УДК 004.056, 656.6

МОДЕЛИРОВАНИЕ И ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ВОДНОГО ТРАНСПОРТА

БАРАНОВ Леонид Аврамович, д-р техн. наук, зав. кафедрой; e-mail: baranov.miit@gmail.com
ИВАНОВА Нина Дмитриевна, аспирант; e-mail: ivanovand.nina@yandex.ru
МИХАЛЕВИЧ Игорь Феодосьевич, канд. техн. наук, доцент, старший научный сотрудник; e-mail: mif-orel@mail.ru

Российский университет транспорта (МИИТ), кафедра «Управление и защита информации», Москва

В статье представлен цифровой испытательный стенд анализа безопасности объектов интеллектуальных систем водного транспорта, в составе которого реализованы цифровые модели автоматизированной системы управления движением судна, подсистем глобальной навигационной спутниковой системы и электронной картографической навигационно-информационной системы, системы гибридного управления безопасностью объекта, телекоммуникационного оборудования, нарушителя информационной безопасности объекта. Рассмотрены алгоритмы оценки риска системой гибридного управления безопасностью, позволяющие выявлять актуальные для объектов угрозы, вырабатывать меры реагирования и принимать обоснованные решения о необходимости их реализации. Показаны особенности, связанные с совместным использованием количественных оценок уязвимостей компонентов компьютеризированных систем, полученных на основе базовых метрик общего назначения, и нечетких экспертных оценок состава и значений лингвистических переменных риска, полученных для конкретных условий функционирования объектов. Указано, что предложенные модели и алгоритмы гибридного управления безопасностью обеспечивают решение задач по автоматизированному поиску и выработке эффективных решений обеспечения безопасности объектов интеллектуальных систем водного транспорта на различных этапах их жизненного цикла.

Ключевые слова: агрегирование информации; безопасность; гибридное управление; информационная безопасность; компьютеризированная система; лингвистическая переменная; нечеткая оценка; риск; угроза; уязвимость; цифровой испытательный стенд; CVSS.

DOI: 10.20295/2412-9186-2025-11-01-07-15

▼ Введение

Обеспечение безопасности интеллектуальных систем водного транспорта (ИСВТ) является актуальной задачей. Интеграция, высокие темпы внедрения и уязвимости информационных, телематических и телекоммуникационных технологий [1–3], технологий искусственного интеллекта [4–6] и связи [7–9] влекут появление новых типов угроз безопасности ИСВТ [10, 11].

Автоматизированные системы корпоративного и технологического управления ИСВТ входят в состав объектов критической информационной инфраструктуры страны, что накладывает на ИСВТ высокие требования безопасности.

В целях решения задач обеспечения требуемого уровня безопасности ИСВТ в статье рассмотрены вопросы развития средств и методов управления рисками [12, 13]. Предложенные решения реализованы на цифровом испытательном стенде (ЦИС), в составе которого функционирует система гибридного управления безопасностью (ГУБ), содержащая подсистему оценки рисков [14].

1. Цифровой испытательный стенд анализа информационной безопасности объектов ИСВТ

В зависимости от решаемых задач ЦИС позволяет создавать различные конфигурации. На рис. 1 приведена конфигурация ЦИС, развернутого для решения задач управления рисками информационной безопасности объектов ИСВТ.

В состав ЦИС включены цифровые модели автоматизированной системы управления движением (АСУД) судна, подсистем глобальной навигационной спутниковой системы (ГНСС) и электронной картографической

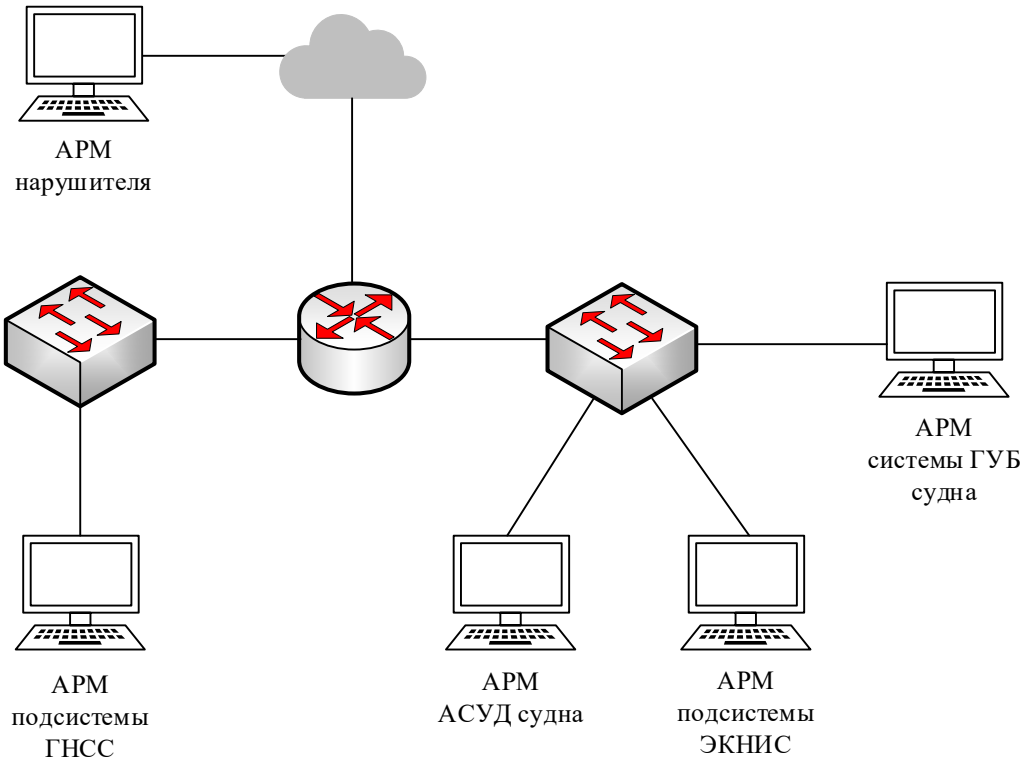


Рис. 1. Цифровой испытательный стенд анализа информационной безопасности объектов ИСВТ

навигационно-информационной системы (ЭКНИС), системы ГУБ судна, телекоммуникационного оборудования ЛВС, автоматизированного рабочего места (АРМ) нарушителя информационной безопасности объекта ИСВТ.

