Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н. Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н. Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления (ИУ)»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии (ИУ7)»

РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

К НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

НА ТЕМУ:

«Классификация методов обнаружения сетевых атак»

Студент ИУ7-73Б (Группа) _____ (Подпись, дата) А. В. Криков (И. О. Фамилия)

Руководитель _____ (Подпись, дата) П. В. Клорикьян (И. О. Фамилия)

2022 г.

РЕФЕРАТ

В работе характеризованы современные методы обнаружения сетевых атак. Рассмотрена актуальность темы и проведен анализ предметной области. Также проведен обзор существующих методов обнаружения сетевых атак и приведена их классификация.

Ключевые слова: сетевая атака, DDOS, DOS, MITM, IP, TCP, Анализ Энтропии, распределенная модель.

Рассчетно-пояснительная записка к научно-исследовательской работе содержит 23 страницы, 10 иллюстраций, 1 таблиц, 14 источников, 1 приложение.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Стремительный рост в сфере информационных технологий вызывает ряд проблем, связанных с защитой сетевых ресурсов в глобальной сети. Так, согласно исследованиям с начала 2022 года количество сетевых атак увеличилось на 15% по сравнению с 2021 годом. При этом увеличилась доля массовых атак: теперь их количество составляет 33% от общего числа. Также в исследовании отмечается, что вырос интерес к интернет-ресурсам: доля атак на них увеличилась до 22% от общего количества по сравнению с 13%, наблюдаемыми в 2021 году [1].

На основании данного исследования можно сделать вывод, что количество сетевых атак лишь растет, а следовательно растет и потребность в защите от них.

Цель работы — классифицировать известные методы обнаружения сетевых атак.

Чтобы достигнуть поставленной цели, требуется решить следующие задачи:

— описать термины предметной области и обозначить проблему;

— рассмотреть возможные способы защиты от сетевых атак;

— классифицировать методы обнаружения сетевых атак;

— сформулировать критерии сравнения методов защиты от сетевых атак;

— сравнить описанные методы по предложенным критериям.

1 Анализ предметной области

Сетевая атака [2] — 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.

1.1 Модели сетевых атак

Классическая модель атаки выстраивается по принципу «один к одному», как показано на рисунке 1.1, или «один ко многим», как показано на рисунке 1.2. Для защиты от таких атак разработчики внедряют сенсоры системы защиты, передающие информацию на центральный аппарат управления. Благодаря этому обеспечивается масштабируемость системы и простота удаленного управления. Однако такое решение не распространяется на модель с распределенными атаками [3].

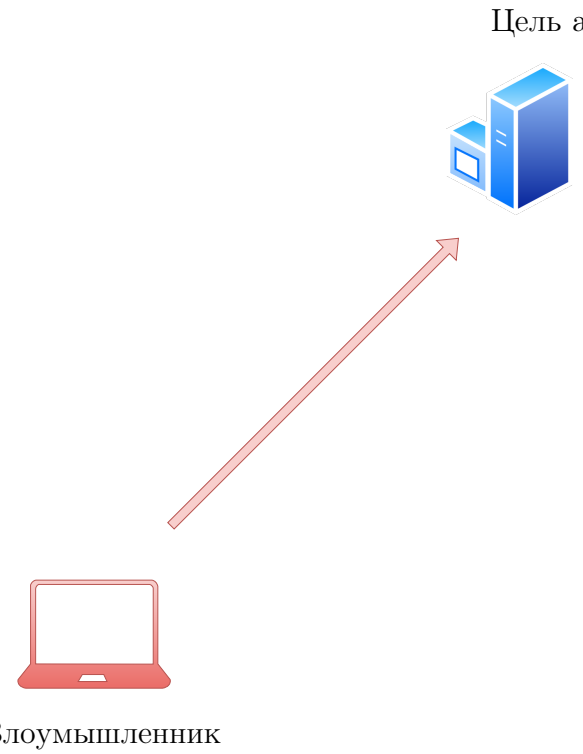


Рисунок 1.1 – Сетевая атака «один к одному»

