ПРОГНОЗИРОВАНИЕ СТАТИСТИЧЕСКИХ ДАННЫХ АТАК НА ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Ларионов К.О.
Email: Larionov17163@scientifictext.ru

Ларионов Константин Олегович – аспирант,
кафедра вычислительной техники и защиты информации,
Оренбургский государственный университет, г. Оренбург

Аннотация: *в статье описывается метод прогнозирования статистических данных атак на прикладное программное обеспечение. Актуальность разработки метода обуславливается тем, что в работе применяется метод прогнозирования сезонных рядов количества атак на прикладное программное обеспечение. В качестве достоинств работы стоит отметить использование метода прогнозирования полигармоническим полиномом узкоспециализированных сезонных рядов, возможность гибко настраивать модель под конкретный ряд в зависимости от внешних условий, где находятся собранные статистические данные, ошибка при построении прогноза составила 12.33%.*
Ключевые слова: *защита, система, информация, программное обеспечение, нефтегазовое оборудование, анализ, методы защиты, прогнозирование, метод, полигармонический полином, сезонность.*

FORECASTING ATTACK STATISTICS ON APPLIED SOFTWARE

Larionov K.O.

Larionov Konstantin Olegovich – Postgraduate,
DEPARTMENT OF COMPUTING AND INFORMATION SECURITY,
ORENBURG STATE UNIVERSITY, ORENBURG

Abstract: *the article describes a method for predicting statistical data of attacks on applied software. The relevance of the development of the method is due to the fact that the method for predicting the seasonal series of the number of attacks on applied software is used in the work. As the advantages of the work, it is worth noting the use of the polyharmonic polynomial forecasting method for highly specialized seasonal series, the ability to flexibly adjust the model for a specific series, depending on the external conditions where the collected statistical data are located, the error in forecasting was 12.33%.*
Keywords: *protection, system, information, software, oil and gas equipment, analysis, protection methods, forecasting, method, polyharmonic polynomial, seasonality.*

УДК 004.421.2

Программное обеспечение (ПО) является одной из основных составляющих любой современной ИС: отдельного ПК, вычислительных и телекоммуникационных сетей различного размера и назначения, от небольших локальных до глобальных.

Современные средства программного обеспечения осуществляют реализацию все более сложных и эффективных ИТ во всех сферах человеческой деятельности. Однако само ПО подвержено воздействию большого числа дестабилизирующих факторов.

Существенный урон программным продуктам наносят такие несанкционированные действия, как несанкционированное копирование программ, их незаконное распространение и использование, в результате чего снижается его качество, вплоть до полного прекращения его функционирования и наносит значительный материальный ущерб фирмам-изготовителям программного обеспечения.

В настоящее время разработано достаточно много средств защиты программного обеспечения:

- программные;
- технические;
- правовые.

Однако реально существует проблема выбора наиболее эффективных методов и средств защиты ПО в конкретных ИС.

Актуальность данной работы заключается в том, что была предпринята попытка использования метода прогнозирования сезонных рядов количества атак на прикладное программное обеспечение.

На рисунке 1 представлен сравнительный график атак на программное средство начала 2020 года по данным ptsecurity.

