Володина Н.Ф., Козлов А.Д., Нога Н.Л.

Методика оценки риска информационной безопасности сложных систем

Аннотация: Рассмотрены возможности совместного использования методов нечеткой логики и регрессионного анализа при оценке риска информационной безопасности. Реализация этих методов позволяет установить зависимость риска информационной безопасности от множества параметров в условиях неопределенности и их взаимного влияния на риск, в том числе в сложных сетевых структурах и системах, и установить параметры, от которых в основном зависит риск информационной безопасности.

Ключевые слова: информационная безопасность, утечка информации, нечеткая логика, эконометрика, продукционные правила, сложные системы

Введение

В настоящее время в результате глобальной цифровизации экономики крайне сложно противодействовать инцидентам, связанным с хакерскими кибератаками, и определять прогнозные значения рисков информационной безопасности сложных систем. Особенно, следует отметить, это проявилось при переходе на удаленный режим работы в связи с пандемией ковида, а также с огромным количеством (несколько тысяч) санкций, введенных против Российской Федерации. В ограниченные временные рамки, в условиях непрекращающихся атак на российские информационные ресурсы приходится решать задачи перехода на технологический суверенитет в области программно-технического и аппаратного обеспечения.

С этими проблемами сталкиваются практически все компании самого разного уровня от больших корпораций и вплоть до малого и среднего бизнеса. За 2023 год количество утечек в мире выросло более чем на 60%, а количество скомпрометированных

персональных данных (ПДн) – более чем в два раза. На одну утечку в 2023 году в среднем приходится более 4 млн записей ПДн [1].

При этом изменения коснулись и направленности кибернарушений. По большей части теперь они направлены на дестабилизацию государства как в политическом, так и в экономическом плане. Т.е. злоумышленники пытаются нанести как можно больший ущерб различным информационным и не только, системам, включая объекты критической информационной инфраструктуры, вплоть до их полного разрушения.

В настоящий момент все больше организаций проявляют заинтересованность в современных решениях для проведения оценки рисков информационной безопасности в своих информационных системах. Такие решения, например, применяются в методиках ГРИФ и программном пакете от Microsoft [2-3]. Оценка рисков безопасности в облачных вычислениях приводится в работах [4-5]. Основой анализа и управления рисками является построение моделей, которые показывают возникающие неблагоприятные условия, при этом учитывая различные параметры, соответствующие этим условиям. Кроме того, такие модели помогают принятию решений с целью уменьшения ущерба, возникающего в результате осуществления угроз или принятия, как превентивных мер, так и мер по предотвращению ущерба от различных атак на информационные системы.

Здесь необходимо отметить, что, если можно количественно оценить параметры, от которых зависит риск, то все вышеуказанные методики дают неплохой результат. В то же время, если существует высокая неопределенность, например, при определении зависимости риска от субъективных факторов [6], то применение этих методик может привести к неверным результатам, что может способствовать нанесению непоправимого ущерба.

В работах [7-10] рассматриваются методики по оценке рисков на основе методов нечеткой логики, реализующих процедуру оценки рисков в условиях неопределенности.

В докладе предлагается к рассмотрению методика, в основе которой лежат как методы нечеткой логики, так и регрессионного анализа. Данная методика дает возможность определить совокупность параметров, значения которых наибольшим образом влияют на уровень риска для некоторого узла или компонента

сложной информационной системы подвергнуться различным угрозам через выявленные уязвимости.

Постановка задачи и алгоритм её решения

В самом общем виде значение риска можно представить в виде некоторой функции, зависящей от значений n параметров, влияющих на значение уровня риска.

Полагаем, что количественные значения всех этих параметров находятся в пределах от 0 до 1, а качественные принимают значения, например, низкий, средний и т.п.

Требуется определить объясняющие лингвистические переменные, наибольшим образом влияющие на значение выходной переменной, определяющей уровень риска, и построить модель множественной регрессии. Переменные, слабо влияющие на уровень риска, предлагается не рассматривать при дальнейшем решении задачи. При этом границы термов наших переменных задаются на основании экспертных оценок.

Для определения уровня риска предлагается использовать методы нечеткой логики, рассмотренные в работах [7, 11-12]. Необходимо отметить, что влияние рассматриваемых параметров может оказаться достаточно неопределенным из-за их взаимной корреляции и, как следствие, возможной их избыточности. При этом точность оценки зависит от качества формирования продукционных правил и правильности задания границ термов для каждой лингвистической переменной.

Поскольку коэффициенты уравнения регрессии, вычисляемые с помощью метода наименьших квадратов (МНК) несравнимы между собой, то для возможности их сравнения [13] и ранжирования параметров по степени влияния на риск, строится уравнение регрессии в стандартизованном масштабе. В результате коэффициенты выстраиваются по степени влияния на риск. По результатам ранжирования определяем избыточные параметры, т.е. параметры, слабо влияющие на риск. Затем исключаем их из уравнения.

Таким образом, примерный алгоритм, основанный на указанной выше методике, с использованием данных из нечеткой базы знаний, полученной при формировании продукционных правил, используя

метод усредненных коэффициентов влияния [14], предлагается реализовать следующим образом.