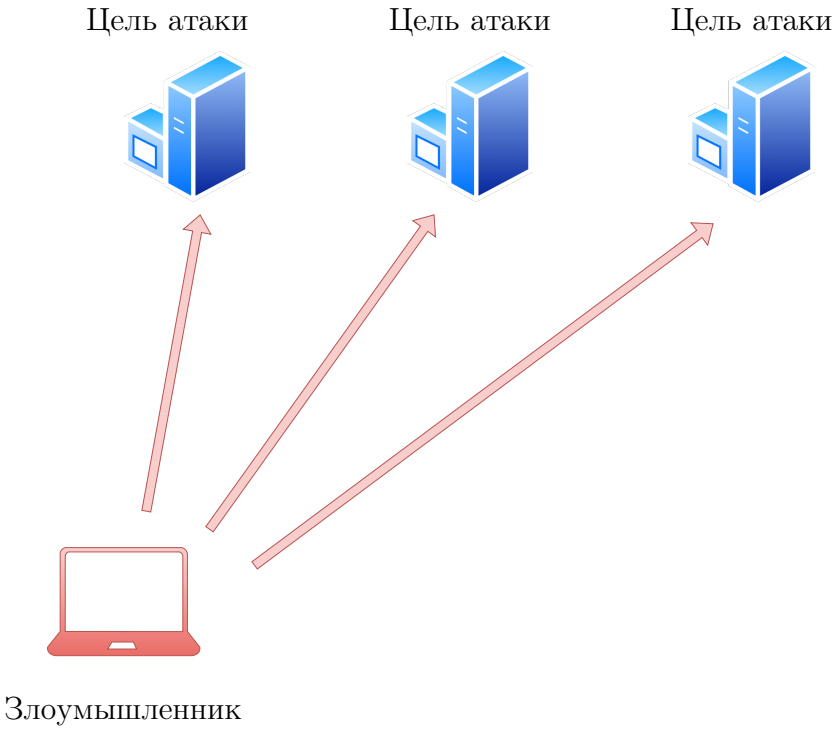


Рисунок 1.2 – Сетевая атака «один ко многим»

В **распределенной модели** используется принцип «многие к одному», как показано на рисунке 1.3, или «многие ко многим», как показано на рисунке 1.4. Данная атака осуществляется в два этапа. На первом этапе ищутся узлы сети, которые впоследствии задействуются для реализации распределенной атаки. Второй этап представляет собой посылку большого количества запросов на атакуемый сетевой узел. Отправка запросов осуществляется с помощью скомпрометированных систем-посредников, на которых установлены специальные агенты, реализующие распределенную атаку. Агенты делятся на два типа: «мастер» и «демон». Злоумышленник управляет небольшим числом «мастеров», а те управляют «демонами». Стоит отметить, что блокирование одного или нескольких «мастеров» или «демонов» не приводит к завершению атаки [3].

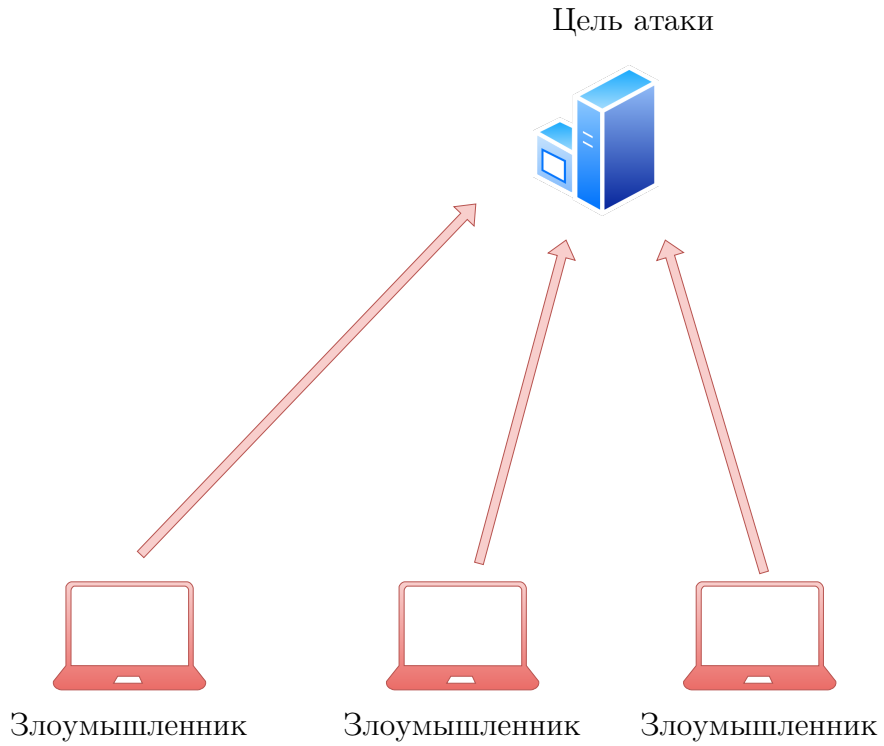


Рисунок 1.3 – Сетевая атака «многие к одному»