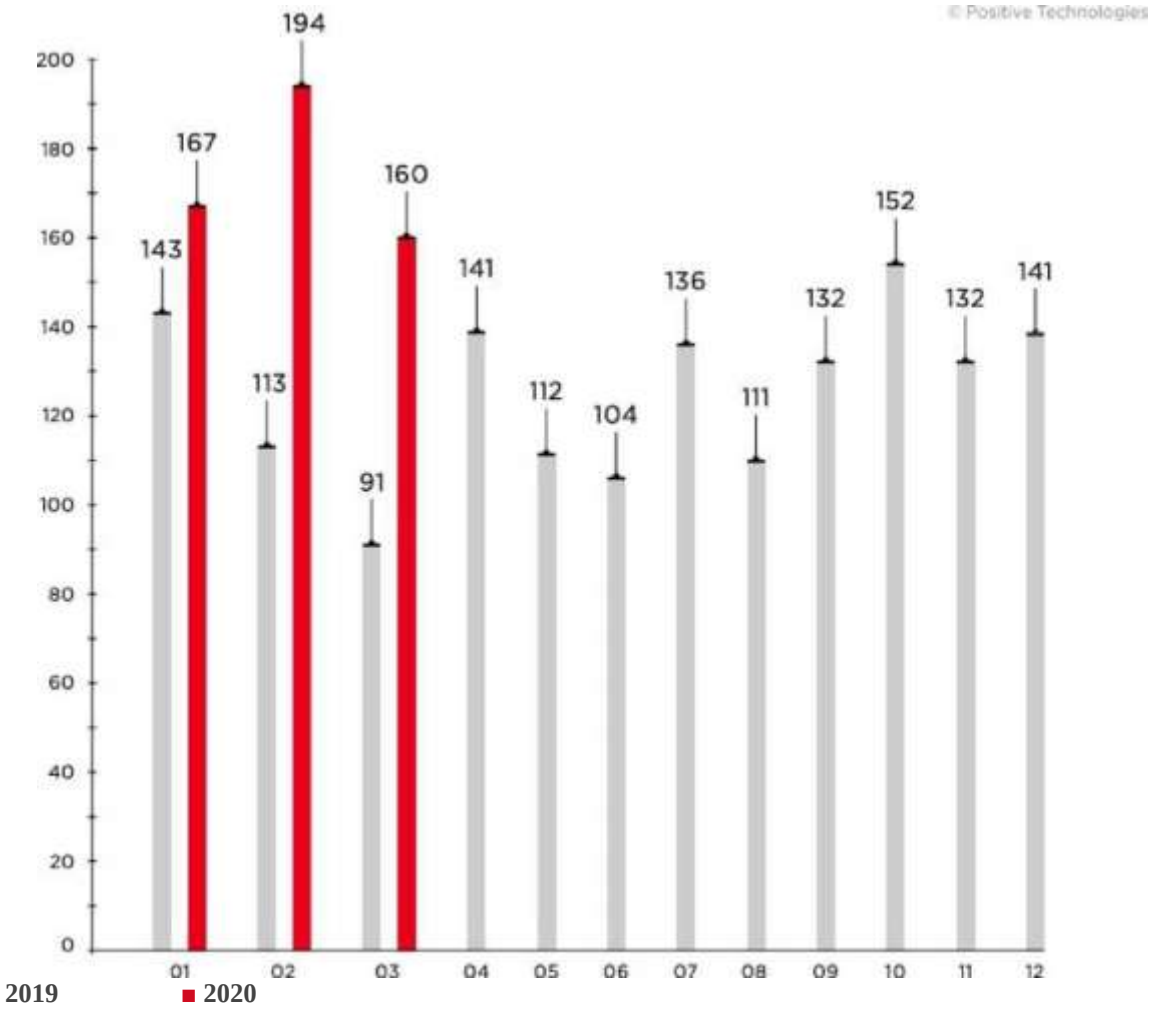

Рис. 1. Сравнительный график атак на программное средство начала 2020

В работе Лебедева С.С. «Разработка методов и средств комплексной оценки качества систем защиты программного обеспечения» дается определение качества системы защиты программного обеспечения. Определены функции системы защиты в составе комплекса из системы защиты и защищаемого программного обеспечения. Разработана модель системы "защищаемое программное обеспечение - система защиты программного обеспечения", а также выполнен анализ работоспособности этой модели с учетом функциональных связей между ее структурными элементами. Однако нет собранных статических данных по угрозам и отсутствует пункт прогнозирование угроз программного обеспечения.

