭКСПЕРТНЫХ ДАННЫХ

А. С. Казарян, А. А. Петросян, Н. Д. Тарасенко

Московский политехнический университет, Россия

E-mail: kazarian.info@gmail.com
E-mail: a.a.petrosyan@mospolytech.ru
E-mail: ntlitaras@gmail.com

АННОТАЦИЯ

Предлагается практический подход к количественной оценке атакующей поверхности автоматизированных систем управления технологическими процессами (АСУ ТП) на основе теории множеств. Модель формализует систему как совокупность множеств компонентов, уязвимостей и векторов атаки, связанных бинарными отношениями. Ключевая метрика — относительный размер атакующей поверхности — рассчитывается как отношение мощности пересечения критических подмножеств к общему числу компонентов системы. На примере абстрактной модели промышленной системы показано, как метод позволяет численно оценить эффект от внедрения мер защиты: применение сегментации сети и установки обновлений снизило коэффициент охвата атакующей поверхности с 0,17 до 0. Подход позволяет формировать измеримое количественное обоснование для инвестиций в кибербезопасность промышленных систем.

Ключевые слова: *атакующая поверхность, количественная оценка, математическое моделирование, метрики безопасности, теория множеств, информационная безопасность*

ABSTRACT

A practical approach for the quantitative assessment of the attack surface in Industrial Control Systems (ICS) based on set theory is proposed. The model formalizes a system as a collection of sets of components, vulnerabilities, and attack vectors connected by binary relations. The key metric — the relative size of the attack surface — is calculated via the cardinality of the intersection of critical subsets. Using an abstract model of an industrial system as an example, it is demonstrated how the method enables a numerical evaluation of the effectiveness of security measures: the implementation of network segmentation and patch installation reduced the Attack Surface Coverage coefficient from 0.17 to 0. The approach provides a measurable quantitative justification for investments in the cybersecurity of industrial systems.

Keywords: *attack surface, quantitative assessment, mathematical modeling, security metrics, set theory, information security*

Введение

Повышение уровня цифровизации промышленности привело к росту числа кибератак на автоматизированные системы управления технологическими процессами (АСУ ТП). Согласно статистике RED Security SOC, в первой половине 2025 года было зафиксировано свыше 63 тысяч кибератак на российские компании, что на 27% превышает показатель

аналогичного периода предыдущего года [1]. Проблема носит глобальный характер: промышленный сектор, включая транспорт и обрабатывающее производство, остается одним из наиболее целенаправленно атакуемых в Европейском союзе, что подчеркивает универсальность задачи оценки и сокращения атакующей поверхности [2].

Анализ атакующей поверхности является этапом оценки защищенности, определяющим совокупность компонентов и интерфейсов системы, через которые потенциально могут быть реализованы угрозы [3]. В классическом формальном определении атакующая поверхность характеризуется как подмножество ресурсов системы, доступных злоумышленнику, что определяет потенциал для атаки [4]. Для целей практической оценки безопасности АСУ ТП, где важна приоритизация исправления известных уязвимостей, в данной работе предлагается сузить это понятие и определять атакующую поверхность как множество компонентов, которые одновременно доступны для атаки извне и содержат известные критические уязвимости (2).

Ряд исследователей указывает на субъективность и расплывчатость понятия «атакующая поверхность», предлагая альтернативные теоретические рамки, такие как концепция «странных машин» (weird machines), которая рассматривает уязвимости как результат расхождения между формальной моделью программы и ее конкретной реализацией [5]. Ранние попытки формализации атакующей поверхности, такие как модель на основе I/O-автоматов, определяли ее через три ключевых ресурса: методы, каналы и данные системы, вводя количественную метрику на основе соотношения потенциального ущерба и усилий злоумышленника [4].

Однако традиционные подходы к оценке защищенности, такие как экспертный анализ и трассировка данных, сталкиваются с двумя ключевыми проблемами применительно к АСУ ТП: высокая субъективность и трудоёмкость [3], а также отсутствие универсальных количественных метрик. Это затрудняет объективное сравнение различных конфигураций системы и прозрачное обоснование экономической эффективности инвестиций в конкретные меры защиты, создавая запрос на более формализованные и измеримые методики. Необходимость таких методик особенно востребована в условиях, когда злоумышленники нацеливаются на цепочки поставок и сторонних провайдеров цифровых услуг, что усложняет ручной контроль и требует четких метрик для управления рисками [2].