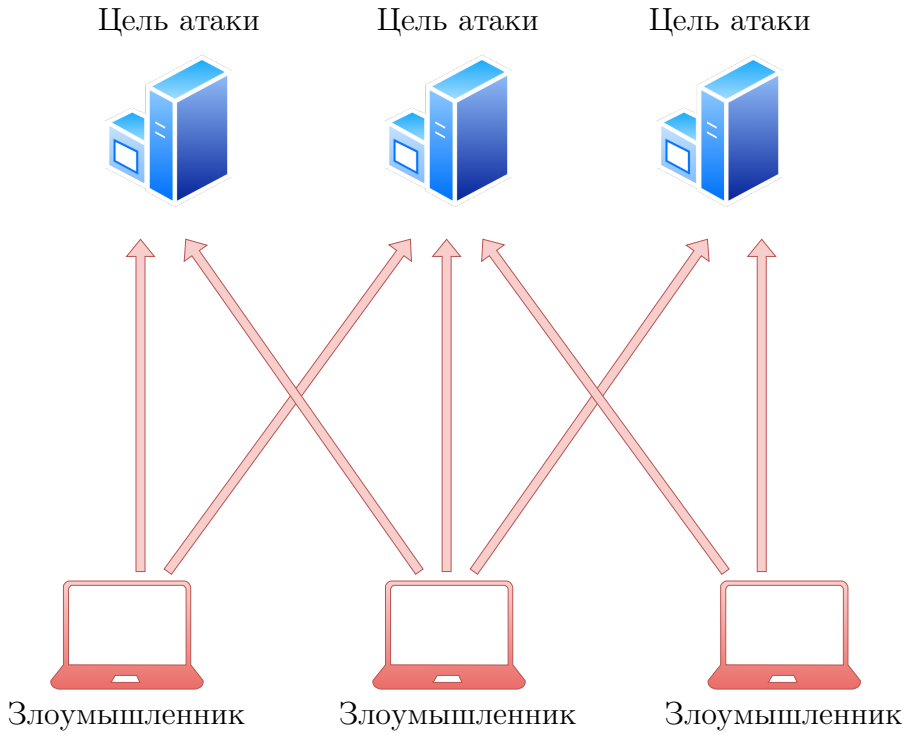


Рисунок 1.4 – Сетевая атака «многие ко многим»

1.2 Классификация сетевых атак

Большинство сетевых атак нацелены на изменение определенных параметров безопасности системы. Например, с помощью некоторых атак злоумышленник может получить возможность просматривать передаваемые сообщения,

но не изменять их. Другие атаки могут позволить злоумышленнику выполнить останов некоторых компонент системы, при этом не предоставляя доступ к ресурсам, хранящимся в данной системе [3].

Существует множество различных типов классификации атак. Например, деление на внешние и внутренние, пассивные и активные, умышленные и неумышленные. Однако, все сетевые атаки можно разделить на два класса: пассивные и активные [3].

Пассивная атака [4] — это атака, при которой у злоумышленника нет доступа к модификации передаваемых сообщений и возможности добавления собственных сообщений в информационный канал между отправителем и получателем. Основная цель пассивной атаки — прослушивание передаваемых сообщений и анализ сетевого трафика.

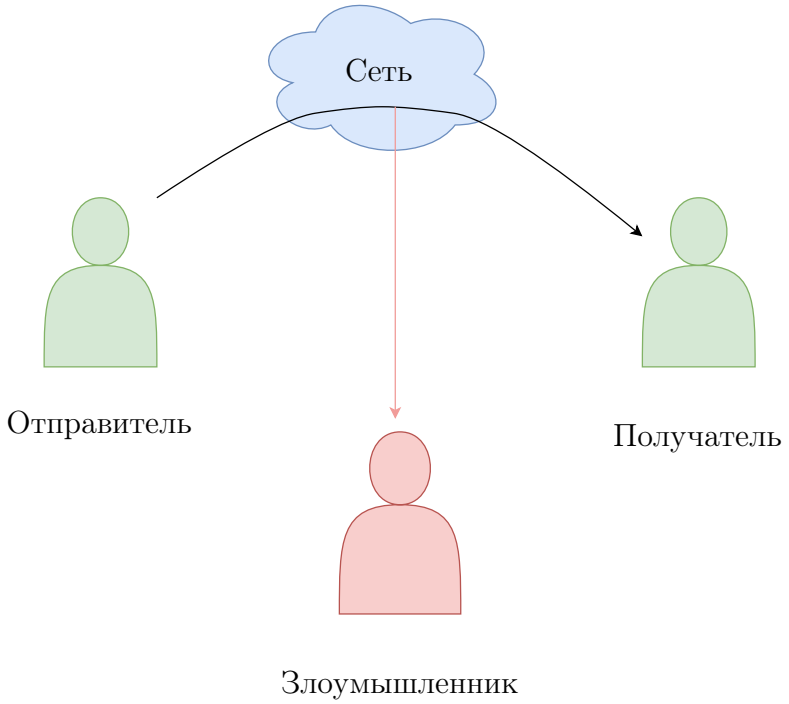


Рисунок 1.5 – Пассивная атака

Одной из разновидностей пассивных атак являются **атаки сканирования** [5]. Атаки сканирования не нацелены на проникновение в систему. Они помогают злоумышленнику определять:

— топологию сети;

— активные хосты в сети;

— выполняемое на хостах ПО сервера;

— номера версий обнаруженного ПО.

На рисунке 1.6 представлены инструментальные средства для осуществления атаки сканирования.

