Анализ существующих методик оценки защищенности показал, что большинство методик не рассчитано на использование в процессе анализа без наличия такой дополнительной информации, как важность актива для бизнеса, его реальная стоимость и ущерб в результате компрометации, которые могут быть получены только с разрешения владельца актива. Также было замечено, что многие методики с точки зрения затрат на введение мер защиты, предпочитают устранять исключительно внешние уязвимости, чтобы, например, уменьшить процент покрытия атаки. Таким образом, они не учитывают потенциальные векторы атак, которые могут быть направлены от элементов сетевой инфраструктуры, не являющихся точками входа. При этом сохраняются все цепочки уязвимостей, расположенные в одном переходе от точек входа.

Появление новых сервисов и открытых портов на узлах сети может привести к возникновению новых точек входа, через которые злоумышленники смогут воспользоваться уже существующими цепочками уязвимостей, что подтверждает актуальность данной работы.

В качестве основной структуры для анализа был выбран граф атак, так как он позволяет максимально точно передать состояние исследуемой системы, взаимосвязи между узлами и сервисами.

В данной работе предлагается новый подход к решению проблемы выбора защитных мер и оценки защищенности сетевой инфраструктуры. Данный подход использует процесс оценки рисков на основе графов атак, что позволяет учесть топологию сети, найденные уязвимости и взаимодействие между узлами в процессе оценки. Таким образом, обеспечивается оптимальная последовательность действий, необходимых для уменьшения уровня риска всей исследуемой системы, а не только нисходящего риска от точек входа, что рассматривается в некоторых работах.

Для решения проблем наличия циклов и значительного времени построения графов атак используется ряд оптимизаций, не накладывающий никаких ограничений на исследуемый граф атак.

Реализованная система может успешно решать задачу оценки защищенности и поиска защитных мер и применяться как дополнение к системам автоматизированного тестирования на проникновение с последующей выработкой рекомендаций.