Введение

Сетевая инфраструктура практически любой организации представляет собой сложную структуру, состоящую из множества различных сервисов, направленных на поддержание функционирования компании. Данная структура очень динамична: добавляются новые сервисы, меняются конфигурации существующих, создаются новые связи между сервисами. В процессе роста системы задачи обеспечения её информационной безопасности и защиты критически важных объектов становятся нетривиальными.

Причиной нарушения информационной безопасности чаще всего становятся:

1. уязвимости в операционных системах;
2. уязвимости приложений, осуществляющих сетевое взаимодействие с пользователем или друг с другом;
3. неправильные конфигурации программного обеспечения;
4. ошибки контроля доступа.

Используя имеющиеся уязвимости и недостатки системы, внешние и внутренние нарушители проводят сетевые атаки, приводящие к компрометации различных узлов и реализации угроз информационной безопасности сети.

Для выявления недостатков компонентов системы, а также поиска уязвимостей и потенциальных векторов атак на информационные ресурсы, проводится анализ защищенности сети. Одним из наиболее эффективных методов анализа является тестирование на проникновение, в ходе которого осуществляется моделирование атак реальных злоумышленников. Такой подход позволяет в полной мере провести оценку защищенности сетевой инфраструктуры, оценить существующие и предложить новые способы защиты.

При этом все возрастающая сложность компьютерных систем: большое количество узлов в сети, множество различных версий сервисов и потенциальных уязвимостей и наличие средств защиты обуславливает необходимость в разработке автоматизированных систем анализа защищенности сети. Такие системы должны не только дать оценку защищенности сети, определить наиболее критические уязвимости и недостатки сети, но и предложить оптимальные пути их исправления.

В результате проведения анализа защищенности посредством тестирования на проникновение проводится описание основных обнаруженных уязвимостей, а также способов их устранения. Однако в крупных компаниях, как и в большинстве рассмотренных методик, существует практика устранения только тех уязвимостей, эксплуатация которых приводит к проникновению во внутреннюю сеть организации или компрометации наиболее критически важных узлов системы. Из-за сложности сетевой инфраструктуры устранение всех прочих уязвимостей затягивается на неопределенный срок, что создаёт опасную ситуацию, в которой злоумышленник, обнаружив новую точку входа, может воспользоваться существующими цепочками уязвимостей для компрометации сети.

Необходимо не только защитить сеть от проникновения извне, но и обеспечить должный уровень защищенности внутренней сети. Так, по данным Positive Technologies за 2019 год [1] при проведении внешнего тестирования на проникновение экспертам удалось преодолеть сетевой периметр 92% организаций, тогда как от лица внутреннего нарушителя был получен полный контроль над инфраструктурой во всех исследуемых системах.

Для оценки уровня защищенности системы в данной работе предлагается использовать подход, основанный на анализе графа потенциальных атак с составлением метрик защищенности узлов и сети в целом для определения наиболее эффективных мер защиты. Рассмотренный подход позволяет оценить уровень риска системы при проникновении нарушителя на любой из узлов сетевой инфраструктуры, включенных в граф атак, и, следовательно, снизить риск компрометации системы с любого из узлов графа.

Процессы оценки защищенности сетевой инфраструктуры, анализа рисков и выбора защитных мер рассмотрены в большом количестве государственных стандартов (ГОСТ Р ИСО/МЭК 31010-2011, ГОСТ Р ИСО/МЭК 27005-2010, ГОСТ Р ИСО/МЭК 27004-2011 и т.д.). Более того, в 2019 году вышел ряд постановлений Центрального Банка (684-П, 683-П, 382-П), обязывающих различные организации, осуществляющие работу с финансами, проводить тестирование на проникновение. Проблема оценки защищенности и выбора защитных мер рассматривается в работах как отечественных, так и зарубежных авторов: Жижелев А.В. [15], Kanoun W. [16], Дойникова Е.В. [13][19], Lippmann R.P. [23], Минаев В.А. [24], Астахов А.М. [11], Fabbri J. [9], Брюховецкая [3].

Проведенный анализ работ по данной проблематике показал, что для оценки рисков и выбора защитных мер используется огромное число различных показателей защищенности и методик их вычисления, в том числе на основе графов атак. Однако большинство методик требует взаимодействия с оператором, например, для заполнения опросных листов, включающих данных о стоимости активов и контрмер, что требует расширенных знаний о тестируемой системе. Наличие подобных ограничений не позволяет использовать данные методики в автоматизированных системах.

Более того, большинство работ, использующих для оценки защищенности графы атак, накладывают ограничения на граф, ввиду сложности проведения вычислений на графе: отсутствие циклов, отсутствие нескольких путей к одному узлу графа.

Поэтому в данной работе предполагается разработать подход, основанный на анализе графа атак, использующий различные оптимизации для сокращения времени вычисления показателей защищенности. Данный подход может быть использован в любой автоматизированной системе оценки защищенности.

Цель данной работы – разработать автоматизированную систему оценки защищенности сетевой инфраструктуры и выбора защитных мер на основе графов атак.

Для достижения поставленной цели определены следующие задачи:

1. Определить основные способы идентификации узлов сети и их уязвимостей в процессе тестирования на проникновение;
2. Проанализировать существующие методики оценки защищенности сетевой инфраструктуры и выбора защитных мер и применимость графов атак в задачах оценки защищенности;
3. Разработать методики оценки защищенности сетевой инфраструктуры и выбора защитных мер на основе анализа графа атак;
4. Реализовать автоматизированную систему анализа защищенности сетевой инфраструктуры на основе анализа графа атак;

В работе используются методы теории графов, теории множеств и оптимизации, а также методы экспертного анализа.

Научная новизна выпускной квалификационной работы заключается в следующем:

1. Разработанные методики используют в качестве показателей защищенности только ту информацию, которая может быть получена тестировщиком в процессе проведения тестирования на проникновение.
2. Методика оценки защищенности учитывает риски компрометации сети с любого узла графа атак, а не только с точки входа.
3. Разработанная методика выбора защитных мер использует ряд уникальных оптимизаций, направленных на ускорение вычислений на графе атак.
4. Разработанная архитектура и программная реализация системы оценки защищенности и выбора контрмер может быть интегрирована в любую другую систему оценки, как дополнительный модуль.

Разработанные в процессе выполнения данной работы методики способствуют выявлению наиболее критических уязвимостей сетевой инфраструктуры и позволяют максимально снизить уровень риска системы в результате проникновения злоумышленника в сеть организации. Устранение даже части уязвимостей, рекомендованных разработанной методикой, позволит значительно снизить ущерб в случае компрометации системы. Данные методики могут применяться в процессе разработки рекомендаций по устранению уязвимостей в результате проведенного тестирования на проникновение.