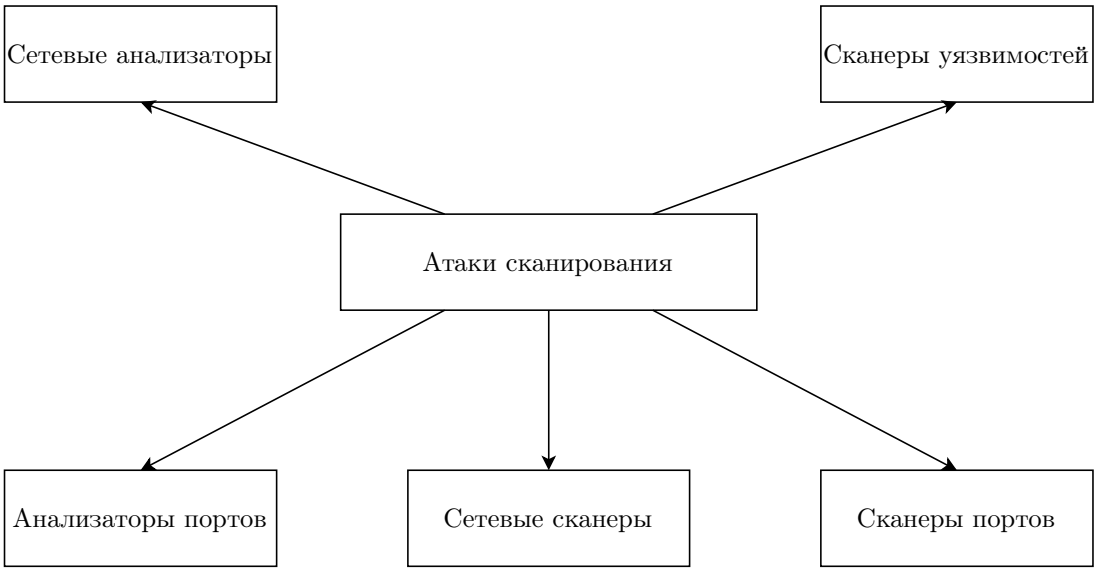


Рисунок 1.6 – Инструментальные средства для осуществления атаки сканирования

Активная атака [6] — это атака, при которой у злоумышленника имеется возможность модифицировать передаваемые сообщения и добавлять собственные. Существуют следующие типы активных атак:

1. **Отказ в обслуживании — DoS-атака (Denial of Service)** [5]. Отказ в обслуживании нарушает функционирование сетевых сервисов. Суть данной атаки заключается в следующем: на сетевой сервис поступает значительное количество запросов, в результате чего сетевой сервис перестает обрабатывать запросы реальных клиентов, а злоумышленник может перехватывать все сообщения направленные определенному адресату. DoS-атака базируется на классической модели атак.

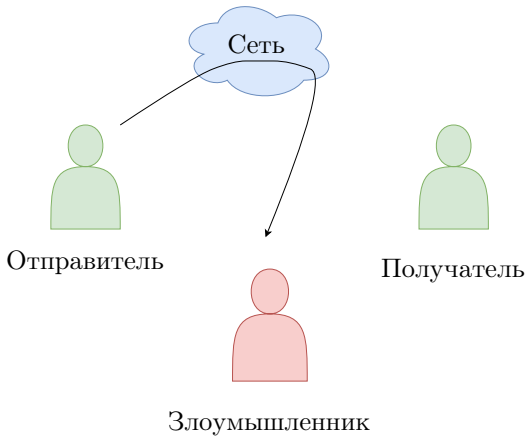


Рисунок 1.7 – DoS-атака

2. **Распределенный отказ в обслуживании — DDoS (Distributed Denial of Service)** [5]. Основным отличием DDoS-атаки от DoS-атаки является использование распределенной модели атак.

3. **Модификация потока данных — MITM-атака (Men In The Middle)** [6]. MITM-атака — это атака, с помощью которой злоумышленник перехватывает связь между клиентом и сервисом. Позиционируя себя между законным клиентом и сервисом, злоумышленник может отключить шифрование и перехватить сообщения, отправляемые клиенту или сервису. Это позволяет злоумышленнику получать конфиденциальную информацию, такую как учетные данные и другую личную информацию.

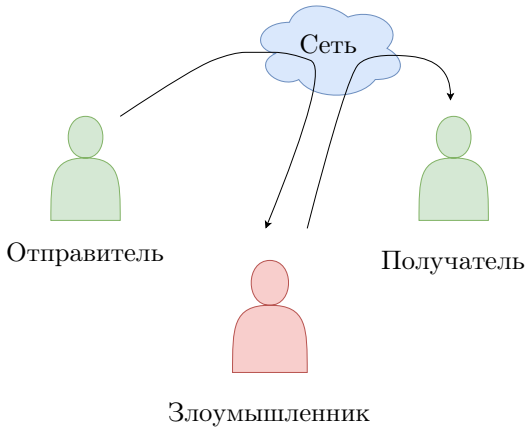


Рисунок 1.8 – MITM-атака

4. **Создание ложного потока (фальсификация)** [7]. Фальсификация означает попытку одного субъекта выдать себя за другого. С помощью

этой атаки злоумышленник может получить привилегии, которые не предусмотрены данной системой. Привилегия позволяет злоумышленнику в дальнейшем нарушить конфиденциальность, доступность или целостность сервиса.

