Инженерный вестник Дона, №4 (2025)
ivdon.ru/ru/magazine/archive/n4y2025/9968

Применение метода нечетких множеств в процессе проведения аудита информационной безопасности

Ю.В. Беликов

Ростовский государственный экономический университет (РИНХ)

Аннотация: Процесс обеспечения информационной безопасности неразрывно связан с оценкой соответствия предъявляемых требований. В сфере защиты информации данный процесс называется аудитом информационной безопасности. В настоящее время существует множество международных и отечественных стандартов аудита, описывающих различные процессы и методы оценки соответствия требованиям. Одним из ключевых недостатков данных стандартов является применение исключительно качественной оценки без числовых расчетов, что в свою очередь не позволяет сделать процедуру наиболее объективной. Применение нечеткой логики позволяет обеспечить процесс аудита надлежащей количественной оценкой, оперируя при этом понятными лингвистическими переменными. В статье проведён анализ существующих стандартов и представлена концептуальная модель применения метода нечетких множеств в рамках процесса аудита информационной безопасности.
Ключевые слова: информационная безопасность, информационная инфраструктура, аудит безопасности, анализ рисков, нечеткие множества, нечеткая логика.

Введение

Основой информационной безопасности является обеспечение конфиденциальности, целостности и доступности хранимых и обрабатываемых данных путём применения организационных, технических, инженерных и прочих мер, направленных на снижение рисков наступления инцидента. При организации системы информационной безопасности перед специалистами встаёт ряд вопросов:

- категорирование информации и информационных систем;
- анализ рисков и угроз безопасности;
- разработка системы безопасности;
- поддержание в актуальном состоянии механизмов информационной безопасности, а также регулярный пересмотр рисков и угроз;
- проведение периодического аудита информационной безопасности;
- и т.д.

В данном случае аудит, как форма независимой оценки отдельных компонентов или всей инфраструктуры в целом, позволяет специалисту по информационной безопасности оценить общее соответствие требованиям безопасности и определить направления, которые наиболее подвержены рискам. К основным целям аудита информационной безопасности можно отнести:

- анализ актуальных рисков компонентов информационной инфраструктуры;

- выявление менее защищённых компонентов или направлений ИТ-технологий в инфраструктуре;

- оценка соответствия требованиям по информационной безопасности;

- выработка стратегии развития информационной безопасности.

При проведении аудита информационной безопасности наиболее важным этапом является определение критериев оценки безопасности на основании утверждённых стандартов или установленных требований, которые отвечают актуальным рискам и угрозам информационной инфраструктуры организации.

Концепция метода аудита

Аудит информационной безопасности зачастую представляет собой комбинированный подход, включающий анализ рисков безопасности инфраструктуры, а также применяемых мер по защите информации. При формализации данного метода можно выделить следующие основные этапы:

1. Анализ информационных активов, то есть совокупности аппаратных и программных средств, каналов и протоколов связи, а также их критичности для функционирования организации.

2. Анализ обрабатываемой информации и её значимости.

3. Оценка уязвимостей и угроз, возможность их эксплуатации и реализации.

4. Оценка вероятного ущерба.
5. Определение рисков информационной безопасности.

К основному методу оценки при проведении аудита информационной безопасности относится экспертный метод оценки, при котором результат анализа рассчитывается на основе консолидаций мнений группы экспертов. Однако главным недостатком данного метода является отсутствие количественной оценки при проведении аудита, что в свою очередь не позволяет получить наиболее объективные численные показатели защищённости информационной инфраструктуры или вероятности наступления риска информационной безопасности.

Процедуру проведения аудита информационной безопасности возможно реализовать с применением математического аппарата нечеткой логики, который позволит детализировать результаты, а также с большей точностью рассчитать возможные величины рисков. Метод, представленный в данной работе, представляет собой применение правил нечеткой логики, основанных на входных переменных, характеризующих перечень мер по информационной безопасности, процедуры фаззификации и выходных данных, представленных в виде величины риска, связанных с невыполнением требований безопасности. Другими словами, представленная модель рассчитывает влияние риска на принятие дополнительных мер по информационной безопасности.

Разработка модели нечеткого вывода

Для определения порядка проведения аудита информационной безопасности, а также формирования алгоритма фаззификации в первую очередь необходимо определить критерии оценки и актуальные угрозы.

Под угрозой принято понимать воздействие совокупность условий и факторов, создающих потенциальную или реально существующую опасность

нарушения безопасности информации [1]. Угрозы по типу источников могу быть:

- антропогенными;
- техногенными;
- стихийными.