Настоящая работа развивает эту идею, адаптируя теоретико-множественный формализм для специфики АСУ ТП, где базовыми элементами выступают физические и программные компоненты, что позволяет более наглядно учитывать архитектурные особенности промышленных систем.

Исходными данными для формирования множеств модели служат разнородные источники: идентификаторы уязвимостей из реестра CVE, описания тактик и техник злоумышленников из матрицы MITRE ATT&CK for ICS, а также результаты аудита и экспертных обследований АСУ ТП. Существенной особенностью данного этапа является необходимость формализации экспертного знания, изначально представленного в неструктурированной, семантически насыщенной форме.

В методологическом плане этот процесс сопоставим с направленным ассоциативным экспериментом, применяемым в психолингвистике для выявления структуры когнитивных представлений и устойчивых связей между понятиями [6]. Аналогично тому, как ассоциативные реакции испытуемых позволяют реконструировать семантическое поле стимула, экспертные данные в области информационной безопасности используются для выявления устойчивых связей между компонентами системы, уязвимостями и векторами атак.

Таким образом, построение множеств можно интерпретировать как результат формализованного отображения когнитивной модели эксперта в строго математическую структуру, что позволяет снизить субъективность анализа и обеспечить воспроизводимость количественной оценки атакующей поверхности.

Математическая модель

В соответствии с теоретико-множественным подходом, применяемым для формализации атакующих поверхностей сложных систем [7], модель АСУ ТП представляется в виде системы из трех базовых множеств:

$$\mathcal{S} = \langle \mathcal{C}, \mathcal{V}, \mathcal{A} \rangle \quad (1)$$

где:

- $\mathcal{C} = \{c_1, c_2, \ldots, c_n\}$ — множество компонентов системы;
- $\mathcal{V} = \{v_1, v_2, \ldots, v_m\}$ — множество уязвимостей;
- $\mathcal{A} = \{a_1, a_2, \ldots, a_k\}$ — множество векторов атаки.

Здесь и далее запись $|\mathcal{M}|$ будет обозначать мощность (количество элементов) множества $\mathcal{M}$ [8]. Например, $|\mathcal{C}|$ — это общее число компонентов системы.

Для анализа выделяются два ключевых подмножества компонентов:

1. $\mathcal{C}_{ext} \subseteq \mathcal{C}$ — компоненты, доступные из внешних или неподконтрольных сетей.
2. $\mathcal{C}_{vuln} \subseteq \mathcal{C}$ — компоненты, на которых присутствует хотя бы одна известная критическая уязвимость.

Связи между элементами моделируются бинарными отношениями:

- Отношение $\mathcal{B} \subseteq \mathcal{V} \times \mathcal{C}$: $(v, c) \in \mathcal{B}$ означает, что уязвимость v существует на компоненте c;
- Отношение $\mathcal{D} \subseteq \mathcal{A} \times \mathcal{C}$: $(a, c) \in \mathcal{D}$ означает, что вектор атаки a может быть применен для воздействия на компонент c.

В практическом применении модели данные о $\mathcal{V}$ и $\mathcal{A}$ служат основой для формирования подмножеств $\mathcal{C}_{vuln}$ (через отношение $\mathcal{B}$) и $\mathcal{C}_{ext}$ (через отношение $\mathcal{D}$), которые непосредственно участвуют в расчете.

Атакующая поверхность *AS* (Attack Surface) в контексте первоначального проникновения определяется как множество компонентов, которые одновременно являются точкой входа для атаки и содержат уязвимости:

$$AS = \mathcal{C}_{ext} \cap \mathcal{C}_{vuln} \quad (2)$$

Для получения относительной и наглядной оценки вводится коэффициент охвата атакующей поверхности *ASC* (Attack Surface Coefficient):

$$ASC = \frac{|AS|}{|C|} = \frac{|Cext \cap Cvuln|}{|C|} \quad (3)$$

Метрика $ASC \in [0,1]$ показывает, какая доля компонентов системы представляет собой непосредственную и потенциально эксплуатируемую угрозу. Снижение *ASC* является прямой количественной мерой повышения безопасности.

Наглядное представление изменений ключевых параметров модели и расчетной метрики *ASC* при внедрении мер защиты приведено в Таблице 1.