5. **Атака повторного воспроизведения — Replay-атака** [7]. Атака повторного воспроизведения — атака на систему аутентификации путём записи и последующего воспроизведения ранее посланных корректных сообщений или их частей. Для совершения данного вида атаки злоумышленник пользуется несовершенством системы аутентификации потока данных. Злоумышленник перехватывает несколько пакетов или команд приложения, изменяет их и воспроизводит с целью выполнения несанкционированных действий.

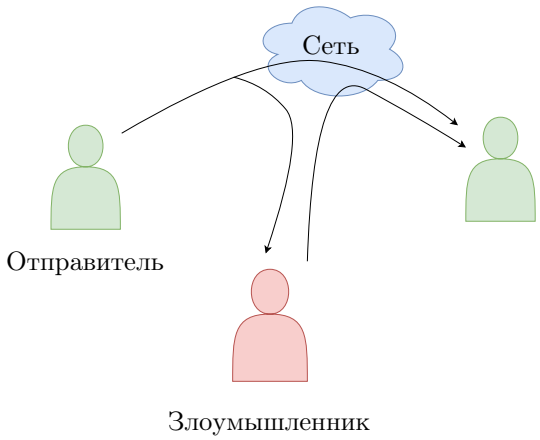


Рисунок 1.9 – Replay-атака

2 Методы обнаружения сетевых атак

Общий алгоритм выявления сетевых атак описывается следующим образом:

1. Собирается весь сетевой трафик, представленный как набор сетевых пакетов.

2. Вычисляются признаковые атрибуты сетевого трафика и строится профиль активности пользователя.

3. Созданный набор признаковых атрибутов сравнивается с набором характеристик нормального поведения пользователя.

4. Если в результате получилось весомое расхождение сравниваемых атрибутов, то фиксируется сетевая атака. В противном случае происходит изменение параметров нормального поведения.

2.1 Обзор методов обнаружения сетевых атак

Пороговый анализ

В методе порогового анализа [8] сначала выбирается набор сетевых параметров, а именно:

— IP-адреса источника и приемника — $\mathbf{S/D}$;

— тип и порт пакета — $\mathbf{Tp}$;

— длина пакета — $\mathbf{L}$;

— время фиксации пакета — $\mathbf{Tm}$.

Следовательное любое зафиксированное событие в сети можно описать вектором-объектом события $Tr =< S/D, Tp, L, Tm >$. Далее из события Tr извлекается объект $X = Tr < L >$, который соответствует длине зафиксированного пакета. Пусть X_i — событие из множества событий X, в некоторый момент времени. Тогда Y_i — аналогичный набор событий из множества, составляющего шаблон штатного функционирования сети. Затем выбирается

коэффициент «чувствительности» $k = 0.8$. Тогда нижний порог определяется как $X_i > kY_i$, а верхний как $X_i < \frac{Y_i}{k}$. После этого определяются краевые значения допустимых интервалов. Для этого берется выборочное среднее $\bar{X}$.

$$\bar{X} = \frac{1}{n} \sum_{i=0}^{n} X_i \tag{2.1}$$

Допустимый диапазон определяется следующим неравенством:

$$\frac{\bar{X}}{2} < X_i < \frac{3}{2}\bar{X} \tag{2.2}$$

Нахождение вне рамок этого диапазона свидетельствует аномальному поведению.

Недостатком данного метода является необходимость точного задания коэффициента «чувствительности» k и отсутствие адаптивных механизмов для автоматического выбора порога [9].

Анализ энтропии

Как известно энтропия множества X определяется следующим образом:

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i, \tag{2.3}$$

где p_i — вероятность i-го состояния системы, n — количество всех возможных состояний системы [10].

Метод анализа энтропии [11] базируется на построении модели, которая максимизировала бы значение энтропии. Так как с увеличением количества уникальных записей происходит их равномерное распределение относительно классов множества X, что приводит к увеличению энтропии.

Для анализа энтропии выбирается следующий набор сетевых параметров

— IP-адрес источника;

— IP-адрес приемника;

— сетевой порт источника;

— сетевой порт приемника.

