Ворончихин Сергей Сергеевич, адъюнкт
Военная академия защиты информации
им. генерала-армии С.М. Штеменко
Voronchikhin Sergey Sergeevich
Military Academy of Information Security
named after army general S.M. Shtemenko

ПРОТИВОРЕЧИЯ В СИСТЕМЕ ВЕСОВЫХ КОЭФФИЦИЕНТОВ МЕТОДИКИ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ: АНАЛИЗ И ПРЕДЛОЖЕНИЯ ПО СОВЕРШЕНСТВОВАНИЮ
CONTRADICTIONS IN THE WEIGHTING COEFFICIENT SYSTEM OF THE FSTEC RUSSIA INFORMATION SECURITY THREAT ASSESSMENT METHODOLOGY: ANALYSIS AND PROPOSALS FOR IMPROVEMENT

Аннотация. Систематизированы несоответствия между Методикой оценки угроз ФСТЭК России 2021 г. и Банком данных угроз, на который она ссылается: расхождение шкал уровня возможностей нарушителя, рассогласование терминологии и неявное взвешивание критериев. Предложено формализовать сопоставление шкал методом анализа иерархий.

Abstract. The paper systematizes inconsistencies between the FSTEC Russia 2021 threat assessment methodology and the Threat Data Bank it references: mismatched intruder-capability scales, inconsistent terminology, and implicit criteria weighting. A formal scale mapping via the analytic hierarchy method is proposed.

Ключевые слова: Модель угроз; ФСТЭК; весовые коэффициенты; актуальность угрозы; потенциал нарушителя.

Keywords: Threat model; FSTEC; weighting coefficients; threat relevance; intruder capability.

Определение актуальных угроз безопасности информации – обязательный этап проектирования систем защиты, требуемый приказами ФСТЭК России №17, №21, №239 и Методикой оценки угроз безопасности информации от 5 февраля 2021 г [1], заменившей Методику определения актуальных угроз безопасности персональных данных 2008 г [3] переходом от частично формализованной количественной оценки к качественной сценарной модели.

Формально методика опирается на экспертные качественные категории, но итоговое решение об актуальности угрозы получается агрегированием разнородных критериев – что по логике эквивалентно взвешиванию без публикации весов. Методика ссылается на Банк данных угроз ФСТЭК [2] как источник угроз, однако классификации двух документов не полностью согласованы. Зарубежные подходы (NIST SP 800-30, ISO/IEC 27005), для сравнения, допускают явные полуколичественные шкалы, что делает степень формализации там прозрачной. Цель статьи – систематизировать эти противоречия и предложить конструктивный способ их частичного устранения без пересмотра методики в целом.

1. Эволюция нормативной базы

Методика 2008 г [3] определяла уровень исходной защищённости пороговым правилом по семи характеристикам (высокий уровень – если не менее 70% характеристик «высокие», остальные «средние»; аналогично для среднего уровня) с присвоением коэффициента Y1 (0, 5 или 10), сочетаемого с вероятностью угрозы (Y2). Практики отмечали слабую дифференциацию систем и неоперационализированные критерии «значительности» последствий, сводившиеся к экспертному опросу [8].

Методика 2021 г [1] заменила эту шкалу сценарным подходом: актуальность определяется через объект воздействия, уровень возможностей нарушителя (H1–H4, Приложение 8, Табл. 8.1) и способ реализации угрозы. По расчёту Д.С. Милько, перебор 10

тактик, 145 техник и 222 угроз БДУ даёт 32 190 сценариев [4]. Переход 2008→2021 не устранил субъективность, а переместил её из одной формулы в тысячи отдельных суждений без формализованных весов.

2. Противоречия в системе критериев методики 2021 г.

Пп. 2.1 и 2.3 фиксируют документированное несоответствие источников (методика ↔ БДУ); п. 2.2 – авторская интерпретация логики агрегирования, а не цитата противоречащих формулировок.