На АРМ ГУБ выполняется алгоритм, разработанный на основе [14, 15].

Шаг 1. Получение экспертами инвентаризационных данных об объекте ИСВТ (с учетом [16, 17]).

Инвентаризационными данными являются сведения об используемых на объекте технологиях, аппаратно-программных платформах, программном обеспечении, аппаратных средствах, средствах защиты и других компьютеризированных систем (КС), их производителях, наименованиях, модификациях, версиях, настройках и т.п.

Шаг 2. Экспертное описание объекта ИСВТ как объекта защиты (с учетом [18, 19]).

Шаг 3. Построение модели системы оценки угроз безопасности объекта ИСВТ как нечеткой иерархической системы агрегирования информации о состоянии объекта и его уязвимостях (с учетом [20, 21]).

В ISO/IEC 27005:2022 уязвимость определена как слабость актива или элемента управления, которая может быть использована для возникновения события с негативными последствиями.

Шаг 4. Непрерывный автоматический мониторинг состояния объекта ИСВТ, относимых к объекту угроз безопасности и индикация обнаружения угроз.

Шаг 5. Если угроза не обнаружена, возврат к шагу 4. При обнаружении угрозы — переход на шаг 6.

Шаг 6. Выполнение алгоритма нечеткой оценки риска, связанного с обнаруженной угрозой, вычисление значения риска.

Шаг 7. Принятие экспертом решения в отношении риска, связанного с обнаруженной угрозой.

В случае признания значения риска приемлемым обнаруженная угроза игнорируется, в противном случае эксперт инициирует переход на шаг 8.

Шаг 8. Автоматическая выработка мер реагирования.

Шаг 9. Принятие экспертом решения в отношении предлагаемых мер реагирования.

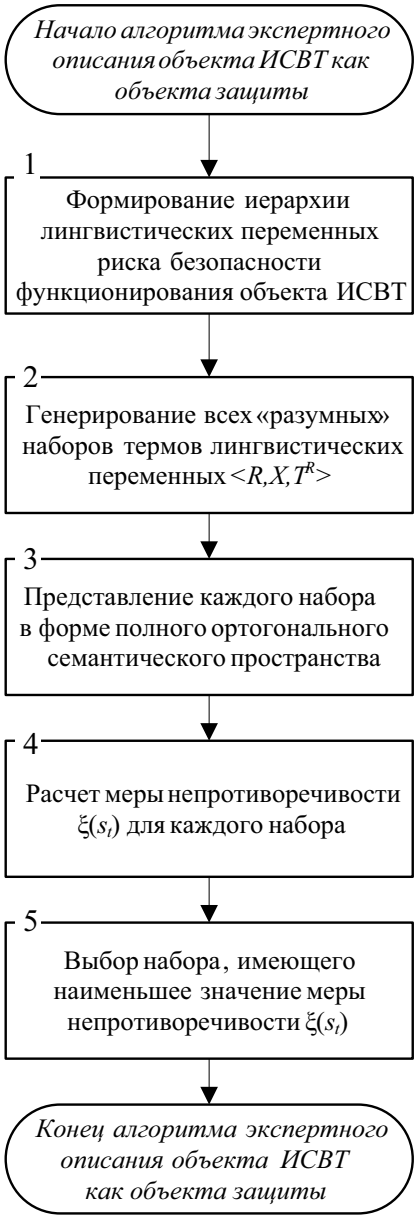


Рис. 2. Алгоритм формирования данных для ГУБ объектов

Эксперт инициирует переход алгоритма ГУБ на шаг 10 в случае признания мер неприемлемыми, на шаг 11 — при приемлемости мер.

Шаг 10. Эксперт оформляет замечания и рекомендации по предложенным мерам реагирования на обнаруженную угрозу безопасности функционирования объекта ИСВТ, возвращает алгоритм ГУБ на шаг 8.

Шаг 11. Выполняются мероприятия по реализации выработанных мер реагирования на обнаруженную угрозу безопасности функционирования объекта ИСВТ.

Шаг 12. Выполняется обновление инвентаризационных данных об объекте ИСВТ. Алгоритм ГУБ функционирования объекта ИСВТ возвращается к шагу 1.

Примечание. Во время выполнения алгоритма ГУБ процедуры, предусмотренные шагом 4, не прерываются.

Алгоритм ГУБ обеспечивает обнаружение актуальных для объекта угроз, выработку и реализацию мер реагирования.

Алгоритм, реализующий процедуры, предусмотренные на шаге 2 вышеописанного алгоритма ГУБ, приведен на рис. 2.

