DOI 10.37882/2223–2966.2021.12–2.14

К ВОПРОСУ О МЕТОДАХ ДЛЯ ОЦЕНКИ ПАРАМЕТРОВ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ[1]

TO THE QUESTION ABOUT METHODS FOR EVALUATION OF INFORMATION SECURITY PARAMETERS ON TECHNICAL CHANNELS OF INFORMATION OBJECTS

E. Tseligorova
A. Poluyan
V. Galushka

Summary. The paper discusses methods published in the open press that make it possible to assess the parameters of information security through the technical channels of informatization objects.

Keywords: information protection, neural networks, dedicated room, fuzzy inference algorithm.

Целигорова Елена Николаевна
К.т.н, доцент, Донской государственный технический университет (Ростов-на-Дону)
celelena@yandex.ru
Полуян Анна Юрьевна
К.т.н, доцент, Донской государственный технический университет (Ростов-на-Дону)
orfiki@rambler.ru
Галушка Василий Викторович
К.т.н, доцент, Донской государственный технический университет (Ростов-на-Дону)
galushkavv@yandex.ru

Аннотация. В работе рассматриваются, опубликованные в открытой печати методы, позволяющие оценить параметры защищенности информации по техническим каналам объектов информатизации.

Ключевые слова: защита информации, нейронные сети, выделенное помещение, алгоритм нечеткого вывода.

Проблема обеспечения защиты информации возникает почти во всех организациях для принятия соответствующих мер по противодействию дестабилизирующим факторам. Эти меры должны отвечать всем требованиям соответствующих регламентирующих документов. Так в [1] описываются термины, которые необходимо использовать как в правовой и технической документации, так и в учебной и научной литературе. Данный стандарт использует ссылки на некоторые другие стандарты, также относящиеся к защите информации:

а) ГОСТ Р ИСО/МЭК 13335–1 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий;
б) ГОСТ Р ИСО/МЭК 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
в) ГОСТ Р 50922 Защита информации. Основные термины и определения;
г) ГОСТ Р 51275 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения;
д) ГОСТ Р 51898 Аспекты безопасности. Правила включения в стандарты;
е) ГОСТ Р 52069.0 Защита информации. Система стандартов. Основные положения.

В документе рассматриваются термины, относящиеся к следующим разделам:

[1] Работа выполнена при поддержке РФФИ, проекты 19–01–00357

- термины, относящиеся к объекту защиты информации;
- термины, относящиеся к угрозам безопасности информации;
- термины, относящиеся к менеджменту информационной безопасности организации;
- термины, относящиеся к контролю и оценке информационной безопасности организации.

В [2] отмечено, в качестве частной задачи, определение наиболее незащищённых мест в выделенном помещении. В выделенном помещении источниками утечки информации могут быть [3–5]:

- акустические сигналы, распространяемые по воздуху;
- сигналы от городской телефонной станции, сотовой связи;
- виброакустические сигналы, распространяемые по инженерно-техническим системам и строительным конструкциям;
- электрические сигналы, распространяемые по проводам и т.п.

В [2] рассмотрены технические средства определения каналов утечки информации и реализующие защиту информации. Однако эти устройства целесообразно использовать после выявления наиболее уязвимых каналов утечки информации.

В статье ставится задача выявления источников утечки информации с использованием имеющихся математических методов, позволяющих оценить определенные параметры из группы неосязаемых и переведенные в численные показатели. Данные источники утечки информации следует проанализировать и ранжировать по критериям и группам риска. Причем каждый критерий должен получить определенный численный показатель оценки качественного состояния защиты от 1 до n, т.е. необходимо перевести неосязаемые параметры в численные показатели.

Для этой цели существуют следующие подходы. Рассмотрим подход предложенный в [6], в котором применен метод анализа иерархий. Метод основан на разбиении проблемы на простые составляющие с последующей обработкой лицом, принимающего решение по парным сравнениям. В результате обработки полученные суждения принимают численные решения.

Алгоритм метода имеет следующие этапы:

1. Очерчивается проблема и выясняется конечная цель.
2. Строится иерархия от намеченной цели через промежуточные критерии к нижнему уровню, являющемуся перечнем альтернатив.
3. Строятся для каждого нижнего уровня матрицы парных сравнений. Элементы любого уровня попарно сравниваются относительно их воздействия, из которых получается матрица суждений, выраженная в целых числах.
4. После проведения парных согласований определяется согласованность.
5. В цикле повторяются этапы 3,4 для всех уровней.
6. Применяя иерархический синтез, вычисляется сумма по взвешенным компонентам соответствующего уровня.
7. Определяется согласованность иерархии путам перемножения индекса согласованности с приоритетом критерия. Полученные числа суммируются. Те же самые вычисления проводятся со случайным индексом согласованности. Полученный первый результат делится на второй. Для каждой альтернативы выбирается лучший описывающий её критерий.
8. Для выяснения приоритета соответствующей альтернативы, складываются и нормализуются все её величины.
9. Выбирается альтернатива, получившая наибольшее значение.

Для решения этого подхода имеется пакет Expert Choice, разработанная фирмой Decision Support Software.

