Мишин Д.В, кандидат технических наук
Мошков Н.Е.

МЕТОДИКА ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ТЕЛЕКОМУНИКАЦИОННЫХ СИСТЕМ

Аннотация: На сегодняшний день актуальной является задача повышения защищенности информационных ресурсов телекоммуникационной сети предприятия. Для решения данной задачи в научно-исследовательской работе предлагается выявить различные показатели защищенности, а также разработать методику повышения уровня защищенности за счет их изменения. Целью работы является разработка методики повышения защищенности информационных ресурсов телекоммуникационной сети предприятия. На данном этапе работы были поставлены следующие задачи: анализ существующих методик оценки защищенности, сравнительный анализ и выбор наиболее приемлемой методики оценки защищенности для достижения поставленной цели.

При анализе предметной области рассмотрено понятие телекоммуникационной сети (определение, ТС на предприятии, типы ТС), понятие защищенности, понятие информационных ресурсов (определение, ИР на предприятии, защищенность ИР), актуализация проблемы защищенности ТС.

При обзоре релевантных работ по теме исследования, были рассмотрены следующие: Simulating Concurrent Intrusions for Testing Intrusion Detection Systems о тестировании системы обнаружения вторжений, Game Strategies in Network Security о разработке метода анализа защищенности компьютерных сетей на основе теории игр (игра между администратором и атакующим), Attack Trees о представлении атак в виде деревьев., «Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности»(1) , методика, основанная на модели безопасности с полным перекрытием Клементса-Хоффмана, разработана на кафедре ИЗИ (2)

Анализ перечисленных выше работ позволил выявить 2 наиболее применимые для достижения цели исследования методики.

(1) Методика базируется на автоматической генерации общего графа атак и использовании качественных метрик защищенности. Граф отражает возможные распределенные сценарии атак с учетом конфигурации сети, реализуемой политики безопасности, а также местоположения, целей, уровня знаний и стратегий нарушителя. Предложенные метрики защищенности позволяют оценивать защищенность компьютерной сети с различной степенью детализации и с учетом различных аспектов. Метрики защищенности базируются на метриках из методологии CVSS.

Достоинства данной методики: наличие графа атак, благодаря которому видны трассы атаки, оценка производится на основе метрик CVSS, что определяет гибкость данной методики.

Недостаток: трудоемкость просчета всех возможных действий нарушителя.

(2) Общий показатель защищенности складывается из различных вероятностных показателей, таких как: вероятность появления угрозы от одного из нарушителей s_{kn}, вероятность прохождения угрозы через одну из уязвимостей q_{kn}, вероятность не прохождения угрозы через все защитные механизмы r_{kn}, расчет итогового показателя защищенности: $P_{kn} = 1 - s_{kn} * q_{kn} * (1-r_{kn})$

Как результат методики: матрица защищенности (угрозы по i, ТС по j) для одного информационного ресурса. Данный показатель имеет значение от 0 до 1.

Достоинство: данная методика проста в использовании, нет сложных расчетов.
Недостатки: методика не предусматривает построение трасс атаки.

Выбор методики для экспериментальных расчетов

В ходе анализа сети возможно получение следующих входных данных: топология сети, значимость узлов сети, возможные трассы атаки, матрица прав доступа.

Выходные данные: Количественная или качественная оценка защищенности

Наиболее существенным критерием выбора методики были: учет трасс атак, соответствие требованиям к входным и выходным данным, простота использования методики, возможность автоматизации.

Как было сказано выше, в методике (2) не предусмотрено построение трасс атаки, но при этом она проста в использовании, методика использует вероятностные входные данные, что слабо применимо для задачи.

Методика (1) сложнее в использовании, однако она позволяет видеть возможные трассы атак, учитывает критичность узла, критичность атакующего действия и другие показатели. На выходе получаем качественную оценку защищенности.

Резюмируя вышесказанное, можно сделать вывод, что методика: «Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности» наиболее применима к задачам исследования, что обосновывает ее выбор для дальнейших этапов НИР.

Итоги текущего этапа работы.

В рамках анализа предметной области, приведены основные положения и определения, так как телекоммуникационная сеть, защищенность, информационный ресурс, актуализация проблемы защищенности ТС.

Приведен анализ релевантных работ и методик оценки защищенности.
В результате анализа была выбрана методика для выполнения дальнейших задач НИР в соответствии с критериями.

На следующем этапе предполагается провести апробацию выбранной методики для расчета показателей защищенности ТС исследуемого предприятия.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Мировые и отечественные информационные ресурсы. Электронный ресурс]. URL: http://www.realib.ru/links/0

2. ГОСТ Р 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения» Электронный ресурс]. URL: http://faculty.ifmo.ru/csd/files/52448-2005.pdf

3. *Chung M., Mukherjee B., Olsson R. A., Puketza N.* Simulating Concurrent Intrusions for Testing Intrusion Detection Systems

4. *Lye K., Wing J.* Game Strategies in Network Security

5. *Schneier B.* Attack Trees // Dr. Dobb's Journal

6. *И. В. Котенко, М. В. Степашкин, В. С. Богданов*, Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности.

7. *М.М. Монахова, И.Ю. Богомазова, М.Ю. Монахов* Автоматизированная система определения уровня целостности информационных ресурсов. // Проблемы эффективности и безопасности функционирования сложных технических и информационных систем: Сборник трудов XXXII Всероссийской научно-технической конференции / Серпухов, 2013. - т.5. – С.168-171. ISBN 978-5-91954-074-8