Эксперты определяют состав лингвистических переменных (ЛП) — R, возможные значения ЛП — X, и наборы терм-множеств ЛП — T^R. Так, в [14] ЛП «Риск» может принимать значения: VL — «Очень низкий»; L — «Низкий»; M — «Средний»; H — «Высокий», VH — «Очень высокий». В этом случае терм-множество ЛП R представляется в виде: $T^R = \left\{t_i^R\right\}, i = \overline{VL, L, M, H, VH}$.

Каждый терм образует нечеткое множество. Функция принадлежности терма к нечеткому множеству является характеристической (индикаторной) функцией четкого множества. Для рассмотренного выше случая функции принадлежности $\mu^{t_i^R}(x)$ устанавливают соответствие между элементами универсального множества X и числовыми значениями степени их принадлежности термам $\left\{t_i^R\right\}, i = \overline{VL, L, M, H, VH}$, на отрезке [0; 1]. Так, значение функции принадлежности $\mu^{t_H^R}(x)$ для некоторого элемента $x \in X$ показывает, в какой степени значение x соответствует терму H — «Высокий».

Алгоритм оценки риска системой ГУБ объекта ИСВТ приведен на рис. 3.

Рассмотрим реализацию данного алгоритма на ЦИС анализа безопасности объектов ИСВТ.

2. Реализация алгоритма оценки риска системой ГУБ объекта ИСВТ

На шаге 1 алгоритма (рис. 3) экспертами определяется состав индикаторов, на основе которого создается модель агрегирования информации о рисках безопасности объекта ИСВТ. Пример модели приведен на рис. 4.

В моделях агрегирования информации каждая вершина описывает риски, а концевые вершины (обозначены пунктирной линией) являются также индикаторами наличия рисков.

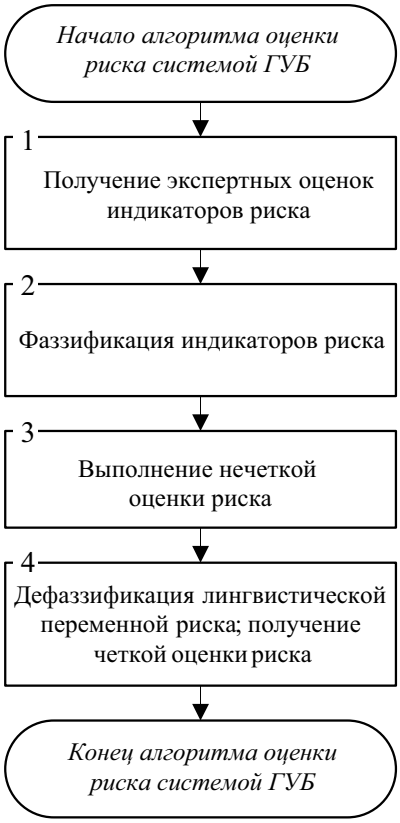


Рис. 3. Алгоритм оценки риска системой ГУБ

Каждый индикатор содержит наименование ЛП и ее оценку. С помощью индикаторов задаются исходные данные для определения совокупного (итогового) значения величины риска.

Включение в модель индикаторов связано с появлением (выявлением) уязвимостей КС объекта ИСВТ. Для этого проводится мониторинг открытых источников, инструментальный и экспертный анализ состояния КС (активов) объекта ИСВТ. Пример выявления уязвимостей КС объекта ИСВТ инструментальными средствами АРМ системы ГУБ (см. рис. 1) приведен на рис. 5.

Для четкой и нечеткой базовой оценки уязвимостей используются метрики общей системы оценки CVSS (Common Vulnerability Scoring System[1]) и BDU банков данных угроз безопасности информации и АСУ ТП ФСТЭК России[2,3]. Группа базовых метрик CVSS и BDU учитывает характеристики уязвимостей в системе триады критериев безопасности информации (конфиденциальность, целостность, доступность) и определяет уровень опасности уязвимости в диапазоне значений от 0.0 до 10.0.

Каждой известной уязвимости присваивается идентификатор CVE (Common Vulnerabilities and Exposures[4]) и дается описание, содержащее оценку риска, год обнаружения и ее порядковый номер в этом году.

[1] Common Vulnerability Scoring System: Specification Document. – URL: https://www.first.org/cvss/specification-document.

[2] Банк данных угроз безопасности информации. – URL: https://bdu.fstec.ru/vul.

[3] Банк данных угроз АСУ ТП. – URL: https://bduasutp.fstec.ru/#/vulnerabilities.

[4] CVE® Program Mission. – URL: https://www.cve.org/.