Алгоритм

1. Выбираются атрибуты для построения энтропийных временных рядов.
2. Строится множество временных рядов T.
3. Для каждого T_i определяется ошибка прогноза на момент времени t:

$$\delta_i = |Pred(T_i(t)) - T_i(t)|. \tag{2.4}$$

4. Нормализуются ошибки предсказания относительно дисперсии соответствующих временных рядов путем умножения на весовой коэффициент. Весовой коэффициент вычисляется по следующей формуле:

$$\omega_i = \frac{1}{\sigma_i} max(\sigma_1, ..., \sigma_n). \tag{2.5}$$

5. Вводится совокупная характеристика AS (anomaly score):

$$AS = \sum_{i=1}^{n} \delta_i \omega_i \tag{2.6}$$

6. Если $AS > AS_{thr}$, то фиксируется некая аномалия сетевого трафика. Пороговая величина AS_{thr} определяется эмпирически в зависимости от количества базовых временных рядов n.

Байесовский метод

Байесовская сеть [12] представляет собой модель, которая кодирует вероятностные отношения между некоторыми событиями и предоставляет механизм для вычисления условных вероятностей их наступления. В данном методе используются оценочные функции для определения вероятностей новых сетевых атак. Вследствие свойств предложенного метода системе не нужны предварительные знания о шаблонах атак.

Алгоритм

На первом этапе собирается информация о сетевых параметрах, а именно:

— IP-адрес источника;

— IP-адрес приемника;

— сетевой порт источника;

— сетевой порт приемника;

— состояние соединения;

— временная метка.

Далее применяются правила ассоциации $X->Y$ к записям соединений, где X и Y предусловие и постусловие правил, описанных внутри ядра системы соответственно. Затем строятся профили нормального поведения клиентов системы и генерируются правила ассоциации, используемые впоследствии для обучения.

Основным преимуществом данного метода является работа в режиме реального времени.

SVM-метод

Метод опорных векторов — SVM-метод (Support Vector Machine) [13] рассматривается как один из ключевых методов обнаружения вторжений. SVM является производным от линейно разделяемой гиперплоскости оптимальной классификации, и его основная идея может быть объяснена двумерным случаем представленным на рисунке 2.1. Существует обучающий набор $D = (X_1, y_1), (X_2, y_2), ..., (X_n, y_n)$, где X_i — характеристический вектор обучающей выборке и y_i — соответствующая метка класса. y_i принимает значения $+1$ или -1, указывая, принадлежит вектор к этому классу или нет. Говорят, что он линейно разделим, если существует линейная функция, которая может полностью разделить на два класса. В противном случае он нелинейно разделим.

Рисунок 2.1 представляет собой линейно разделяемый случай, поскольку можно провести прямую линию, чтобы отделить вектор класса $+1$ от вектора класса -1. Существует бесчисленное множество таких линий, и так называемая оптимальная линия классификации требующая, чтобы две выборки были правильно разделены и чтобы интервал разделения был наибольшим.

SVM завершает классификацию выборки путем поиска той, которая имеет наибольший интервал классификации.

