III. Проблемы обеспечения информационной безопасности

Баранов Л.А., Иванова Н.Д., Михалевич И.Ф.

Формализация риска информационной безопасности интеллектуальных системах водного транспорта как нечеткой лингвистической оценки на основе теории принятия решений

Аннотация: В статье предложена модель формализации риска информационной безопасности интеллектуальных систем водного транспорта (ИСВТ) как нечеткой лингвистической переменной, преодолевающая ограничения статистических методов в условиях неопределенности и дефицита данных. Модель синтезирует принципы теории статистического принятия решений и аппарата нечеткой логики. Для агрегации оценок применяется схема нечеткого вывода Мамдани, а процедура дефаззификации методом центроида получает байесовское обоснование как условное математическое ожидание риска. Предложенная модель обеспечивает высокую интерпретируемость и гибкость, что делает ее эффективным инструментом для построения адаптивных систем поддержки принятия решений в области защиты объектов ИСВТ.

Ключевые слова: безопасность транспорта, нечеткая логика, лингвистическая переменная, критическая информационная инфраструктура, схема Мамдани, байесовская оценка

Введение

Интеллектуальные системы водного транспорта (ИСВТ) представляют собой сложные киберфизические системы, интегрирующие технологии Интернета вещей, искусственного интеллекта и промышленной автоматики [1]. Их функционирование

напрямую влияет на безопасность, эффективность и устойчивость транспортных процессов. Вместе с тем, расширение поверхности атаки и появление новых, ранее неизвестных уязвимостей (включая уязвимости нулевого дня) требуют адаптивных и гибких подходов к управлению рисками информационной безопасности (ИБ). Статистические методы, несмотря на свою теоретическую обоснованность, оказываются неприменимыми в условиях дефицита достоверных данных и высокой неопределенности [2]. В данной работе предлагается альтернативный подход – формализация риска как нечеткой лингвистической переменной, позволяющая интегрировать экспертные знания, частичную статистику и качественные оценки в единую вычислительную модель.

Теоретическая основа: интерпретация риска в рамках теории принятия решений

В теории статистических решений [3-4] риск для состояния системы s_j определяется как условное математическое ожидание негативных последствий при фиксированном состоянии

$$r_j = \sum_{k=0}^{m} \Pi_{jk} \cdot P(\gamma_k \mid s_j), \quad (1)$$

где Π_{jk} – величина негативных последствий при принятии решения γ_k, когда истинное состояние системы – s_j;

$P(\gamma_k \mid s_j)$ – условная вероятность принятия этого решения.

В контексте ИБ ИСВТ данное определение может быть интерпретировано следующим образом:

– состояние s_j отождествляется с наличием конкретной уязвимости V;

– решение γ_k интерпретируется как внедренный комплекс мер защиты, направленный на предотвращение успешной эксплуатации уязвимости V;

– негативные последствия Π_{jk} соответствуют потенциальным негативным последствиям (социальным, финансовым, технологическим) в случае преодоления злоумышленником комплекса мер γ_k.

Таким образом, риск ИБ, обусловленный уязвимостью V и комплексом мер γ_k, формализуется как

$$R(\gamma_k \mid V) = \Pi(V) \cdot P(\gamma_k \mid V), \quad (2)$$

где $\Pi(V)$ – оценка негативных последствий при успешной эксплуатации уязвимости V;

$P(\gamma_k \mid V)$ – вероятность несрабатывания мер защиты γ_k на уязвимость V (т.е. вероятность успешной реализации угрозы).

В предлагаемой модели риска комплекс мер защиты γ_k формируется на основе двух факторов:

1. Категория значимости объекта критической информационной инфраструктуры (КИИ) согласно законодательству РФ в области КИИ [5]:

C_0: отсутствие категории значимости (базовые требования к защите);

C_1: третья категория значимости;

C_2: вторая категория значимости;

C_3: первая категория значимости (наиболее высокий требуемый уровень защиты).

2. Степень устранения уязвимости:

S_0: уязвимость не устранена.