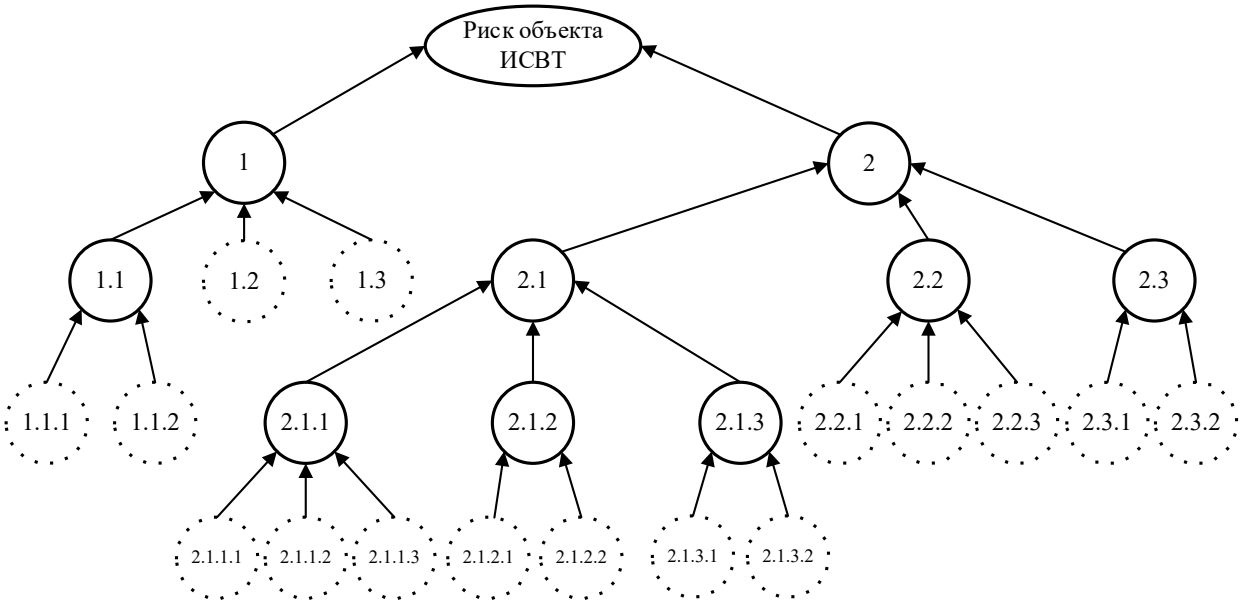


Рис. 4. Модель агрегирования информации о рисках безопасности объекта ИСВТ

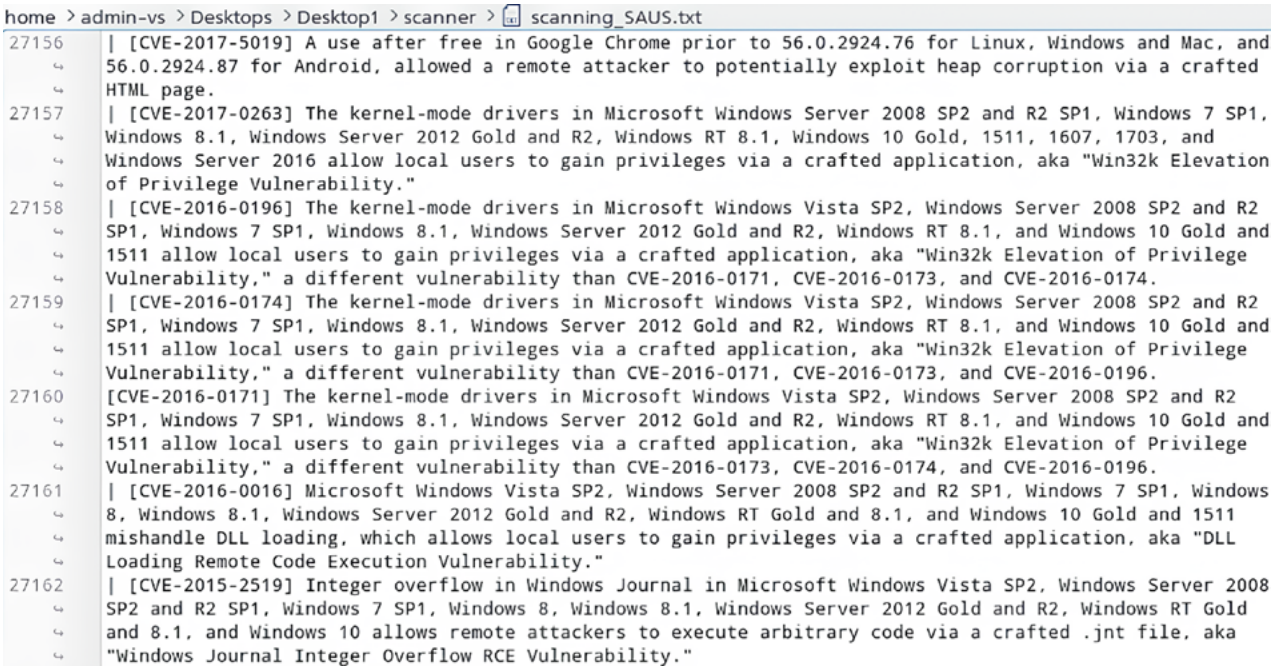


Рис. 5. Результат сканирования КС АРМ АСУД судна на наличие уязвимостей

Как видно из рис. 5, на АРМ АСУД судна были выявлены уязвимости.

Дальнейшее выполнение алгоритма оценки риска системой ГУБ объекта ИСВТ рассмотрим на примере уязвимости с идентификатором CVE-2017-5019. В Российской Федерации ей присвоен идентификатор BDU:2017-00382[5] и дано следующее описание: «Уязвимость браузера Google Chrome связана с использованием памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить доступ к защищаемой информации при помощи специально сформированной HTML страницы».

Уязвимости BDU:2017-00382 присвоен средний уровень опасности, базовая оценка уязвимости составляет 6.8 по версии CVSS 2.0[6].

Отметим, что базовые оценки CVSS не связаны с условиями функционирования конкретных объектов. В системе ГУБ они используются экспертами для присвоения индикаторам риска значений, актуальных для объекта ИСВТ. Результаты присвоения значений индикаторам (ЛП) экспертами, оценившими влияние рассматриваемой уязвимости на безопасность объекта ИСВТ, приведены в таблице.

Шаги 2–4 алгоритма (рис. 3) подробно изложены в [14], в связи с чем их описание приведем кратко.

На шаге 2 значения индикаторов риска нормализуются и проходят процедуру фаззификации, устанавливающую соответствие между четкими значениям входных переменных и нечеткими лингвистическими термами.