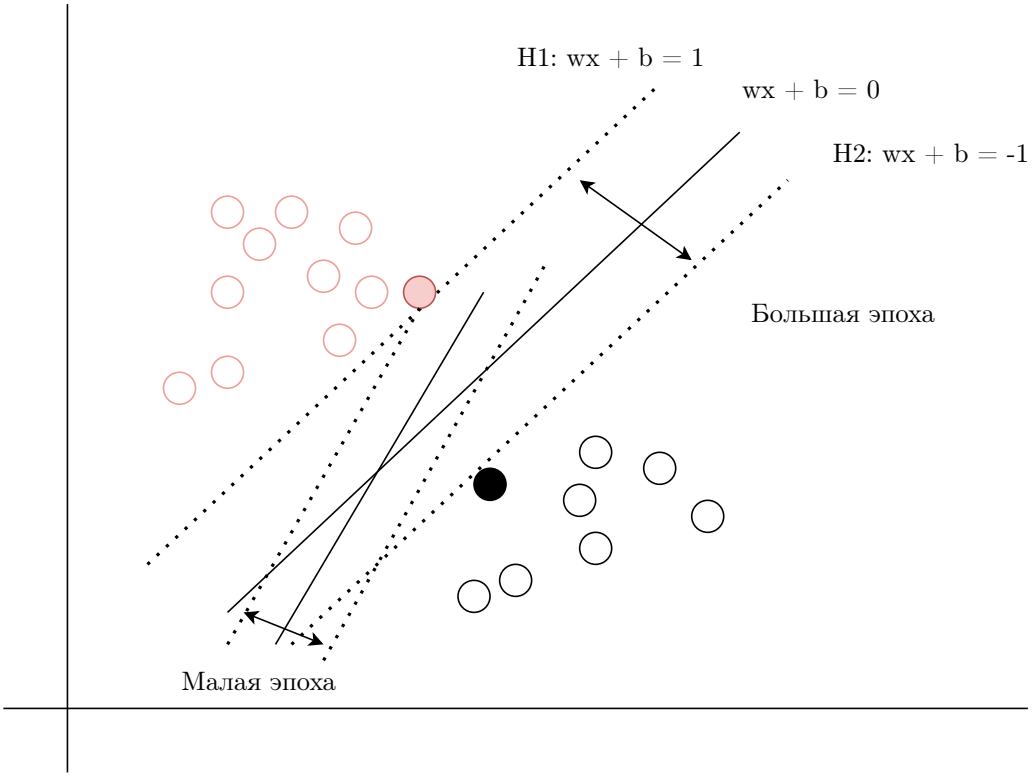


Рисунок 2.1 – SVM-метод

Оптимальная линия классификации может быть выражена уравнением $\omega x + b = 0 (\omega \in R^n, b \in R)$, ω представляет собой вектор веса, а b — скаляр, называемый смещением. Точки над разделяющей гиперплоскостью удовлетворяются следующим образом:

$$\omega x + b > 0. \tag{2.7}$$

Аналогично, точки ниже разделяющей гиперплоскости удовлетворяются следующим образом:

$$\omega x + b < 0. \tag{2.8}$$

Мы можем отрегулировать вес, чтобы крайняя сторона гиперплоскости могла быть выражена как:

$$\begin{aligned} H1 : \omega x + b \geq 1, y_i = 1; \\ H2 : \omega x + b \leq 1, y_i = -1. \end{aligned} \tag{2.9}$$

Это означает, что векторы, падающие на или выше $H1$, принадлежат классу $+1$, а векторы, падающие на или ниже $H2$, принадлежат классу -1.

Обнаружение сетевой атаки эквивалентно задаче с двумя классификациями. Сначала собираются данные сетевого подключения для обучения, затем находится оптимальная классификационная гиперплоскость между данными нормального поведения и данными сетевой атаки [14].

2.2 Сравнение и оценка методов

Сравнение методов обнаружения сетевых атак произведено по следующим критериям:

— К1 — адаптивность;

— К2 — устойчивость;

— К3 — уровень наблюдения;

Результаты сравнений приведены в таблице 2.1.

Таблица 2.1 – Сравнение методов

	К1	**К2**	**К3**
Анализ энтропии	+	-	HIDS, NIDS, AIDS, Hybrid
Пороговый анализ	+	-	HIDS, NIDS, AIDS, Hybrid
Байесовский метод	-	+	NIDS, HIDS
SVM-метод	+	-	NIDS, HIDS

В таблице используется обозначения уровня наблюдения появления аномалии в сети:

— HIDS [15] — наблюдение на уровне операционной системы отдельного узла сети;

— NIDS [15] — наблюдение на уровне сетевого взаимодействия объектов на узлах;

— AIDS [15] — наблюдение на уровне отдельных приложений узла сети;

— Hybrid [15] — комбинация наблюдателей разных уровней.

2.3 Вывод

Таким образом, по результатам сравнительного анализа было выявлено, что методы порогового анализа и анализа энтропии обладают наиболее высокой адаптивностью к новым данным и способны проводить наблюдение на всех выделенных уровнях сети.

ЗАКЛЮЧЕНИЕ

В рамках данной научно-исследовательской работы была приведена классификация методов обнаружения сетевых атак и произведено их сравнение. С точки зрения устойчивости адаптивности и обширности уровней наблюдения оказались методы порогового анализа и анализа энтропии. При написании работы были выполнены следующие задачи:

— 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;

Таким образом, все поставленные задачи выполнены, а цель достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Исупов А. О.* Актуальные киберугрозы: IV квартал 2022 года [Электронный ресурс] // Россия, Positive Technologies Researches. — 2022. — URL: `https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/`.
2. *Лукацкий А. В.* Обнаружение сетевых атак // Россия, СПб, БХВ-Петербург. — 2016.
3. *Шаньгин В. Ф.* Информационная безопасность компьютерных систем и сетей // Россия, Москва, ИНФРА-М. — 2018.
4. *Seredinski F.* Anomaly detection in TCP/IP networks using immune systems paradigm // Poland, Warsaw, Computer Communications. — 2010.
5. *Hofmeyr S. A.* Architecture for an Artificial Immune System // Journal of Evolutionary Computation. — 2010.
6. *Chen W. H.* Application of SVM and ANN for intrusion detection // Computers and Operations Research. — 2011.
7. *Vaitsekhovich L.* Intrusion Detection in TCP/IP Networks Using Immune Systems Paradigm and Neural Network Detectors // XI International PhD Workshop OWD. — 2019.
8. *Komar M.* Development of Neural Network Immune Detectors for Computer Attacks Recognition and Classification // IEEE 7th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems. — 2013.
9. *Cannady J.* The Application of Artificial Neural Networks to Misuse Detection: Initial Results // Proceedings of the 1st International Workshop on Recent Advances in Intrusion Detection. — 2008.
10. *Sharma S. D.* Improved Algorithm for Intrusion Detection Using Genetic Algorithm and SNORT // International Journal of Emerging Technology and Advanced Engineering. — 2014.
11. *Котенко И. В.* Использование многоагентных технологий для комплексной защиты информации в компьютерных сетях // Россия, Томск, Известия ТРТУ. — 2001.