В работе Барабанова А.В. «О систематике информационной безопасности цепей поставки программного обеспечения» представлены результаты систематизации мер защиты информационных ресурсов от компьютерных атак на цепи поставок программного обеспечения и программно-аппаратных комплексов. Отмечены феномены, актуальность и востребованность тематики защиты цепей поставки ИТ-продукции. Приведена статистика по заимствованным компонентам программной продукции и программных комплексов. Приведены примеры компьютерных атак на ресурсы и процессы цепи поставок программного обеспечения. Проведен анализ существующей терминологической базы в области безопасности цепей поставок программного обеспечения. Сформулированы основные свойства, характерные для терминов «цепь поставок» и «атака на цепь поставок». Проведен анализ существующих моделей угроз информационной безопасности, связанных с компьютерными атаками на цепи поставок программной продукции. Выявлены ограничения моделей угроз информационной безопасности цепи поставок программного обеспечения. Выполнен обзор и систематизация мер защиты информации от угроз информационной сферы, связанных с компьютерными атаками на цепи поставок программного обеспечения. Однако не рассматриваются глубоко атаки и их статистические данные на программное обеспечение.

Целью работы является снижение риска угроз атак на прикладное программное обеспечение в узкоспециализированных сферах.

Для достижения цели в работе поставлены следующие задачи:

1 Проанализировать временной ряд угрозы внедрения в прикладное программное средство стороннего вредоносного кода

Для построения прогнозного ряда была использована модель прогнозирования на базе полигармонического полинома, которая лучше всего подходит для сезонных временных рядов.

Модель полигармонического полинома описывается формулой 1.

$$X(t) = a_0 + \sum_{i=1}^{n} [a_i \cdot \cos(2 \cdot \pi \cdot K_i \cdot t / N) + b_i \cdot \sin(2 \cdot \pi \cdot K_i \cdot t / N)] + \varepsilon(t) + d_0 + c \quad (1)$$

где:

N - число элементов исходного ряда;

n - число гармоник полигармонического полинома;

Ki - коэффициенты, определяющие номер гармонии;

ε(t) - прогнозная оценка случайной компоненты;

t - порядковый номер элементов исходного ряда, *t* = 1,2, ...

На рисунке 2 представлен анализ статистических данных временного ряда угрозы внедрения вредоносного кода в программное обеспечение.

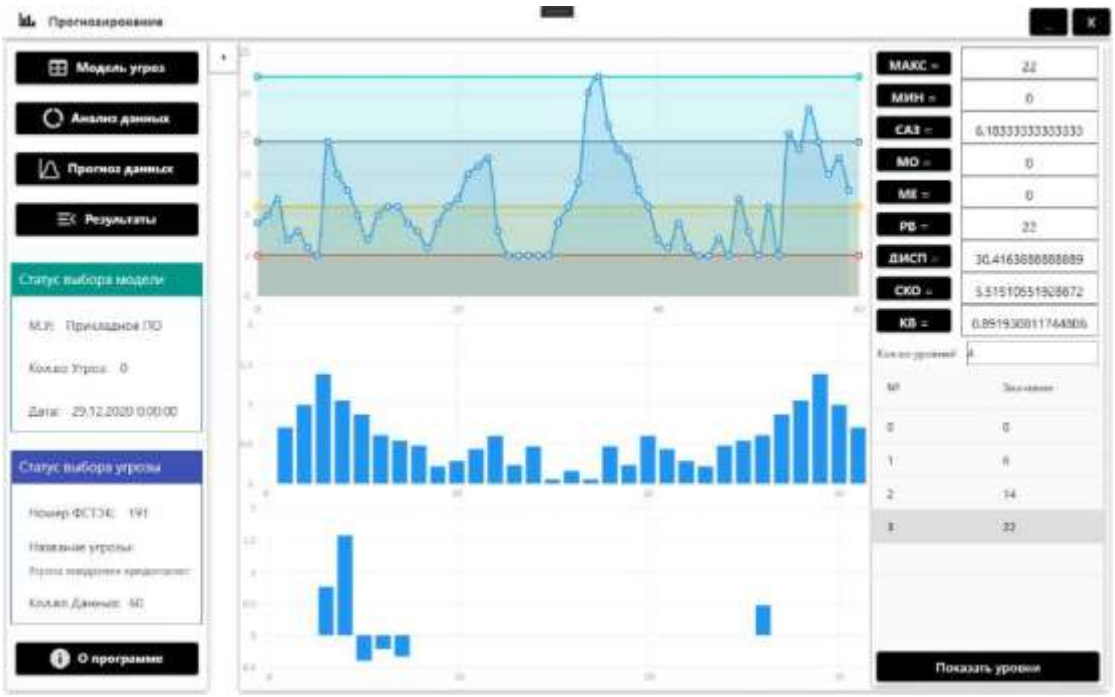

Рис. 2. Анализ статистических данных угрозы внедрения вредоносного кода в программное обеспечение