На шаге 3 выполняется нечеткая оценка состояний вышестоящий вершин на основе известных состояний нижестоящих вершин с применением операторов агрегирования информации.

На шаге 4 происходит дефаззификация нечетких значений и вычисление четкого (числового) значения риска в области определения от 0 до 1.

Результаты выполнения на АРМ системы ГУБ алгоритма оценки рисков безопасности объекта ИСВТ приведены на рис. 6.

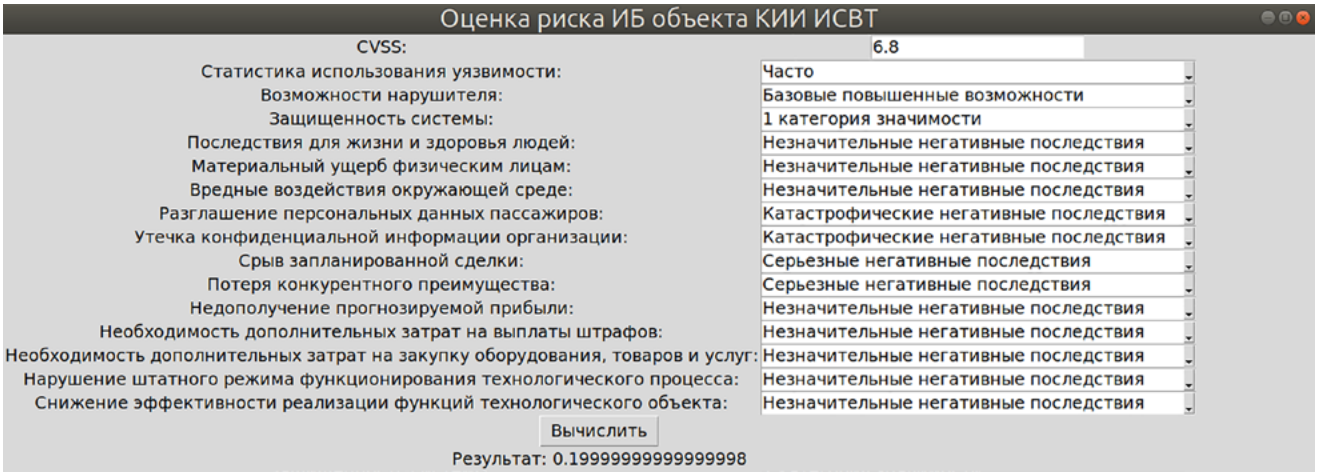
Итоговое значение величины риска определяется путем свертки четких (числовых) и нечетких (лингвистических) значений показателей частных критериев риска (табл.) с использованием рассмотренного алгоритма (рис. 3) и методики, приведенной в [14].

[5] BDU:2017-00382: Уязвимость браузера Google Chrome, позволяющая нарушителю получить доступ к защищаемой информации. – URL:https://bdu.fstec.ru/vul/2017-00382.

[6] CVE-2017-5019 Detail. – URL: https://nvd.nist.gov/vuln/detail/CVE-2017-5019.

Значения индикаторов модели агрегирования информации о рисках безопасности объекта ИСВТ в отношении уязвимости BDU:2017-00382

Характеристики индикаторов модели агрегирования информации		
Код	Наименование индикатора (ЛП)	Значение индикатора (ЛП)
1.1.1	Оценка уязвимости CVSS	6.8
1.1.2	Статистика использования уязвимости	Часто
1.2	Возможности нарушителя, достаточные для использования уязвимости	Базовые повышенные
1.3	Защищенность системы	1 категория значимости
2.1.1.1	Последствия для жизни и здоровья людей	Незначительные
2.1.1.2	Материальный ущерб физическим лицам	Незначительные
2.1.1.3	Вредные воздействия окружающей среде	Незначительные
2.1.2.1	Разглашение персональных данных пассажиров	Катастрофические
2.1.2.2	Утечка конфиденциальной информации организации	Катастрофические
2.1.3.1	Срыв запланированной сделки	Серьезные
2.1.3.2	Потеря конкурентного преимущества	Серьезные
2.2.1	Недополучение прогнозируемой прибыли	Незначительные
2.2.2	Необходимость дополнительных затрат на выплаты штрафов	Незначительные
2.2.3	Необходимость дополнительных затрат на закупку оборудования, товаров и услуг	Незначительные
2.3.1	Нарушение штатного режима функционирования технологического процесса	Незначительные
2.3.2	Снижение эффективности реализации функций технологического объекта	Незначительные




```
In [5]: risk_assesment(6.8, 'Часто', 'Базовые повышенные возможности', '1 категория значимости',
                       'Незначительные негативные последствия', 'Незначительные негативные последствия',
                       'Катастрофические негативные последствия', 'Катастрофические негативные последств
                       'Серьезные негативные последствия', 'Серьезные негативные последствия',
                       'Незначительные негативные последствия', 'Незначительные негативные последствия',
                       'Незначительные негативные последствия', 'Незначительные негативные последствия')
        0.19999999999999998

Out[5]: 0.19999999999999998
```

Рис. 6. Окна ввода исходных данных и вычисления значения величины риска безопасности объекта ИСВТ в отношении уязвимости BDU:2017-00382

Риск нарушения безопасности объекта ИСВТ для условий, описанных в таблице, составил значение 0,199.

Отметим, что итоговая оценка риска безопасности конкретного объекта защиты оказалась значительно ниже базовой оценки по CVSS. Это означает, что установленные системой базовых метрик оценки уязвимостей фактически не имеют отношения к объекту ИСВТ и оперативные меры по устранению уязвимости не требуются.