Пример применения

Рассмотрим упрощенную модель АСУ ТП с 12 компонентами ($\mathscr{C} = \{c_1,c_2,\ldots,c_{12}\}$), представляющую собой абстракцию типичного промышленного сегмента:

- $\mathscr{C}_{ext} = \{c_1,c_2,c_3,c_4,c_5\}$, где c_1 — сервер в DMZ, c_2 — межсетевой экран, c_3 — первый инженерный ПК, c_4 — второй инженерный ПК, c_5 — система резервного копирования;
- $\mathscr{C}_{vuln} = \{c_2,c_3,c_6,c_7,c_8,c_9\}$, где c_2 — межсетевой экран, c_3 — первый инженерный ПК, c_6 — ПЛК1, c_7 — ПЛК2, c_8 — сервер SCADA, c_9 — HMI;

Оставшиеся три компонента (c_{10},c_{11},c_{12}) не являются ни доступными извне, ни содержащими известные критические уязвимости, то есть представляют текущую безопасную часть системы. Обозначим множество безопасных компонентов как:

$$\mathscr{C}_{safe} = \mathscr{C} \setminus (\mathscr{C}_{ext} \cup \mathscr{C}_{vuln}) = \{c_{10},c_{11},c_{12}\} \quad (4)$$

- $AS_{before} = \mathscr{C}_{ext} \cap \mathscr{C}_{vuln} = \{c_2,c_3\}$;
- $ASC_{before} = \frac{|AS_{before}|}{|C|} = \frac{2}{12} \approx 0.17.$

Предлагаемые меры защиты и инвестиции:

1. Патч-менеджмент: установка обновлений на межсетевой экран (c_2) — исключение его из $\mathscr{C}_{vuln}$.
2. Сегментация сети [9]: выделение сети АСУ ТП в отдельный сегмент, изоляция инженерных ПК (c_3,c_4) — исключение c_3 и c_4 из $\mathscr{C}_{ext}$.
3. Обновление ПО: обновление прошивки ПЛК1 (c_6) — исключение c_6 из $\mathscr{C}_{vuln}$.

Состояние после внедрения мер:

- $\mathcal{C}_{ext}^{new} = \{c_1,c_2,c_5\}$;
- $\mathcal{C}_{vuln}^{new} = \{c_3,c_7,c_8,c_9\}$;
- $AS_{after} = \mathcal{C}_{ext}^{new} \cap \mathcal{C}_{vuln}^{new} = \varnothing$;
- $ASC_{after} = \frac{0}{12} = 0.$

Аналогично подходу, применяемому в тестировании ПО для исключения из анализа нерелевантных модулей [3], фокус модели на пересечении множеств $\mathscr{C}_{ext}$ и $\mathscr{C}_{vuln}$ позволил четко идентифицировать и количественно оценить именно те компоненты, которые представляют непосредственный риск и показать полное устранение этой зоны после внедрения мер защиты АСУ ТП.

Таблица 1

Результаты оценки изменения атакующей поверхности АСУ ТП после внедрения защитных мер

Параметр	Исходное состояние	Состояние после внедрения мер защиты
Число всех компонентов системы, $\lvert\mathscr{C}\rvert$	12	
Число компонентов, доступных извне, $\lvert\mathscr{C}_{ext}\rvert$	5	2
Число компонентов, содержащих уязвимости, $\lvert\mathscr{C}_{vuln}\rvert$	6	3
Мощность атакующей поверхности, $\lvert AS\rvert$	2	0
Коэффициент охвата атакующей поверхности, *ASC*	0.17	0
Коэффициент *ASC*, %	17%	0%

Для интеграции модели в процессы управления кибербезопасностью промышленных объектов рекомендуется использовать ее в качестве инструмента приоритизации мероприятий — первоочередному устранению подлежат уязвимости, находящиеся в пересечении $\mathscr{C}_{ext}$ и $\mathscr{C}_{vuln}$, так как они напрямую определяют размер измеряемой атакующей поверхности.

Выводы

Моделирование реализации комплекса мер показывает их эффективность: коэффициент охвата атакующей поверхности (*ASC*) снижается с 0,17 до 0. Значение *ASC* = 0 в рамках модели означает, что не осталось компонентов, одновременно доступных для атаки извне и содержащих известные критические уязвимости, что соответствует состоянию минимального риска при принятых допущениях. Важно отметить, что общее количество уязвимых компонентов уменьшилось лишь с 6 до 3, однако ключевым фактором стало именно их выведение из зоны доступа, что и фиксирует метрика *ASC*.

