МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)

Классификация методов обнаружения сетевых атак

Студент: Криков Антон Владимирович

Группа: ИУ7-73Б

Руководитель: Клорикьян Петрос Вазгенович

Цель и задачи

Цель – классифицировать известные методы обнаружения сетевых атак.

Задачи:

- описать термины предметной области и обозначить проблему;
- рассмотреть возможные способы защиты от сетевых атак;
- классифицировать методы обнаружения сетевых атак;
- сформулировать критерии сравнения методов обнаружения сетевых атак;
- сравнить описанные методы по предложенным критериям.

Термины предметной области

Сетевая атака — это действие или последовательность связанных между собой действий, использующих уязвимости информационной системы и приводящих к нарушению политики безопасности.

Под **политикой безопасности** подразумевается набор критериев и правил, описывающих информационные процессы в системе, выполнение которых обеспечивает необходимое условие безопасности системы.

Пассивная атака — это атака, при которой у злоумышленника нет доступа к модификации передаваемых сообщений и возможности добавления собственных сообщений в информационный канал между отправителем и получателем.

Активная атака — это атака, при которой у злоумышленника имеется возможность модифицировать передаваемые сообщения и добавлять собственные.

Пороговый анализ

Используемый набор сетевых параметров:

- IP-адреса источника и приемника;
- тип и порт пакета;
- длина пакета;
- время фиксации пакета.

Анализ энтропии

Используемый набор сетевых параметров:

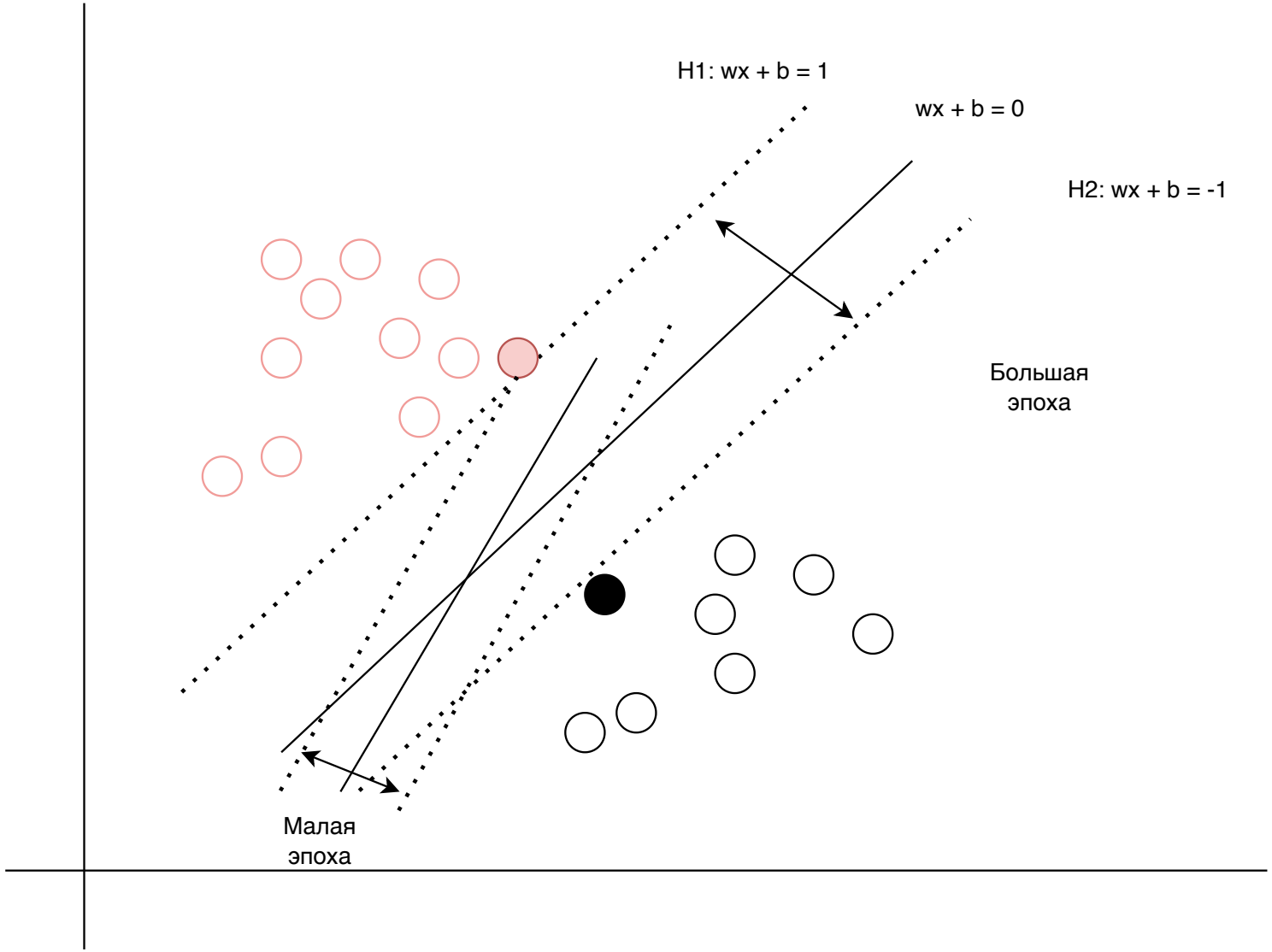
- IP-адреса источника и приемника;
- сетевой порт источника;
- сетевой порт приемника.

Байесовский метод

Используемый набор сетевых параметров:

- IP-адреса источника и приемника;
- сетевой порт источника;
- сетевой порт приемника;
- состояние соединения;
- временная метка.

SVM-метод



Анализ существующих решений

	Адаптивность	Устойчивость	Уровень наблюдения
Анализ энтропии	+	-	HIDS, NIDS, AIDS, Hybrid
Пороговый анализ	+	-	HIDS, NIDS, AIDS, Hybrid
Байесовский метод	-	+	NIDS, HIDS
SVM-метод	+	-	NIDS, HIDS

Выводы

- описаны термины предметной области и обозначена проблема;
- проведен обзор существующих методов обнаружения сетевых атак;
- классифицированы методы обнаружения сетевых атак;
- сформулированы критерии сравнения методов;
- проведено сравнение рассмотренных методов по выделенным критериям.