УДК 004.056

Аникин С.А.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

Научный руководитель:
Козырева Н.И.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

ПРИМЕНЕНИЕ МЕТОДА ХОЛЬТА-ВИНТЕРСА ДЛЯ ПРОГНОЗИРОВАНИЯ КОЛИЧЕСТВА СЕТЕВЫХ АТАК

Аннотация. В работе рассматривается применение метода Холта-Винтерса для прогнозирования кибератак. Исследуются аддитивная и мультипликативная модели, позволяющие учитывать тренд и сезонность в данных о киберугрозах. Приведены основные формулы метода, а также проведен анализ их применимости для задач информационной безопасности.

Ключевые слова: прогнозирование кибератак, метод Холта-Винтерса, аддитивная модель, мультипликативная модель, временные ряды, информационная безопасность.

Прогнозирование сетевых атак с помощью статических методов – это одна из ключевых техник в области информационной безопасности. Статические методы, в отличие от динамических, не требуют анализа поведения системы в реальном времени. Вместо этого они основаны на предварительном анализе данных, которые не изменяются во времени, и использованию различных алгоритмов для выявления уязвимостей и угроз.

Современные киберугрозы обладают выраженной временной динамикой и сезонными паттернами, что делает методы анализа временных рядов, в частности подход Хольта-Винтерса, перспективным инструментом для прогнозирования атак на основе исторических данных, выявления аномальной активности в сетевом трафике и эффективного использования ресурсов систем защиты. Практическая реализация может достигаться путем сбора исторических данных об атаках, выявления сезонности.

Вопрос выбора модели метода Хольта-Винтерса зависит от характера анализируемых данных и типа угроз. Мультипликативная модель будет применяться при:

- растущей амплитуде колебаний (например, объем DDoS-атак, который увеличивается пропорционально общему трафику);
- при анализе интенсивности атак, где сезонные всплески усиливаются с ростом базового уровня угроз;

• для финансовых показателей киберпреступности (объемы украденных средств).

Пример использования: прогнозирование пиков фишинговых атак в предпраздничные периоды, когда их количество растет в процентном соотношении к базовому уровню.

Аддитивная модель:

• для показателей с постоянной амплитудой колебаний (например, количество попыток сканирования портов);

• при мониторинге рутинных угроз с устойчивыми сезонными паттернами;

• для показателей, где сезонные колебания не зависят от базового уровня.

Пример: прогнозирование суточной активности бот-сетей, где ночные атаки всегда превышают дневные на примерно постоянную величину.

Было рассмотрено две модели посредствам языка программирования python3, с целью изучения и прогнозирования возможных атак. Исходные данные были взяты из отчетов компании ddos-guard [3]. Поскольку в рассматриваемом случае не наблюдается постоянной амплитуды колебаний, то аддитивную модель можно не рассматривать.

Математическая форма аддитивной модели записи имеет вид [2]:

$$L_t = \alpha \cdot (Y_t - S_{t-s}) + (1 - \alpha) \cdot (L_{t-1} + T_{t-1}), \quad (1)$$

$$T_t = \beta \cdot (L_t - L_{t-1}) + (1 - \beta) \cdot T_{t-1}, \quad (2)$$

$$S_t = \gamma \cdot (Y_t - L_t) + (1 - \gamma) \cdot S_{t-m}, \quad (3)$$

$$\acute{Y}_{t+h} = L_t + h \cdot T_t + S_{s+t-m}\ , \quad (4)$$

где Y_t – фактическое значение в момент времени t; L_t – уровень в момент времени t; T_t – тренд в момент времени; S_t – сезонность в момент времени t; $\alpha,\ \beta, \gamma$ – параметры сглаживания, которые определяют вес каждого компонента; h – это количество периодов вперед, на которые нужно сделать прогноз; m – длина сезонного периода.

Математическая запись мультипликативной модели имеет следующий вид и описывается формулами 5–8 [1].

$$L_t = \alpha \cdot \frac{Y_t}{S_{t-s}} + (1 - \alpha) \cdot (L_{t-1} + T_{t-1}), \quad (5)$$

$$T_t = \beta \cdot (L_t - L_{t-1}) + (1 - \beta) \cdot T_{t-1}, \quad (6)$$

$$S_t = \gamma \cdot \frac{Y_t}{L_t} + (1 - \gamma) \cdot S_{t-m}, \quad (7)$$

$$\acute{Y}_{t+h} = (L_t + h \cdot T_t) + S_{s+t-m}\ , \quad (8)$$

где Y_t – фактическое значение в момент времени t; L_t – уровень в момент времени t; T_t – тренд в момент времени; S_t – сезонность в момент времени t; $\alpha,\ \beta, \gamma$ – параметры сглаживания, которые определяют вес каждого компонента; h – это количество периодов вперед, на которые нужно сделать прогноз; m – длина сезонного периода.

Проведенное исследование выявило ключевые ограничения классических методов прогнозирования временных рядов, в частности модели Хольта-Винтерса, для задач информационной безопасности.

В качестве перспективы можно выделить разработку гибридных систем, учитывающие тренд аномалии и внешние факторы, а также модели способные адаптироваться к новым угрозам.

Список использованных источников:

1. А. С. Поздняков. Применение метода Хольта-Винтерса при анализе и прогнозировании динамики временных рядов. URL: https://masters.donntu.ru/2017/fknt/vudvud/library/article6.pdf (дата обращения 10.01.2025).

2. Прогноз по методу экспоненциального сглаживания с трендом и сезонностью (Хольта-Винтерса) // 4Analytics: [сайт]. URL: https://4analytics.ru/prognozirovanie/prognoz-po-metodu-eksponencialnogo-sglajivaniya-s-trendom-i-sezonnostyu-xolta-vintersa.html (дата обращения: 10.01.2025).

3. Статистика DDoS-атак: [ежеквартальные отчеты] / DDoS-Guard. URL: https://ddos-guard.ru/reports (дата обращения: 09.01.2025).

Anikin S.A.
Volga Region State University of
Telecommunications and Informatics, Samara

Scientific supervisor:
Kozyreva N.I.
Volga Region State University of
Telecommunications and Informatics, Samara

INVESTIGATION OF THE HOLT-WINTERS METHOD FOR PREDICTING THE NUMBER OF NETWORK ATTACKS

Abstract. This paper explores the application of the Holt-Winters method for forecasting cyberattacks. The additive and multiplicative models are examined, enabling the analysis of trends and seasonality in cyber threat data. Key formulas of the method are presented, along with an evaluation of their applicability in cybersecurity tasks. The study demonstrates the effectiveness of this approach for short- and medium-term attack prediction, which can support the development of proactive defense measures.

Keywords: cyberattack forecasting, Holt-Winters method, additive model, multiplicative model, time series analysis, cybersecurity.