Из проведенного статистического анализа видно, что статистические данные представляют временной сезонный ряд, были выявлены основные уровни поддержки и сопротивления технического анализ графика. Основной уровень сопротивления 1 со значением в 6 единиц. Максимум графика не является основным уровнем сопротивления, потому что на нем находится минимальное количество статистических данных.

Ниже, на рисунке 3, приведено разложение временного ряда на сезонные компоненты.

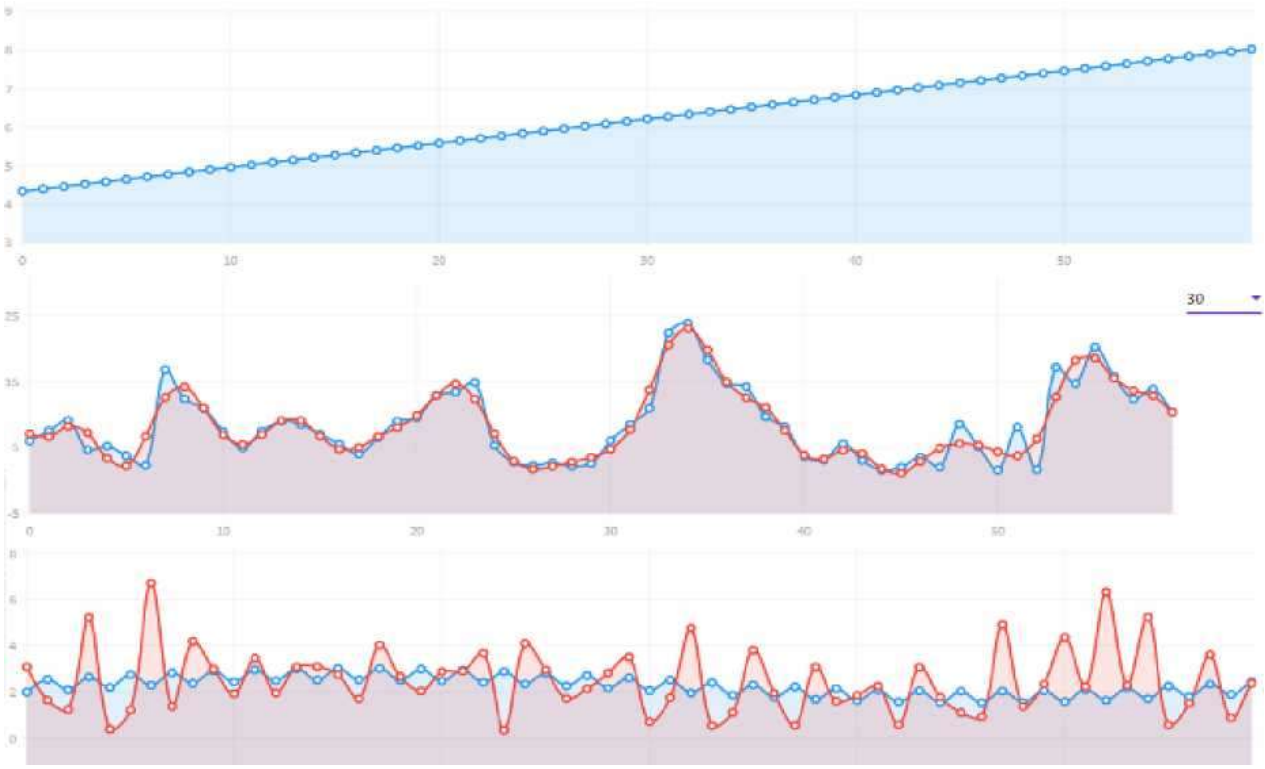

Рис. 3. Разложение временного ряда на сезонные компоненты

На рисунке 4 представлен анализ временного ряда угрозы внедрения вредоносного кода в программное обеспечение.