В отношении других уязвимостей КС объекта ИСВТ на ЦИС были получены оценки как близкие, так и значительно превышающие базовые оценки по CVSS. В последнем случае это означает, что на объекте необходимо оперативно разрабатывать меры по устранению уязвимости, дополнительно к мерам, предусмотренным в БДУ ФСТЭК.

Заключение

В результате выполненных работ создан цифровой испытательный стенд. Развернутая в его составе система гибридного управления позволяет выявлять актуальные для объекта ИСВТ угрозы, вырабатывать меры реагирования и принимать обоснованные решения о необходимости их реализации.

Выполненные на стенде эксперименты показали, что базовые оценки уязвимостей по CVSS не являются абсолютными. Они не учитывают особенности объектов, на которых может использоваться уязвимый компонент (система). Значение величины риска (уровня опасности уязвимости) на конкретном объекте может быть как ниже, так и выше значения базовой оценки по CVSS. Это связано с методикой базовой оценки CVSS на основе триады критериев безопасности (конфиденциальность, целостность, доступность), в то время как вклад показателя конфиденциальность, например, применительно к конкретному объекту ИСВТ, может не иметь смысла и должен быть нивелирован.

Предложенные модели и алгоритмы гибридного управления безопасностью обеспечивают решение задач по автоматизированному поиску и выработке эффективных решений обеспечения безопасности объектов ИСВТ на различных этапах их жизненного цикла. ▲

Список источников

1. Розенберг И. Н. Методы и алгоритмы создания интеллектуальных геоинформационных систем для управления транспортными процессами / И. Н. Розенберг, С. Л. Беляков, А. В. Боженюк [и др.]; под ред. И. Н. Розенберга. — М.: ВИНИТИ РАН, 2019. — 289 с.
2. Pundir A. Cyber-Physical Systems Enabled Transport Networks in Smart Cities: Challenges and Enabling Technologies of the New Mobility Era / A. Pundir, S. Singh, M. Kumar, A. Bafila, G. J. Saxena // IEEE Access. — January, 2022. — Vol. 10. — Pp. 16350–16364. — DOI: 10.1109/ACCESS.2022.3147323.
3. Kul'ba V. V. A Comprehensive Software Verification Technology for Onboard Control Systems of Spacecraft / V. V. Kul'ba, E. A. Mikrin, B. V. Pavlov, S. K. Somov // Automation and Remote Control. — 2023. — Vol. 84. — № 10. — Pp. 1047–1054. — DOI: 10.1134/S0005117923100065.
4. Kurek W. Explainable Artificial Intelligence 101: Techniques, Applications and Challenges / W. Kurek, M. Pawlicki, A. Pawlicka, R. Kozik, M. Choraś // Advanced Intelligent Computing Technology and Applications. — 2023. — Pp. 310–318. — DOI: 10.1007/978-981-99-4752-26.
5. Walter M. J. A Red Teaming Framework for Securing AI in Maritime Autonomous Systems / M. J. Walter, A. Barrett, K. Tam // Applied Artificial Intelligence. — 2024. — Vol. 38(1). — DOI: 10.1080/08839514.2024.2395750.
6. Sai S. Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E, and Other Models for Enhancing the Security Space / S. Sai, U. Yashvardhan, V. Chamola, B. Sikdar // IEEE Access. — 2024. — Vol. 12. — Pp. 53497–53516. — DOI: 10.1109/ACCESS.2024.3385107.
7. Moya Osorio D. P. Towards 6G-Enabled Internet of Vehicles: Security and Privacy / D. P. Moya Osorio, I. Ahmad, J. D. Vega Sanchez, A. Gurtov, J. Scholliers, M. Kutila, P. Porambage // IEEE Open Journal of the Communications Society. — 2022. — Vol. 3. — Pp. 82–105. — DOI: 10.1109/OJCOMS.2022.3143098.
8. Shrestha R. 6G Enabled Unmanned Aerial Vehicle Traffic Management: A Perspective / R. Shrestha, R. Bajracharya, S. Kim // IEEE Access. —2021. — Vol. 9. — Pp. 91119–91136. — DOI: 10.1109/ACCESS.2021.3092039.
9. Khan S. K. Security assessment in Vehicle-to-Everything communications with the integration of 5G and 6G networks / S. K. Khan, N. Shiwakoti, P. Stasinopoulos, M. Warren // 2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC). — Rome. Italy, 2021. — Pp. 154–158. — DOI: 10.1109/ISCSIC54682.2021.00037.
10. Михалевич И. Ф. Концептуальные проблемы транспортной безопасности водных интеллектуальных транспортных систем / И. Ф. Михалевич // Надежность. — 2024. —