S_1: уязвимость устранена частично (внедрены временные меры смягчения);

S_2: уязвимость устранена (применены постоянные меры).

Комбинаторное сочетание данных факторов порождает 12 уникальных значений комплекса мер

$$\Gamma = \{\gamma_{ij} \mid i \in \{0,1,2,3\}, j \in \{0,1,2\}\}, \quad (3)$$

где Γ – множество всех возможных значений комплекса мер защиты;

$\gamma_{ij} = (C_i, S_j)$ – конкретное значение комплекса мер защиты, определяемое комбинацией двух факторов (категорией значимости объекта КИИ и степенью устранения конкретной уязвимости).

Нечеткая лингвистическая модель риска

В условиях недостатка количественных данных предлагается замена классического умножения на операцию нечеткой конъюнкции, а всех переменных – на лингвистические. Лингвистическая переменная «Риск» определяется пятиэлементным терм-множеством, коррелирующим со шкалой CVSS v3.x:

T = {VL (Очень низкий), L (Низкий), M (Средний), H (Высокий), VH (Очень высокий)}

Функции принадлежности для термов строятся на основе нормализованных значений CVSS [6] (диапазон [0;1]), что обеспечивает преемственность с существующими стандартами оценки уязвимостей.

Нечеткий аналог риска выражается как

$$\tilde{R}(\gamma_k \mid V) = \tilde{\Pi}(V) \otimes \tilde{P}(\gamma_k \mid V), \quad (4)$$

где $\otimes$ – операция нечеткого умножения (min);

$\tilde{\Pi}$ и $\tilde{P}$ – нечеткие лингвистические переменные, соответствующие оценкам негативных последствий и вероятности несрабатывания защиты.

Реализация модели: схема Мамдани и байесовская интерпретация дефаззификации

Для агрегации оценок в рамках иерархической структуры характеристик рисков (представлена в работах [7-9]) применяется схема нечеткого логического вывода Мамдани, обладающая следующими преимуществами:

– высокая интерпретируемость за счет использования продукционных правил вида «ЕСЛИ... ТО...»;

– возможность агрегации количественных (CVSS) и качественных (экспертные оценки) данных;

– соответствие иерархической декомпозиции риска (от терминальных узлов к корневому).

Для родительского узла $L_{\text{род}}$, зависящего от дочерних $L_{\text{доч}_1}, L_{\text{доч}_2}, \ldots, L_{\text{доч}_n}$, справедливо

$$\boldsymbol{L}_{\text{род}} = \boldsymbol{L}_{\text{доч}_1} \otimes \boldsymbol{L}_{\text{доч}_2} \otimes \ldots \otimes \boldsymbol{L}_{\text{доч}_{n-1}} \otimes \boldsymbol{L}_{\text{доч}_n}, \quad (5)$$

где $\otimes$ — операция min.

На этапе дефаззификации применяется метод центроида для получения четкого числового значения риска x^R по шкале [0;1]

$$x^R = \frac{\sum_{i=1}^{n} C_{t_i} \cdot \mu_{t_i}}{\sum_{j=1}^{n} \mu_{t_j}}, \quad (6)$$

где C_i – центр масс (центроид) функции принадлежности μ_{t_i} терма t_i.

Данный метод допускает теоретическое обоснование в рамках байесовского подхода: если интерпретировать $P(t_i \mid R) = \frac{\mu_{t_i}}{\sum_{j=1}^{n} \mu_{t_j}}$ как апостериорную вероятность принадлежности истинного уровня риска к классу t_i, то центроид представляет собой условное математическое ожидание риска, что согласуется с принципами теории статистического принятия решений.

Заключение

Предложенная модель формализации риска ИБ как нечеткой лингвистической переменной представляет собой синтез классической теории принятия решений и современного аппарата нечеткой логики. Применение схемы Мамдани обеспечивает гибкость, интерпретируемость и возможность интеграции разнородных источников данных, что особенно актуально для специализированных систем, таких как ИСВТ. Модель открывает путь к созданию адаптивных, экспертно-ориентированных систем поддержки принятия решений в области информационной безопасности критической транспортной инфраструктуры.