По «локализации» угроз относительно информационной инфраструктуры угрозы могут быть:

- внутренними (угрозы исходят от субъектов, имеющих непосредственный доступ к компонентам инфраструктуры);
- внешними (угрозы исходят от субъектов, не имеющих санкционированного доступа к компонентам инфраструктуры);
- комбинированными [2].

Процедура моделирования угроз детально описана в методическом документе «Методика оценки угроз безопасности информации», утверждённой ФСТЭК России 05.02.2021 г.

Анализируя международные и отечественные стандарты в первую очередь, стоит обратить внимание на такие, как:

- BS 7799 «Code of Practice for Information Security Management»;
- ISO/IEC 17799 «Information technology – Security techniques – Code of practice for information security management» (ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»);
- ISO/IEC 15408 «Information technology — Security techniques — Evaluation criteria for IT» (ГОСТ Р ИСО/МЭК 15408-1-2008 « Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»).

При формировании нечеткой модели стоит внимательнее обратиться к ISO/IEC 17799 (ГОСТ Р ИСО/МЭК 17799-2005), разработанному на основе британского BS 7799 и использующегося для оценки механизмов безопасности информации [3]. Рекомендации данного стандарта включают в себя 10 основных разделов, а также ряд дополнительных средств контроля информационной безопасности:

1. Политика безопасности.
2. Организационные вопросы безопасности.
3. Классификация и управление активами.
4. Вопросы безопасности, связанные с персоналом.
5. Физическая защита и защита от воздействий окружающей среды.
6. Управление передачей данных и операционной деятельностью.
7. Контроль доступа.
8. Разработка и обслуживание систем.
9. Управление непрерывностью бизнеса.
10. Соответствие требованиям [4].

На основе данных рекомендаций и в соответствии с актуальными угрозами безопасности необходимо сформировать критерии оценки, которые в последующем будут применены для разработки нечеткого вывода.

Формирование нечеткого классификатора

В основе принципа построения нечеткого классификатора лежат следующие принципы:

- помимо числовых значений применяются так называемые «лингвистические» переменные;
- взаимодействия между переменными определяются с помощью нечетких высказываний;
- отдельные операции описываются специальными нечеткими алгоритмами.

Данный подход оптимален для принятия решений в условиях неопределённости, поэтому нечеткая логика повсеместно применяется в системах помощи принятия решений, машинном обучении, а также в сфере информационной безопасности [5].

Принцип построения нечеткой модели заключается в дифференцированном подходе к ключевым категориям аудита информационной безопасности, определении весовых коэффициентов каждого параметра для дальнейшего формирования нечетких переменных, определении величины отклонения от ключевых показателей и расчёте конечных значений при оценке безопасности [6]. В первую очередь необходимо определить входные и выходные показатели, на основании которых и будет осуществляться оценка защищённости информации или соответствие защищённости ранее определённым требованиям [7].

В целях более детального аудита информационной безопасности предлагается провести вертикальную многоуровневую оценку состояния защищённости информационной инфраструктуры [8]. В таком случае аудит представляет собой не просто линейное анкетирование, а итерационную оценку установленных показателей, позволяющих с помощью аппарата нечеткой логики выявить менее защищённые направления инфраструктуры [9]. Данный метод концептуально представляет собой следующую структуру:

1. Первый раздел.

1.1. Первый уровень соответствия (зрелости) информационной безопасности.

1.2. Второй уровень соответствия (зрелости) информационной безопасности.

1.n. n-уровень соответствия (зрелости) информационной безопасности.

2. Второй раздел.

2.1. Первый уровень соответствия (зрелости) информационной безопасности.

2.2. Второй уровень соответствия (зрелости) информационной безопасности.

2.n. n-уровень соответствия (зрелости) информационной безопасности.

Входные показатели представляют собой набор установленных аудитом требований информационной безопасности, выходные – конечная оценка. При построении нечеткой логики входным и выходным параметрам назначаются соответсвенные лингвистические переменные – термы [10]. Входные показатели могут быть однозначно и неоднозначно определяемыми, например, на вопрос аудита «В организации назначено лицо, ответственное за информационную безопасность» можно ответить либо положительно, либо отрицательно, но при этом на вопрос «В организации антивирусное программное обеспечение установлено на 60% или более рабочих станций пользователей» ответ может быть неоднозначным, например, 53%, 56% или 59%. Для однозначно определяемых показателей термами являются лингвистические переменные:

- U (*Up*) – требования выполняются;
- D (*Down*) – требования не выполняются.

В свою очередь числовые значения для однозначных термов будут следующими: для терма U – $X_j = 1$; для терма D – $X_j = 0$.

