Оригинал-макет тезиса доклада

1. Индекс УДК: 004.056.53
2. Название тезиса доклада: изучение систем обнаружения вторжений
3. Автор: Нечухрин Н.С., место учёбы – Университет ИТМО, г. Санкт-Петербург
4. Научный руководитель: Поляков В.И., Университет ИТМО, г. Санкт-Петербург
5. В настоящее время вычислительные системы и сети стали неотъемлемой частью нашей жизни. Почти все компьютеры, в том числе корпоративные и государственные, имеют выход в сеть. В связи с этим встает серьезный вопрос об обеспечении безопасности информации. Данная процедура – есть система, которая состоит из ряда элементов, одним из которых является система обнаружения вторжений (СОВ).

Цель работы: изучить типы системы обнаружения вторжений (СОВ), определить их достоинства и недостатки.

Базовые положения исследования: в ходе научно исследовательской работы рассматривается классификация СОВ:

1. Типы СОВ: локальная, которая использует ресурсы компьютера (мощности, системные журналы) для выявления вторжения, и сетевая, сенсоры которой расположенные в важных точках сети и которая перехватывает в ней трафик для анализа содержимого.
2. Виды: Сетевая СОВ (NIDS), основанная на протоколе СОВ (PIDS), основанная на прикладных протоколах СОВ (APIDS), узловая СОВ (HIDS), гибридная СОВ.
3. Способы реализации СОВ: активные, которые не только способствуют обнаружению вторжения, но и пытаются ему противостоять, и пассивные, которые проводят логирование и оповещение об опасности.

Рассматриваются реализации СОВ на примере ПО с открытым исходным кодом.

Промежуточные результаты: изучены типы СОВ, особенности их работы, достоинства и недостатки.

Основные результаты: результатом выполнения научно-исследовательской работы было изучение классификации, особенностей реализации и выявление достоинств и недостатков существующих систем обнаружения вторжений для оценки их применения при разработке методик выявления вторжений в компьютерных сетях.

Автор: Нечухрин Н.С.

Научный руководитель: Поляков В.И.

Руководитель образовательной программы: Маркина Т.А.