УДК 51-74

А. А. Персичкин, Д. А. Хватов, А. А. Шпилевой

МЕТОДИКА ОБРАБОТКИ РЕЗУЛЬТАТОВ ЭКСПЕРТНОЙ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Поступила в редакцию 16.05.2021 г.
Рецензия от 03.06.2021 г.

Проанализированы возможности оценки угроз безопасности информации, основанные на методике ФСТЭК России в части обработки результатов работы экспертной группы. Предложен способ перевода лингвистических переменных в числовые значения на основе функции желательности Харрингтона. Использование математического базиса позволяет оптимизировать процесс обработки результатов экспертной группы, повысить точность и результативность принятия окончательных выводов.

The paper analyzes the possibilities of assessing information security threats based on the methodology of the FSTEC of Russia in terms of processing the results of the work of the expert group. A method for translating linguistic variables into numerical values based on the Harrington desirability function is proposed. The use of the mathematical basis makes it possible to optimize the process of processing the results of the expert group, to increase the accuracy and effectiveness of making final conclusions.

Ключевые слова: методика ФСТЭК, экспертная группа, оценка угроз, информационная безопасность, лингвистические переменные

Keywords: FSTEC's methodology, expert group, threat assessment, information security, linguistic variables

Как известно, с февраля 2021 г. вступила в силу методика оценки угроз безопасности информации, разработанная ФСТЭК России [1]. Методика применяется для определения угроз безопасности информации [2; 3] в государственных и муниципальных информационных системах, информационных системах персональных данных, значимых объектах критической информационной инфраструктуры Российской Федерации и т. д.

Для оценки угрозы в методике предложен экспертный метод, с этой целью разработаны рекомендации по формированию экспертной группы (приложение 2 к методике), а также по определению итоговой оценки [1].

В настоящей работе рассматривается подход к обработке результатов работы экспертной группы по оценке угроз информационной безопасности, основанный на психометрических функциях. В его рамках предлагается использовать аппарат лингвистических переменных, который, в отличие от аппарата числовых переменных, позволяет экспертно оценить достаточно сложные явления и при этом минимизировать разброс результатов такой оценки [4; 5].

При конструировании градаций шкал значений лингвистической переменной следует учитывать тот факт, что человек плохо воспринимает излишне детализированные шкалы. Анализ психофизических данных свидетельствует о том, что человек уверенно различает семь градаций на шкале некоторого признака, чему мы находим множество подтверждений: семь основных цветов, семь нот и т.д. Если же шкала содержит большее число градаций, то соседние уровни начинают сливаться и уже не могут быть с уверенностью разграничены, в связи с чем на практике преимущественно используются только пять градаций для оценки события (явления), которых, как правило, вполне достаточно [6].

С учетом данного обстоятельства в настоящей методике устанавливается и в дальнейшем используется шкала лингвистических переменных для экспертной оценки угрозы информационной безопасности, ограниченная следующими значениями: очень высокая; высокая; средняя; низкая; очень низкая.

Для формирования объективных выводов, подлежащих документальному оформлению, требуется конкретная количественная оценка значений, полученных с использованием аппарата «лингвистических переменных». Одним из наиболее удобных и часто применяемых на практике способов установления соответствия между лингвистическими и количественными переменными является использование обобщенной функции желательности Харрингтона [6]. Функция возникла в результате множества наблюдений за реальными оценками экспертов в разных областях человеческой деятельности и описывается следующим математическим выражением:

$$d = \exp[-\exp(-x)]. \qquad (1)$$

Исходя из формулы (1) процедуру перевода лингвистических переменных в числовые параметры можно пояснить графиком зависимости, представленным ниже.

Рис. Обобщенная функция желательности Харрингтона

Выбор значений на шкале желательности не является случайным [6]: например, значение d = 0,37 соответствует точке перегиба графика (1), что для лингвистической переменной совпадает с моментом перехода из удовлетворительного состояния в неудовлетворительное. Другое название указанной точки — «точка принятия решений».