Для неоднозначно определяемых показателей термами являются лингвистические переменные:

- L (*Low*) – низкий уровень соответствия;
- M (*Medium*) – средний уровень соответствия;
- H (*High*) – высокий уровень соответствия.

Числовые значения термов в данном случае будут следующими интервалам: для терма *L* – $X_i \in [0;0,3]$; для *M* – $X_i \in [0,3;0,9]$; для *H* – $X_i \in [0,9;1]$.

Выходные параметры будут обозначаться следующими лингвистическими термами:

- *A* – уровень зрелости информационной безопасности высокий;
- *B* – уровень зрелости информационной безопасности выше среднего;
- *C* – уровень зрелости информационной безопасности средний;
- *D* – уровень зрелости информационной безопасности ниже среднего;
- *E* – уровень зрелости информационной безопасности низкий.

Числовые значения для выходных терм: для терма E – $Y_i \in [0;0,1]$; для терма *D* – $Y_i \in [0,1;0,3]$; для терма *C* – $Y_i \in [0,3;0,7]$; для терма *B* – $Y_i \in [0,7;0,9]$; для терма *A* – $Y_i \in [0.9;1]$.

Формирование алгоритма нечеткого вывода

Правила нечеткого вывода принимают вид выражения *ЕСЛИ «Условие 1» И «Условие 2» и «Условие n» ТОГДА «Следствие 1»*. Для составления правил необходимо определить критерии оценки при проведении аудита [11]. В качестве основы были использованы следующие стандарты:

- BS 7799 «Code of Practice for Information Security Management»;
- ISO/IEC 17799 «Information technology – Security techniques – Code of practice for information security management» (ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»).

В результате компиляции рекомендаций вышеуказанных стандартов предлагается оценка информационной инфраструктуры по следующим направлениям (входным переменным, V):

- организационная защита информации (V_1);
- защита конфиденциальных данных (V_2);
- защита автоматизированных рабочих мест, серверной и сетевой инфраструктуры (V_3);
- мониторинг событий информационной безопасности (V_4);
- осведомленность сотрудников о мерах информационной безопасности (V_5);
- управление информационными активами (V_6);
- анализ защищённости информационной инфраструктуры (V_7);
- управление рисками и уязвимостями (V_8).

Каждый раздел включает в себя соответствующие подразделы, направленные на детальный аудит и определения уровня зрелости процессов информационной безопасности. В конечном виде правила алгоритма представляются в следующей формуле (1):

$$K_i: IF\ (V_1\ IS\ L_1^j)\ AND\ (V_2\ IS\ L_2^j)\ AND \ldots AND\ (V_n\ IS\ L_i^j)\ THEN\ Y_i = Z_i^j, \quad (1)$$

где, K_i – номер i-го правила; IF, AND, THEN – логические операторы; K_n – входные лингвистические данные, L_i^j, Z_i^j – нечеткие подмножества, Y_i – выходная переменная i-го правила.

Для наглядности применения алгоритма в таблице 1 представлен фрагмент правила для пяти критериев оценки проведения аудита информационной безопасности.

Представим указанные в таблице термы в виде числовых значений:

- организационная защита информации (V_1) – $U = 1$;
- защита конфиденциальных данных (V_2) – $D = 0{,}4$;

- защита автоматизированных рабочих мест, серверной и сетевой инфраструктуры (V_3) – B = 0,7;
- мониторинг событий информационной безопасности (V_4) – D = 0,4;
- осведомленность сотрудников о мерах информационной безопасности (V_5) – A = 1.

Таблица 1

Критерии оценки безопасности

Входные параметры					Y
V_1	V_2	V_3	V_4	V_5	
U	*D*	*B*	*D*	*A*	*C*

Рассчитав числовые значения параметров безопасности, представим их в виде таблицы 2.

Таблица № 2

Численные критерии оценки безопасности

Входные параметры					Y
V_1	V_2	V_3	V_4	V_5	
1	0,4	0,7	0,4	1	0,6

Допустим, что результат, представленный в таблице 1 и 2, является результатом аудита некоторой организации. В данном случае результирующий показатель уровня зрелости информационной безопасности равен C = 0,6 или 60%. Данная оценка соответствует уровню зрелости выше среднего согласно принятой ранее классификации. Исходя из результатов видно, что наиболее низкими показателями являются сферы защиты конфиденциальных данных и процесс мониторинга информационной безопасности. Результат работы нечеткой логики, используемой в ходе аудита информационной безопасности представлен на рисунке 1.