В [7] предлагается подход, использующий методы количественной оценки, основанный на объектно-ориентированных методах системного анализа. Применяемый подход реализует следующий алгоритм:

1. Проводится нечеткое экспертное оценивания элемента.
2. На полученной основе проводится нечеткого оценивания показателей совокупности с использованием эвристических методов.
3. Вычисляются веса важности показателей.
4. Вычисляются оценки в соответствии с иерархической структурой.

В работах [8, 9] предлагается использовать нейронные сети для оценки защищенности объектов информатизации (ОИ). Это связано с тем, что нейронные сети позволяют решать более широкий круг задач, чем традиционные методы, которые трудоемки и слабо отражают реальные физические процессы. В круг решаемых задач входят следующие:

1. Оценка защищенности информационной системы.
2. Выявление незащищенных участков информационной системы.
3. Моделирование осуществления несанкционированного доступа и др.

Для решения поставленных задач для анализа защищенности ОИ можно использовать пакет Neural Network Toolbox

В [10] описывается графовый метод оценки защищенности объектов. При этом вершины графа описывают защищаемые объекты, а связи — пути возможного продвижения нарушителя. Результатом вычисления является некоторый оценочный параметр, являющийся дробью, числитель которой характеризуется временем взлома системы (отражает защищенность объекта), а знаменатель является суммой трех времен:

- интервал времени от входа в систему до обнаружения;
- интервал времени от момента доступа к конкретному элементу защиты до обнаружения, т.е. о попытки несанкционированного доступа;
- интервал времени, затраченный на предотвращение несанкционированного доступа.

Исследуя полученный граф системы для определения защищенности конкретного объекта, вычисляют некоторое среднее время прохождения нарушителем от каждого входа до выхода. Если полученный оценочный параметр ≥1, то объект защищен адекватно. В случае больших значений оценочного параметра имеется возможность для упрощения системы защиты. В случае, если оценочный параметр <1, возникает необходимость увеличения оценочного параметра, т.к. степень защиты объекта недостаточна.

В работе [11] разработан метод оценки эффективности систем защиты информации, в основу которого положен алгоритм нечеткого вывода. Разработанный метод позволяет в режиме реального времени оценить эффективность средств защиты информации. Тем более, что такую оценку можно осуществить на всех этапах жизненного цикла. Кроме оценки средств защиты информации, метод позволяет оценить пути на уменьшение затрат на приобретение этих средств.

Выводы

Проведенный анализ имеющихся в открытой печати публикаций, оценивающих параметры защищенности информации по техническим каналам объектов информатизации, показывает, что проявляется тенденция к использованию алгоритмов нечеткого вывода и применению нейронной сети, что позволяет расширить круг решаемых задач, чем при использовании традиционных методов.

ЛИТЕРАТУРА

1. ГОСТ Р 53114–2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения, 2008.
2. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова.— М.: ООО «Издательство Машиностроение», 2009–508 с.
3. Ерохин С.С. Модели и методы оценки защищенности информации и информационной безопасности объекта / С.С. Ерохин, Р.В. Мещеряков, С.С. Бондарчук // Безопасность информационных технологий.— 2007.— № 4.— С. 39–46.
4. Хорев А.А. Организация защиты информации от утечки по техническим каналам // Специальная техника.— 2006.— № 3.с. 53–64.
5. Сагдеев К.М., Сагдеева Е.К. Рекомендации по оценке защищенности выделенных помещений от утечки речевой информации по акустическим и виброакустическим каналам // Международный журнал прикладных и фундаментальных исследований.— 2015.— № 8–3.— С. 466–471; URL: https://applied-research.ru/ru/article/view?id=7128 (дата обращения: 10.09.2021).
6. Саати Т., Кернс К. Аналитическое планирование. Организация систем// М.: Радио и связь, 1991. С. 224
7. Зюзин А.С. Современные тенденции оценки защиты информации// Научный журнал КубГАУ — 2015, № 107(03).—С. 1–12.
8. Бахтин А.М. Применение нейросетевого подхода для оценки защищенности объекта информатизации / А.М. Бахтин, Е.Н. Пивкин // Матер. X Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых «Наука и молодежь — 2013» [Электронный ресурс].— Режим доступа: http://edu.secna.ru/media/f/vsib_tez_2013.pdf, свободный (дата обращения: 25.06.2013)
9. Пивкин Е.Н., Белов В.М., Белкин С.А. К вопросу об анализе защищенности объектов информатизации с использованием нейронных сетей/ Доклады ТУСУРа — 2014, № 2 (32).— С. 157–161.
10. Полянский Д.А. Оценка защищенности: учеб. пособие / Д.А. Полянский; Владим. гос. ун-т.— Владимир: Изд-во Владим. гос. ун-та, 2005.— 80 с. (Комплексная защита объектов информатизации. Кн. 10 / под. ред. М.Ю. Монахова).
11. Миняев А.А. Методика оценки эффективности системы защиты территориально распределенных информационных систем. Автореферат диссертации на соискание ученой степени кандидата технических наук. 2021, 19с.

© Целигорова Елена Николаевна (celelena@yandex.ru),
Полуян Анна Юрьевна (orfiki@rambler.ru), Галушка Василий Викторович (galushkavv@yandex.ru).
Журнал «Современная наука: актуальные проблемы теории и практики»