ВВЕДЕНИЕ

Актуальность темы исследования. На сегодняшний день рабочее место практически любого человека является автоматизированным. Автоматизированное рабочее место (АРМ) - программно-технический комплекс автоматизированной системы (АС) предназначенный для автоматизации деятельности определенного вида [8]. В связи с широкой распространенностью АРМ во всех сферах деятельности человека, существует множество угроз безопасности информации, обрабатываемой на таких рабочих местах. Для разработки эффективной системы защиты информации и подбора необходимых средств защиты информации (СЗИ) необходимо проводить риск-анализ защищаемого объекта.

В ходе риск-анализа происходит выявление существующих уязвимостей, актуальных угроз и расчет величины возможного ущерба при реализации конкретной угрозы. В завершение риск-анализа получается полная картина риска для исследуемого объекта, также составляются рекомендации по управлению риском. Основываясь на результатах риск-анализа, строится эффективная система защиты информации [11, 12]. В данной работе риск-анализ проводится на основе методов экспертных оценок и теории нечетких множеств. Так как в данной работе риск-анализ проводится на основе экспертных оценок, была выбрана именно теория нечетких множеств, так как задачи, стоящие перед человеком в различных областях знаний являются по своей природе слишком сложными и многогранными для того, чтобы использовать для их решения только точные, хорошо определенные модели и алгоритмы.

Многие понятия вследствие человеческого мышления, приближенного характера умозаключений и лингвистического их описания являются нечеткими по своей природе и требуют для своего описания соответствующего аппарата, в частности, аппарата теории нечетких множеств [16].

В отличие от традиционной математики, требующей на каждом шаге вычислений точных и однозначных описаний закономерностей, нечеткая логика предлагает совершенно иной уровень мышления, благодаря которому творческий процесс

моделирования происходит на наивысшем уровне абстракции, при котором постулируется лишь минимальный набор закономерностей.

Нечеткие числа, получаемые в результате «не вполне точных измерений», во многом аналогичны распределениям теории вероятностей, но свободны от присущих последним недостатков: малое количество пригодных к анализу функций распределения, необходимость их принудительной нормализации, соблюдение требований аддитивности, трудность обоснования адекватности математической абстракции для описания поведения фактических величин. В пределе, при возрастании точности, нечеткая логика приходит к стандартной, Булевой. По сравнению с вероятностным методом, нечеткий метод позволяет резко сократить объем производимых вычислений, что, в свою очередь, приводит к увеличению быстродействия нечетких систем [15, 20].

ЗАКЛЮЧЕНИЕ

Преимущество модели оценки рисков информационной безопасности на основе нечетких множеств состоит в применении аппарата нечеткой логики, т.к. процесс защиты информации не всегда можно описать однозначно, особенно это касается поведения персонала. Метод оценки рисков информационной безопасности на основе теории нечетких множеств даже при недостаточном объеме входных данных позволяет построить адекватную модель воздействия угроз на объект, который подлежит защите. При этом возможно рассматривать несколько ветвлений реализации угрозы или множества угроз на объект. Таким образом, можно оценить наиболее вероятные угрозы на объект защиты и, на базе полученной информации, создать или модернизировать систему защиты информации.

Преимуществом экспертных оценок является индивидуальный подход к каждой организации, так как привлекая к оценке экспертов из организации, можно адаптировать модель под специфику конкретной компании.

В данной работе рассматриваются два новых метода ранжирования применительно к анализу рисков информационной безопасности.

Методом на основе взвешенного коэффициента корреляции ранжируется множество существующих для объекта угроз, для того, чтобы выявить направленность наиболее опасных угроз: конфиденциальность, целостность или доступность информации. Затем по результатам ранжирования выбирается адекватная для объекта защиты СЗИ.

После применения СЗИ ранжирование производится повторно для проверки работоспособности системы защиты. Повторное ранжирование производится двумя разными методами для сравнения результатов, так как данные методы применяются в области информационной безопасности в первые.

Примечательно, что результаты расчетов по обоим методам получились схожими с небольшими отклонениями в области рисков среднего значения. Схожесть результатов доказывает работоспособность методов.