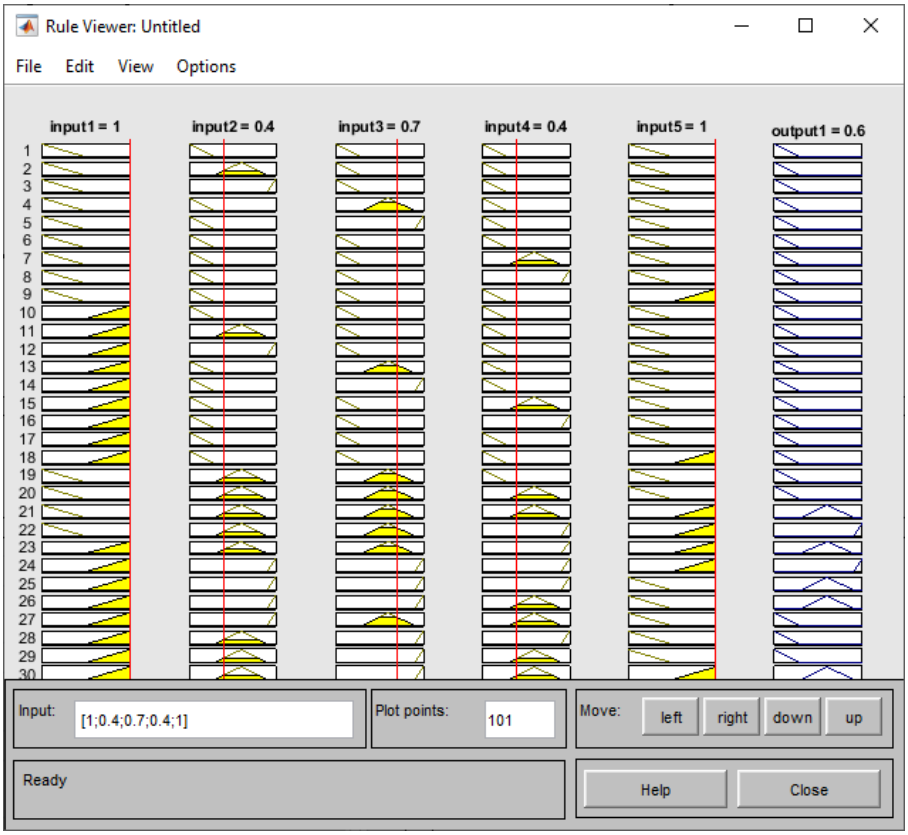

Рис. 1. – Результат работы алгоритма нечеткой логики в ходе аудита

Заключение

Анализ международных и отечественных стандартов в области аудита информационной безопасности показал их высокую детализацию и разнообразие методов оценки. Однако отсутствие числовых подходов и алгоритмов снижают эффективность данных стандартов, что негативно влияет на объективность результирующих показателей. В представленной статье описан метод проведения аудита с применением нечеткой логики, что позволяет использовать количественную оценку и обеспечить повышенную детализацию процесса проверки соответствия требованиям информационной безопасности.

Литература

1. Рыленков Д.А. Алгоритм ранжирования угроз информационной безопасности на основе метода анализа иерархий // Инженерный вестник Дона, 2024, № 8. URL: ivdon.ru/ru/magazine/archive/n8y2024/9428.

2. Менциев А.У., Чебиева Х.С. Современные угрозы безопасности в сети Интернет и контрмеры (обзор) // Инженерный вестник Дона, 2019, № 3. URL: ivdon.ru/ru/magazine/archive/N3y2019/5859

3. Mynuddin Mohammed, Hossain Iqbal Mohammad, Khan Uddin Sultan, Islam Anwarul Mohammad. Cyber Security System Using Fuzzy Logic // Conference: 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). URL: researchgate.net/publication/374137561_Cyber_Security_System_Using_Fuzzy_Logic

4. Mansour Alali, Almogren Ahmad, Hassan Mohammad Mehedi, Rassan Iehab A.L., Bhuiyan Md Zakirul Alam Improving risk assessment model of cyber security using fuzzy logic inference system // Computers & Security, 2018, № 74 URL: sciencedirect.com/science/article/abs/pii/S0167404817302006

5. Валеев С.С., Кондратьева Н.В., Гузаиров М.Б., Исмагилова А.С. Иерархическая динамическая система управления информационной безопасностью информационной системы предприятия // Инженерный вестник Дона, 2023, № 11. URL: ivdon.ru/ru/magazine/archive/n11y2023/8802

6. Анисимова Э.С. Нечёткая логика: предпосылки возникновения и основные принципы // Экономика и социум, 2015, №2-5 (15) URL: cyberleninka.ru/article/n/nechyotkaya-logika-predposylki-vozniknoveniya-i-osnovnye-printsipy