№ 24(2) — С. 72–87. — DOI: 10.21683/1729-2646-2024-24-2-72-87.
11. Михалевич И. Ф. Проблемы обеспечения безопасности автономного судоходства на внутренних водных путях: монография / И. Ф. Михалевич. — М.: Горячая линия – Телеком, 2024. — 336 с.
12. Попов П. А. Комплексная безопасность АСУ ТП объектов КИИ железнодорожного транспорта / П. А. Попов, Е. Н. Розенберг, А. Г. Сабанов, И. Б. Шубинский // Надежность. —2024. — № 24(4). — С. 48–57. — DOI: 10.21683/1729-2646-2024-24-4-48-57.
13. Шубинский И. Б. Надежность, риски, безопасность систем управления на железнодорожном транспорте: монография / И. Б. Шубинский, Е. Н. Розенберг, А. В. Бочков. — М.; Вологда: Инфра – Инженерия, 2024. — 416 с.
14. Баранов Л. А. Нечеткая система оценки рисков информационной безопасности интеллектуальных систем водного транспорта / Л. А. Баранов, Н. Д. Иванова, И. Ф. Михалевич // Автоматика на транспорте. — 2024. — Т. 10. — № 1. — С. 7–17. — DOI 10.20295/2412-9186-2024-10-01-7-17.
15. Ryjov A. P. Hybrid intelligence framework for improvement of information security of critical infrastructures / A. P. Ryjov, I. F. Mikhalevich // Handbook of Research on Cyber Crime and Information Privacy. — Hershey, PA, US, 2021. — DOI: 10.4018/978-1-7998-5728-0.ch016.
16. Tam K. MaCRA: a model-based framework for maritime cyber-risk assessment / K. Tam, K. Jones // WMU J Marit Affairs. —2019. — Vol. 18. — Pp. 129–163. — DOI: 10.1007/s13437-019-00162-2.
17. Kharchenko V. AI Cybersecurity Assurance for Autonomous Transport Systems: Scenario, Model, and IMECA-Based Analysis / V. Kharchenko, O. Illiashenko, H. Fesenko, I. Babeshko // Communications in Computer and Information Science. — 2022. — Vol. 1689. — Pp. 66–79. — DOI: 10.1007/978-3-031-20215-5_6.
18. Amro A. Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth / A. Amro, V. Gkioulos // International Journal of Information Security. — 2023. — Vol. 22. — Pp. 249–288. — DOI: 10.1007/s10207-022-00638-y.
19. Kavallieratos G. Managing Cyber Security Risks of the Cyber-Enabled Ship / G. Kavallieratos, S. Katsikas // Journal of Marine Science and Engineering. — 2020. — № 8 (768). — 19 p. — DOI: 10.3390/jmse8100768.
20. Kerimkhulle S. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things / S. Kerimkhulle, Z. Dildebayeva, F. Tokhmetov, A. Amirova, J. Tussupov, U. Makhazhanova, A. Adalbek, R. Taberkhan, A. Zakirova, A. Salykbayeva // Symmetry. — 2023. Vol. 15(10), 1958. — DOI: 10.3390/sym15101958.
21. Azam M. H. Fuzzy Type-1 Triangular Membership Function Approximation Using Fuzzy C-Means / M. H. Azam, M. H. Hasan, S. Hassan, S. J Abdulkadir // 2020 International Conference on Computational Intelligence (ICCI). — Bandar Seri Iskandar, Malaysia. — 2020. — Pp. 115–120. — DOI: 10.1109/ICCI51257.2020.9247773.

TRANSPORT AUTOMATION RESEARCH, 2025, Vol. 11, No. 1, pp. 7–15
DOI: 10.20295/2412-9186-2025-11-01-7-15

Modeling and Assessment of Security Risks of Intelligent Water Transport Systems

Information about authors
Baranov L. A., Doctor in Engineering, Head of the Department.
E-mail: baranov.miit@gmail.com
Ivanova N. D., Postgraduate Student. E-mail: ivanovand.nina@yandex.ru
Mikhalevich I. F., PhD in Engineering, Associate Professor. E-mail: mif-orel@mail.ru

Russian University of Transport (MIIT), Department of Control and Protection of Information, Moscow

Abstract: A digital test bench for the analysis of IWTS object security is presented in this paper. Digital models of the automated vessel operation system, subsystems of the global navigation satellite system and the electronic chart display and information system, as well as the system of hybrid control security (HCS), telecommunications equipment, and an IWTS object information security violator have been developed. It allows promptly identifying new threats and vulnerabilities, their direction and relevance to the object developing response measures and making justified decisions on the need to implement these measures. The specific features of the joint application of vulnerability quantitative assessments of computerized system components obtained from basic general-purpose metrics, fuzzy expert assessments and linguistic risk variables obtained for a particular object functioning are presented. The proposed models and algorithms for hybrid control security provide solutions to problems of automated search and development of effective measures to ensure the ISWT security at various stages of their life cycle.

Keywords: aggregation of information; security; hybrid control; information security; computer based system; linguistic variable; fuzzy assessment; risk; threat; vulnerability; digital test bench; CVSS.

References

1. Rosenberg I. N., Belyakov S. L., Bozhenyuk A. V., Gerasimenko E. M., Glushkov A. A., Kosenko O. V., Savelyeva M. N. *Metody i algoritmy sozdaniya intellektual'nykh geoinformatsionnykh sistem dlya upravleniya transportnymi protsessami* [Methods and algorithms for creating intelligent geoinformation systems for managing transport processes], Moscow: VINITI RAS Publ., 2019, 292 p. (In Russian)
2. Pundir A., Singh S., Kumar M., Bafila A., Saxena G. J. Cyber-Physical Systems Enabled Transport Networks in Smart Cities: Challenges and Enabling Technologies of the

New Mobility Era. IEEE Access, January 2022, vol. 10, DOI: 10.1109/ACCESS.2022.3147323.