12. *Уланов А. В.* Проактивные механизмы защиты от сетевых червей: подход, реализация и результаты экспериментов // Россия, Омск, Информационные технологии ОГУ. — 2014.

13. *Govindarajan M.* Intrusion Detection Using an Ensemble of Classification Methods // Proc. of the World Congress on Engineering and Computer Science. — 2012.

14. *Powers S. T.* Hybrid Artificial Immune System and Self Organising Map for Network Intrusion Detection // Information Sciences. — 2018.

15. *Abraham A.* Distributed intrusion detection systems: a computational intelligence approach // Applications of Information Systems to Homeland Security and Defense. — 2015.

ПРИЛОЖЕНИЕ А

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:

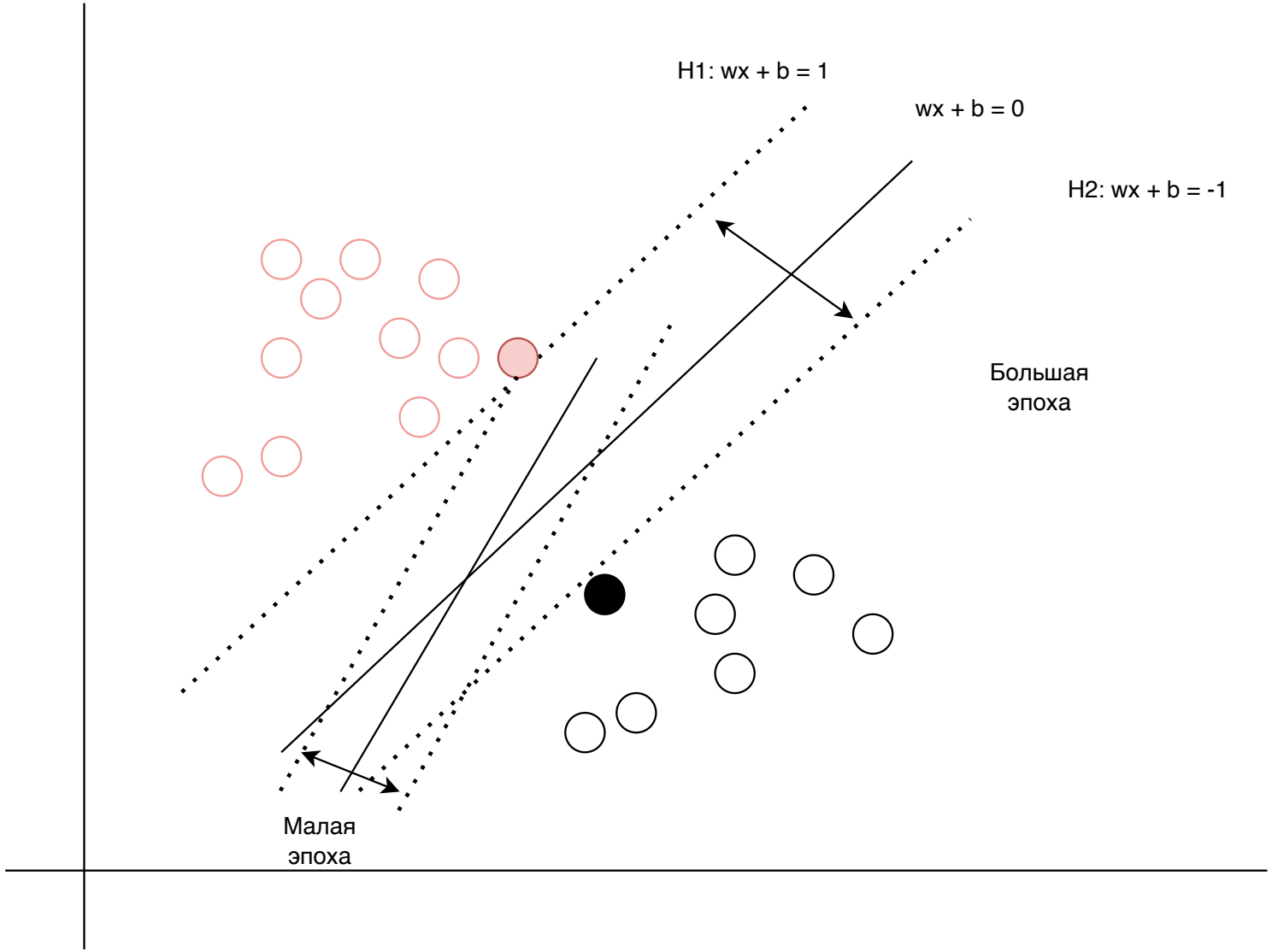
- IP-адреса источника и приемника;
- сетевой порт источника;
- сетевой порт приемника.

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.