Работа выполнена за счет бюджетного финансирования в рамках государственного задания от 20.03.2025 № 103-00001-25-02

Литература:

1. *Kavallieratos G., Katsikas S.* Managing Cyber Security Risks of the Cyber-Enabled Ship // Journal of Marine Science and Engineering. – 2020. – N 8(768). – 19 p. – DOI: 10.3390/jmse8100768/.

2. *Amro A.W.; Gkioulos V.* Communication and Cybersecurity Testbed for Autonomous Passenger Ship // Computer Security. ESORICS 2021 International Workshops. – 2022. – Vol. 13106. – P. 5-22. – DOI: 10.1007/978-3-030-95484-0_1.

3. *Левин Б.Р.* Теоретические основы статистической радиотехники: в 3-х кн. – М.: Советское радио, 1975. – Кн. 2. – 392 с.

4. *Ван Трис Г.* Теория обнаружения, оценок и модуляции. Т. I: Теория обнаружения, оценок и линейной модуляции / пер. с англ. под ред. В.И. Тихонова. – М.: Советское радио, 1972. – 744 с.

5. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды – утверждены Приказом ФСТЭК России от 14.03.2014. № 31 (с изменениями на 15 марта 2021 года). – URL: https://docs.cntd.ru/document/499084780 (дата обращения 15.09.2025).

6. Common Vulnerability Scoring System (CVSS) Version 4.0. FIRST (Forum of Incident Response and Security Teams). – URL: https://www.first.org/cvss/v4-0/ (дата обращения 15.09.2025).

7. *Баранов Л.А., Иванова Н.Д., Михалевич И.Ф.* Моделирование и оценка рисков безопасности интеллектуальных систем водного транспорта // Автоматика на транспорте. – 2025. – Т. 11, № 1. – С. 7-15. – DOI: 10.20295/2412-9186-2025-11-01-7-15.

8. *Баранов Л.А., Иванова Н.Д., Михалевич И.Ф.* Нечеткая система оценки рисков информационной безопасности интеллектуальных систем водного транспорта // Автоматика на транспорте. – 2024. – Т. 10, № 1. – С. 7-17. – DOI: 10.20295/2412-9186-2024-10-01-7-17.

9. *Баранов Л.А., Михалевич И.Ф., Иванова Н.Д., Соколов С.С.* Информационная безопасность системы автономного судовождения в контексте специфических для интеллектуальных транспортных систем угроз / Проблемы управления безопасностью сложных

систем: Материалы XXXI международной конференции (Москва, 13 декабря 2023 года). – М.: ИПУ РАН, 2023. – С. 249-256. – DOI: 10.25728/iccss.2023.53.91.033.

Кереселидзе Н.Г.

Модель информационной безопасности с учетом санкции

Аннотация: Представлена новая, модифицированная математическая и компьютерная модель эффективного противодействия дезинформации. В моделях учитываются «криминализация дезинформации», когда в ряде стран на законодательном уровне приняты административные и уголовные санкции за распространения дезинформации. Таким образом, представленные модели учитывают в борьбе с дезинформацией как разоблачающие дезинформацию потоки, так и возможные санкции за распространения дезинформации. Ставится задача эффективной борьбы с дезинформацией. С помощью компьютерного эксперимента построенная модель исследуется на управляемость.

Ключевые слова: математическая и компьютерная модель, динамическая система, дезинформация, информационная безопасность, санкция, управляемость

Введение

В этой работе мы представим новую, модифицированную математическую и компьютерную модель эффективного противодействия дезинформации. Ранее, в работах [1] – [4] были представлены модели, в которых противодействие дезинформации осуществлялось только лишь посредством информационных потоков. С помощью этих информационных потоков происходит разоблачение дезинформации. Считается, что дезинформационные и разоблачающие их потоки, имеют целью воздействие на умы членов общества, где происходит распространение этих потоков, превращая их в сторонников – адептов той или иной информации. В процессе распространения ложной и разоблачающей ее информации,