3. Kul'ba V. V., Mikrin E. A., Pavlov B. V., Somov S. K. A Comprehensive Software Verification Technology for Onboard Control Systems of Spacecraft. Automation and Remote Control, 2023, vol. 84, I. 10, pp. 1047–1054, DOI: 10.1134/S0005117923100065.
4. Kurek W., Pawlicki M., Pawlicka A., Kozik R., Choraś M. Explainable Artificial Intelligence 101: Techniques, Applications and Challenges. Advanced Intelligent Computing Technology and Applications, 2023, pp. 310–318, DOI: 10.1007/978-981-99-4752-26.
5. Walter M. J., Barrett A., Tam K. A Red Teaming Framework for Securing AI in Maritime Autonomous Systems. Applied Artificial Intelligence, 2024, vol. 38(1), DOI: 10.1080/08839514.2024.2395750.
6. Sai S., Yashvardhan U., Chamola V., Sikdar B. Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E, and Other Models for Enhancing the Security Space. IEEE Access, 2024, vol. 12, pp. 53497–53516, DOI: 10.1109/ACCESS.2024.3385107.
7. Moya Osorio D. P., Ahmad I., Vega Sanchez J. D., Gurtov A., Scholliers J., Kutila M., Porambage P. Towards 6G-Enabled Internet of Vehicles: Security and Privacy. IEEE Open Journal of the Communications Society, 2022, vol. 3, pp. 82–105, DOI: 10.1109/OJCOMS.2022.3143098.
8. Shrestha R., Bajracharya R., Kim S. 6G Enabled Unmanned Aerial Vehicle Traffic Management: A Perspective. IEEE Access, 2021, vol. 9, pp. 91119–91136, DOI: 10.1109/ACCESS.2021.3092039.
9. Khan S. K., Shiwakoti N., Stasinopoulos P., Warren M. Security assessment in Vehicle-to-Everything communications with the integration of 5G and 6G networks. 2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC), Rome, Italy, 2021, pp. 154–158, DOI: 10.1109/ISCSIC54682.2021.00037.
10. Mikhalevich I. F. Kontseptual'nye problemy transportnoy bezopasnosti vodnykh intellektual'nykh transportnykh sistem [Conceptual problems of transportation security of intelligent water transportation systems]. *Nadezhnost'* [Dependability], 2024, № 24(2), pp. 72–87, DOI: 10.21683/1729-2646-2024-24-2-72-87 (In Russian)
11. Mikhalevich I. F. *Problemy obespecheniya bezopasnosti avtonomnogo sudokhodstva na vnutrennikh vodnykh putyakh* [Problems of Ensuring the Security of Autonomous Shipping on Inland Waterways]. Moscow: Goryachaya Liniya – Telecom Publ., 2024, 336 p. (In Russian)
12. Popov P. A., Rozenberg E. N., Sabanov A. G., Shubinsky I. B. Kompleksnaya bezopasnost' ASU TP ob"ektov KII zheleznodorozhnogo transporta [Integrated Safety of ACS of Railway CII Facilities]. *Nadezhnost'* [Dependability], 2024, I. 24(4), pp. 48–57, DOI: 10.21683/1729-2646-2024-24-4-48-57. (In Russian)
13. Shubinsky I. B., Rosenberg E. N., Bochkov A. V. *Nadezhnost', riski, bezopasnost' sistem upravleniya na zheleznodorozhnom transporte* [Reliability, risks, safety of control systems in railway transport]. Moscow; Vologda: Infra-Engineering, 2024, 416 p. (In Russian)
14. Baranov L. A., Ivanova N. D., Mikhalevich I. F. Nechetkaya sistema otsenki riskov informatsionnoy bezopasnosti intellektual'nykh sistem vodnogo transporta [Fuzzy system for assessing the information security risk of intelligent water transport systems]. *Avtomatika na transporte* [Transport automation research], 2024, vol. 10, I. 1, pp. 7–17, DOI: 10.20295/2412-9186-2024-10-01-7-17. (In Russian)
15. Ryjov A. P., Mikhalevich I. F. Hybrid intelligence framework for improvement of information security of critical infrastructures. Handbook of Research on Cyber Crime and Information Privacy, Hershey, PA, US 2021, DOI: 10.4018/978-1-7998-5728-0.ch016.
16. Tam K., Jones K. MaCRA: a model-based framework for maritime cyber-risk assessment. WMU J Marit Affairs, 2019, vol. 18, pp. 129–163, DOI: 10.1007/s13437-019-00162-2.
17. Kharchenko V., Illiashenko O., Fesenko H., Babeshko I. AI Cybersecurity Assurance for Autonomous Transport Systems: Scenario, Model, and IMECA-Based Analysis. Dziech A., Mees W., Niemiec M. (eds) Multimedia Communications, Services and Security. MCSS 2022. Communications in Computer and Information Science, 2022, vol. 1689, pp. 66–79. Springer, Cham. DOI: 10.1007/978-3-031-20215-5_6.
18. Amro A., Gkioulos V. Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. International Journal of Information Security, 2023, vol. 22, pp. 249–288, DOI: 10.1007/s10207-022-00638-y.
19. Kavallieratos G., Katsikas S. Managing Cyber Security Risks of the Cyber-Enabled Ship. Journal of Marine Science and Engineering, 2020, I. 8 (768), 19 p., DOI: 10.3390/jmse8100768.
20. Kerimkhulle S., Dildebayeva Z., Tokhmetov F., Amirova A, Tussupov J., Makhazhanova U., Adalbek A., Taberkhan R., Zakirova A., Salykbayeva A. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things. Symmetry, 2023, vol. 15(10), 1958, DOI: 10.3390/sym15101958.
21. Azam M. H., Hasan M. H., Hassan S., Abdulkadir S. J. Fuzzy Type-1 Triangular Membership Function Approximation Using Fuzzy C-Means. 2020 International Conference on Computational Intelligence (ICCI), Bandar Seri Iskandar, Malaysia, 2020, pp. 115–120, DOI: 10.1109/ICCI51257.2020.9247773.