7. Любухин А.С. Методы анализа рисков информационной безопасности: нечеткая логика // International Journal of Open Information

Technologies, 2023, №2, URL: cyberleninka.ru/article/n/metody-analiza-riskov-informatsionnoy-bezopasnosti-nechetkaya-logika

8. Борисов В.В., Гончаров М.М. Модель выбора мероприятий по обеспечению информационной безопасности на основе нечетких автоматов // Программные продукты и системы, 2014, №1 (105). URL: cyberleninka.ru/article/n/model-vybora-meropriyatiy-po-obespecheniyu-informatsionnoy-bezopasnosti-na-osnove-nechetkih-avtomatov

9. Сахно В.В., Маршаков Д.В., Айдинян А.Р. Применение методов нечеткой логики для решения задачи обеспечения информационной безопасности // Молодой исследователь Дона, 2018, №4. URL: cyberleninka.ru/article/n/primenenie-metodov-nechetkoy-logiki-dlya-resheniya-zadachi-obespecheniya-informatsionnoy-bezopasnosti

10. Астахова Л.В., Цимбол В.И. Применение самообучающейся системы корреляции событий информационной безопасности на основе нечеткой логики при автоматизации систем менеджмента информационной безопасности // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника, 2016, №1. URL: cyberleninka.ru/article/n/primenenie-samoobuchayuscheysya-sistemy-korrelyatsii-sobytiy-informatsionnoy-bezopasnosti-na-osnove-nechetkoy-logiki-pri

11. Лысенко А.Ф. Нечеткая логика в моделях экспертных систем // Вопросы науки и образования, 2018, №16 (28). URL: cyberleninka.ru/article/n/nechetkaya-logika-v-modelyah-ekspertnyh-sistem

References

1. Rylenkov D.A. Inzhenernyj vestnik Dona, 2024, № 8. URL: ivdon.ru/ru/magazine/archive/n8y2024/9428.

2. Menciev A.U., Chebieva H.S. Inzhenernyj vestnik Dona, 2019, № 3. URL: ivdon.ru/ru/magazine/archive/N3y2019/5859

3. Mynuddin Mohammed, Hossain Iqbal Mohammad, Khan Uddin Sultan, Islam Anwarul Mohammad. Cyber Security System Using Fuzzy Logic // Conference: 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). URL: researchgate.net/publication/374137561_Cyber_Security_System_Using_Fuzzy_Logic

4. Mansour Alali, Almogren Ahmad, Hassan Mohammad Mehedi, Rassan Iehab A.L., Bhuiyan Md Zakirul. Computers & Security, 2018, № 74. URL: sciencedirect.com/science/article/abs/pii/S0167404817302006

5. Valeev S.S., Kondrat'eva N.V., Guzairov M.B., Ismagilova A.S. Inzhenernyj vestnik Dona, 2023, № 11. URL: ivdon.ru/ru/magazine/archive/n11y2023/8802

6. Anisimova Je.S. Jekonomika i socium, 2015, №2-5 (15). URL: cyberleninka.ru/article/n/nechyotkaya-logika-predposylki-vozniknoveniya-i-osnovnye-printsipy

7. Ljubuhin A.S. International Journal of Open Information Technologies, 2023, №2. URL: cyberleninka.ru/article/n/metody-analiza-riskov-informatsionnoy-bezopasnosti-nechetkaya-logika

8. Borisov V.V., Goncharov M.M. Programmnye produkty i sistemy, 2014, №1 (105). URL: cyberleninka.ru/article/n/model-vybora-meropriyatiy-po-obespecheniyu-informatsionnoy-bezopasnosti-na-osnove-nechetkih-avtomatov

9. Sahno V.V., Marshakov D.V., Ajdinjan A.R. Molodoj issledovatel' Dona, 2018, №4 (13). URL: cyberleninka.ru/article/n/primenenie-metodov-nechetkoy-logiki-dlya-resheniya-zadachi-obespecheniya-informatsionnoy-bezopasnosti

10. Astahova L.V., Cimbol V.I. Vestnik JuUrGU. Serija: Komp'juternye tehnologii, upravlenie, radiojelektronika, 2016, №1. URL:

cyberleninka.ru/article/n/primenenie-samoobuchayuscheysya-sistemy-korrelyatsii-sobytiy-informatsionnoy-bezopasnosti-na-osnove-nechetkoy-logiki-pri

11. Lysenko A.F. Voprosy nauki i obrazovanija, 2018, №16 (28). URL: cyberleninka.ru/article/n/nechetkaya-logika-v-modelyah-ekspertnyh-sistem

Дата поступления: 17.02.2025
Дата публикации: 15.03.2025