Все входные переменные оцениваются каждая по своей шкале, как на качественном уровне, так и в количественном виде в промежутке от 0 до 1. Затем в таблице продукционных правил, качественным значениям переменных ставятся в соответствие усредненные количественные значения. Получаем множество данных для возможности использования методов регрессионного анализа, т.е. строим, например, линейную модель множественной регрессии с введенными в рассмотрение объясняющими переменными P_i:

$$R = a_0 + \sum_{i=1}^{n} k_i P_i + \varepsilon \qquad (1)$$

где a_0 и $k_i, i = 1,..., n$, несравнимые коэффициенты, определяемые с помощью МНК, ε-погрешность. Затем осуществляем переход к уравнению в стандартизованном масштабе и находим стандартизованные коэффициенты. Выстраиваем их в порядке возрастания для определения переменных, от которых в большей степени зависит риск информационной безопасности. Кроме того, исследуем переменные на зависимость. Переменные, слабо влияющие на значение риска, исключаем из рассмотрения. Вычисляем значение уровня риска.

Заключение

Совместное использование методов нечеткой логики и эконометрики для оценки уровня риска информационной безопасности сложных систем позволяет вычислять прогнозные значения уровня риска в условиях неопределенности и неочевидности зависимости риска от различных факторов, включая субъективные.

Возможность определения параметров, наибольшим образом влияющих на значение риска, позволяет сосредоточить внимание компаний на противодействие угрозам на наиболее опасных направлениях и минимизировать затраты на мероприятия по защите своих информационных ресурсов.

Предложенную методику можно применять к любой сложной сетевой структуре в различных компаниях, имеющих разветвленную сеть региональных подразделений (филиалов). Причем методика позволяет не только определять риск и критические узлы, но и оценивать эффективность работы филиалов [12].

Литература:

1. Утечки информации в мире, 2022-2023 годы. Отчет. – URL: https://www.infowatch.ru/sites/default/files/analytics/files/issledovaniye-utechek-informatsii-v-mire-za-2022-2023-gody.pdf (дата обращения 10.07.2024).

2. *Разумников С.В.* Анализ возможности применения методов OCTAVE, RiskWatch, CRAMM для оценки рисков ИТ для облачных сервисов // Современные проблемы науки и образования. – 2014. – № 1. – С. 247-248.

3. *Баранова С.Ю.* Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. Серия 3. Образовательные ресурсы и технологии. – 2015. – № 1(9). – С. 73-79.

4. *Царегородцев А.В., Зеленина А.Н., Савельев В.А*. Двухэтапная процедура количественной оценки риска информационной безопасности облачных вычислений // Моделирование, оптимизация и информационные технологии. – 2017. – №4(19). – URL: http://moit.vivt.ru (дата обращения 10.07.2024).

5. *Shirisha Reddy K., Bala Raju M., Naik R.* Security measures in distributed approach of cloud computing // Advances in Intelligent Systems and Computing. – 2019. – Vol. 768. – P. 19-30.

6. *Kozlov A.D., Noga N.L.* About Some Risks Associated with Subjective Factors, and the Methodology for their Assessment // Review of Business and Economics Studies. – 2021. – No. 9(3). – P. 94-102.

7. *Kozlov A., Noga N.* Some Method of Complex Structures Information Security Risk Assessment in Conditions of Uncertainty / Proceedings of the 13th International Conference "Management of Large-Scale System Development" (MLSD). – M.: IEEE, 2020. – URL: https://ieeexplore.ieee.org/document/9247662 (дата обращения 10.07.2024).

8. *Choudhary R., Raghuvanshi A.* Risk Assessment of a System Security on Fuzzy Logic // International Journal of Scientific & Engineering Research. – 2012. – V. 3(12). – URL: https://www.ijser.org/researchpaper/Risk-Assessment-of-a-System-Security-on-Fuzzy-Logic.pdf (дата обращения 10.07.2024).

9. *Hany Sallem.* Cyber security risk assessment using multi fuzzy inference system // International Journal of Engineering and Innovative Technology (IJEIT). – 2015. – V. 4(8). – P. 13-19.

10. *Ventresca M., Aleman D.* Efficiently identifying critical nodes in large complex networks // Computational Social Networks. – 2015. – Vol. 2, No. 6. – P. 3-16.

11. *Kozlov A.D., Noga N.L.* Applying the Methods of Regression Analysis and Fuzzy Logic for Assessing the Information Security Risk of Complex Systems / Proceedings of the 14th International Conference "Management of Large-Scale System Development" (MLSD). – Moscow: IEEE, 2021. – URL: https://ieeexplore.ieee.org/document/9600245 (дата обращения 10.07.2024).

12. *Козлов А.Д., Нога Н.Л.* Методика определения наиболее критичных узлов сетевых информационных инфраструктур с целью обеспечения информационной безопасности // Информационные технологии. – 2023. – Т. 29, №6. – С. 296-306.

13. *Елисеева И.И.* и др. Эконометрика. – М.: Финансы и статистика, 2003. – 344 с.

14. *Козлов А.Д., Нога Н.Л.* Метод усредненных коэффициентов влияния для формирования нечеткой базы знаний при оценке рисков информационной безопасности / Проблемы управления безопасностью сложных систем: материалы XXX Международной научной конференции (ПУБСС'2022, Москва). – М.: ИПУ РАН, 2022. – С. 174-180.