2.1. Структурное расхождение шкал. Методика выделяет четыре уровня нарушителя: Н1 (базовые), Н2 (базовые повышенные), Н3 (средние), Н4 (высокие) [1]. БДУ, на который методика ссылается как на источник [1; 2], использует трёхуровневую шкалу: низкий, средний, высокий [2]. Официального правила сопоставления шкал нет; несовместимость независимо зафиксирована в [4]. Контраргумент – расхождение может быть намеренным (разная гранулярность задач); но без опубликованного правила перехода 3→4 это создаёт непроверяемую вариативность между исполнителями.

2.2. Отсутствие явных весов. Р.А. Смирнов и С.Н. Новиков, сопоставив методику ФСТЭК с ATT&CK, таксономией Ховарда – Лонгстаффа и моделью мотивации/квалификации, отмечают общую субъективность качественной оценки без количественного аппарата [5]. Вердикт об актуальности требует суждения о сочетании факторов – неявного взвешивания, нигде не документируемого.

2.3. Рассогласование терминологии. Милько фиксирует несоответствие типов последствий между методикой и описаниями угроз БДУ и рассогласование терминологии «объектов воздействия» [4].

3. Предложения по совершенствованию

Задача – не заменить методику, а наметить направления дополнения; ниже описаны направления для дальнейшей проработки, а не готовые решения.

Для 2.1 предлагается crosswalk-таблица уровней Н1–Н4 и шкалы БДУ методом анализа иерархий Т. Саати. Р.В. Жук показал применимость этого метода для потенциала нарушителя через попарное сравнение [7]; тот же принцип применим к таблице «низкий/средний/высокий → Н1–Н4»: веса фиксируются централизованно. Метод структурирует, но не устраняет экспертное суждение полностью; выигрыш – в воспроизводимости. Статус таблицы – методическая рекомендация, не изменение самой методики; официальное утверждение потребовало бы инициативы регулятора.

Для 2.2 целесообразен явный чек-лист весов агрегирования. В.И. Васильев с соавторами показывают реализуемость: веса на основе семантической близости (Doc2Vec) описаний угроз, уязвимостей и техник ATT&CK/CAPEC позволяют отфильтровывать недостижимые сценарии [6]; адаптация к паре «Методика – БДУ» способна сократить анализ из 32 190 сценариев [4] до релевантного подмножества.

Обе меры не требуют изменения текста методики. Отметим обратный риск: crosswalk-таблица может создать видимость объективности там, где текущая практика прозрачно признаёт решение экспертным – компромисс требует обсуждения при внедрении.

Заключение

Методика 2021 г. решает часть проблем 2008 г. (дифференциация по Y1), но привносит задокументированное противоречие: несовместимость своей четырёхуровневой шкалы нарушителя с трёхуровневой шкалой БДУ, на который сама ссылается, плюс отсутствие логики взвешивания и рассогласование терминологии. Предложенное сочетание AHP и семантического взвешивания не заменяет методику, а восполняет конкретный пробел, что может стать предметом апробации.

Ограничение: официального разъяснения ФСТЭК по расхождению 4 vs. 3 уровня не обнаружено; вопрос требует уточнения у регулятора или в дальнейших публикациях.

Список литературы:

1. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021).
2. Банк данных угроз безопасности информации ФСТЭК России. – [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru.
3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК России 14.02.2008).
4. Милько Д.С. Экспертная система оценки угроз безопасности информации: обоснование необходимости разработки, метод и сложности при реализации // Современные технологии. Системный анализ. Моделирование. 2021. №2 (70).
5. Смирнов Р.А., Новиков С.Н. Исследование методик оценки угроз безопасности информации // Интерэкспо ГЕО-Сибирь. 2022. Т. 6. С. 250–257.
6. Васильев В.И., Вульфин А.М., Кириллова А.Д., Кучкарова Н.В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. 2021. №3. С. 110–134.
7. Жук Р.В. Способ определения потенциала нарушителя безопасности информации и реализуемых им уязвимостей программного обеспечения // Труды учебных заведений связи. 2021. Т.7. №2. С. 95–101.
8. Проблемы действующей методики определения актуальных угроз от ФСТЭК. – [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/ic-dv/blog/453756/