Пример реализации перевода лингвистических переменных в числовые значения на основе функции желательности Харрингтона приводится в таблице 1.

Таблица 1

Перевод лингвистических переменных в числовые значения

Возможность реализации угрозы	Диапазон значений возможности реализации угрозы на шкале желательности	Весовой коэффициент возможности реализации угрозы
Очень высокая	0,80—1,00	0,94
Высокая	0,63—0,80	0,72
Средняя	0,37—0,63	0,51
Низкая	0,2—0,37	0,29
Очень низкая	0—0,2	0,02

Весовые коэффициенты возможности реализации угрозы, представленные в таблице 1, являются средними значениями функции желательности в диапазонах значений возможности реализации угрозы.

Суть процесса обработки результатов по указанной методике состоит в следующей последовательности действий:

— эксперты оценивают угрозу с помощью пяти лингвистических переменных (угроза очень высокая, высокая, средняя, низкая, очень низкая);

— каждая лингвистическая переменная сопоставляется с ее весовым коэффициентом;

— вычисляется общий итог оценки как среднее значение весовых коэффициентов;

— выносится заключение относительно актуальности угрозы (угроза считается актуальной, если итоговое значение оценки больше значения «точки принятия решений», то есть больше 0,37).

Пример результатов обработки оценок экспертной группы представлен в таблице 2.

Таблица 2

Результаты обработки оценок экспертной группы

Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Эксперт 5
Ущерб физическому лицу				
Финансовый, иной материальный ущерб физическому лицу				
Очень высокая	Средняя	Очень высокая	Высокая	Низкая
0,94	0,51	0,94	0,72	0,29

Общий итог оценки (среднее значение) — 0,68.

Вывод: угроза актуальна.

Предложенная методика позволяет оптимизировать процесс обработки результатов работы экспертной группы по оценке угроз информационной безопасности, так как от экспертов в данном случае требуется только лингвистическая оценка возможности реализации угрозы. Точность и корректность окончательных выводов также можно считать оптимальными, поскольку они основываются на конкретном математическом базисе.

Список литературы

1. *Методика* оценки угроз безопасности информации : метод. документ (утв. ФСТЭК России 5 февраля 2021). Доступ из справ.-правовой системы «Гарант».

2. *Вострецова Е.В.* Основы информационной безопасности : учеб. пособие. Екатеринбург, 2019.

3. *Плетнев П.В., Белов В.М.* Методика оценки рисков информационной безопасности // Математическое обоснование и теоретические аспекты информационной безопасности. Доклады ТУСУР. 2018. №1 (25), ч. 2. С. 83—86.

4. *Заде Л.А.* Понятие лингвистической переменной и его применение к принятию приближенных решений / пер. с англ. М., 1976.

5. *Дилигенский Н.В., Дымова Л.Г., Севастьянов П.В.* Нечеткое моделирование и многокритериальная оптимизация производственных систем в условиях неопределенности: технология, экономика, экология. М., 2004.

6. *Адлер Ю.П., Маркова Е.В., Грановский Ю.В.* Планирование эксперимента при поиске оптимальных условий. М., 1976.

Об авторах

Андрей Андреевич Персичкин — ст. преп., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: a.persichkin@kgnic.ru

Дмитрий Александрович Хватов — начальник отдела дополнительного образования, Калининградский государственный научно-исследовательский центр информационной и технической безопасности, Россия.
E-mail: hvatov-dmitrii@mail.ru

Андрей Алексеевич Шпилевой — канд. физ.-мат. наук, доц., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: AShpilevoi@kantiana.ru

The authors

Andrey A. Persichkin, Assistant Professor, Immanuel Kant Baltic Federal University, Russia.
E-mail: a.persichkin@kgnic.ru

Dmitry A. Khvatov, Head of the Department of Continuing Education, Kaliningrad State Research Center for Information and Technical Security, Russia.
E-mail: hvatov-dmitrii@mail.ru

Dr Andrey A. Shpilevoy, Associate Professor, Immanuel Kant Baltic Federal University, Russia.
E-mail: AShpilevoi@kantiana.ru