Трансформируя качественные экспертные суждения в формальную количественную систему, предлагаемая модель реализует подход, схожий с принципом когнитивного усилия в парадигме дополненного интеллекта [10], что можно рассматривать как аналог реконструкции когнитивных представлений из психолингвистики. Формализация связей между компонентами АСУ ТП, уязвимостями и векторами атак отражает структуру профессионального знания специалиста по информационной безопасности и переводит ее из неявной когнитивной формы в явную математическую модель. Это обеспечивает не только количественную оценку атакующей поверхности, но и методологическую основу для последующего анализа и сравнения различных архитектурных решений.

Рассчитанный коэффициент *ASC* может служить входным параметром для более детализированных динамических моделей оценки рисков. Множество компонентов *AS*, формирующее атакующую поверхность, составляет предметную область для последующего анализа с помощью моделей, оценивающих временны́е параметры эксплуатации уязвимостей или вероятность успеха конкретных атак [11]. Таким образом, предлагаемая модель выполняет функцию первичного анализа.

Литература

[1] RED Security SOC: характер кибератак меняется от массовых к целенаправленным // ООО «Ред Секьюрити». — 15 июля 2025. — URL: https://redsecurity.ru/news/red-security-soc-kharakter-kiberatak-menyaetsya-ot-massovykh-k-tselenapravlennym. — (дата обращения: 24.12.2025).

[2] ENISA Threat Landscape 2025 / European Union Agency for Cybersecurity (ENISA). — Version 1.1. — 1 October 2025; updated 19 December 2025. — Luxembourg: Publications Office of the European Union, 2025. — Cat. No. TP-01-25-025-EN-N. — ISBN 978-92-9204-721-4. — URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025. — DOI: 10.2824/2445233 (дата обращения: 26.12.2025).

[3] Козачок, А. В. Подходы к оценке поверхности атаки и фаззингу веб-браузеров / А. В. Козачок, Д. А. Николаев, Н. С. Ерохина // Вопросы кибербезопасности. – 2022. – № 3(49). – С. 32-43. – DOI 10.21681/2311-3456-2022-3-32-43. – EDN CHZAAJ.

[4] Manadhata P. K., Kaynar D. K., Wing J. M. A Formal Model for a System's Attack Surface / P. K. Manadhata, D. K. Kaynar, J. M. Wing // School of Computer Science, Carnegie Mellon University. – 2007. – Technical Report CMU-CS-07-144.

[5] Levy, M. Attack Surface Measurement: A Weird Machines Perspective / M. Levy, F. Maldonado // EICC '24: Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference. – June 5–6, 2024, Xanthi, Greece. – New York, NY, USA : ACM, 2024. – P. 90–94. – DOI 10.1145/3655693.3655705.

[6] A. Petrosian and A. Philippovich, "Assessing the Knowledge of Students in the Field of Computer Networks Using Associative Experiments," 2025 International Russian Smart Industry Conference (SmartIndustryCon), Sochi, Russian Federation, 2025, pp. 855-860, doi: 10.1109/SmartIndustryCon65166.2025.10986104.

[7] Миронова, В. Г. Модель поверхности атак для сложных систем на основе микросервисной архитектуры / В. Г. Миронова // Известия Юго-Западного государственного университета. – 2025. – Т. 29, № 1. – С. 96-106. – DOI 10.21869/2223-1560-2025-29-1-96-106. – EDN OSVHAG.

[8] Верещагин Н. К., Шень А. Лекции по математической логике и теории алгоритмов. Ч. 1: Начала теории множеств. 4-е изд., доп. М.: МЦНМО, 2012. 112 с. ISBN 978-5-4439-0012-4.

[9] Stouffer K., Pease M., Tang C. Y., Zimmerman T., Pillitteri V., Lightman S., Hahn A., Saravia S., Sherule A., Thompson M. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82r3, September 2023. DOI: 10.6028/NIST.SP.800-82r3.

[10] Kazarian, A. S. Augmented intelligence: research on the effectiveness of collaboration between humans and artificial intelligence / A. S. Kazarian // , 17 марта – 23 2025 года, 2025. – P. 24-26. – EDN VNVWBH.

[11] Богер, А. М. Математическая модель вектора DDOS-атаки на сетевую инфраструктуру АСУ ТП с использованием метода топологического преобразования стохастических сетей / А. М. Богер, А. Н. Соколов // Вопросы кибербезопасности. – 2023. – № 4(56). – С. 72-79. – DOI 10.21681/2311-3456-2023-4-72-79. – EDN DUEPTF.