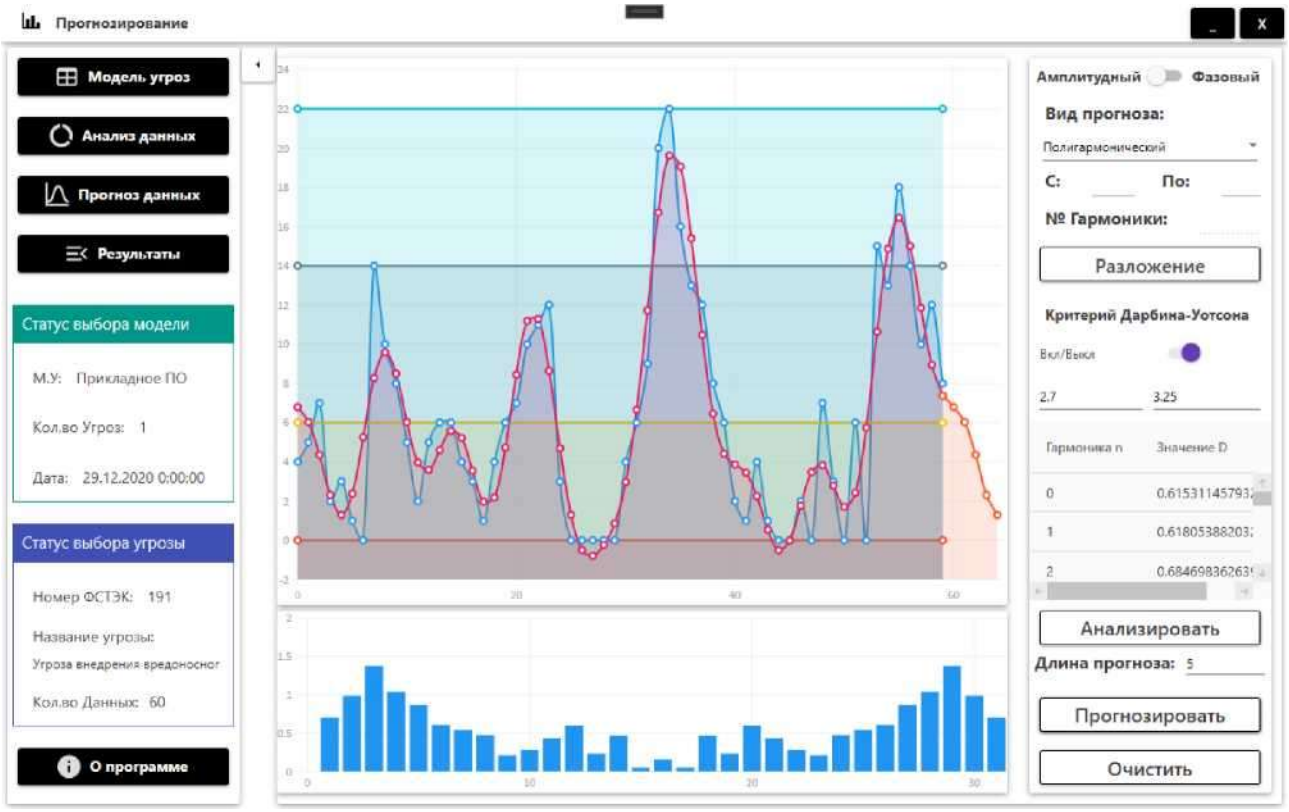

Рис. 4. Анализ временного ряда угрозы внедрения вредоносного кода в программное обеспечение

Из разложения видно, что случайная компонента в среднем равна 2 единицам, трендовая линия временного ряда направлена вверх, а сам временной ряд включает в себя 31 гармонику.

2 Построить прогнозный ряд количества попыток внедрения вредоносного кода в прикладное программное обеспечение.

Так как статистические данные изначально собраны за определенный сезонный промежуток в 2 месяца то проведем построение линии прогноза на области обучения всего графика, как представлено на рисунке 5.

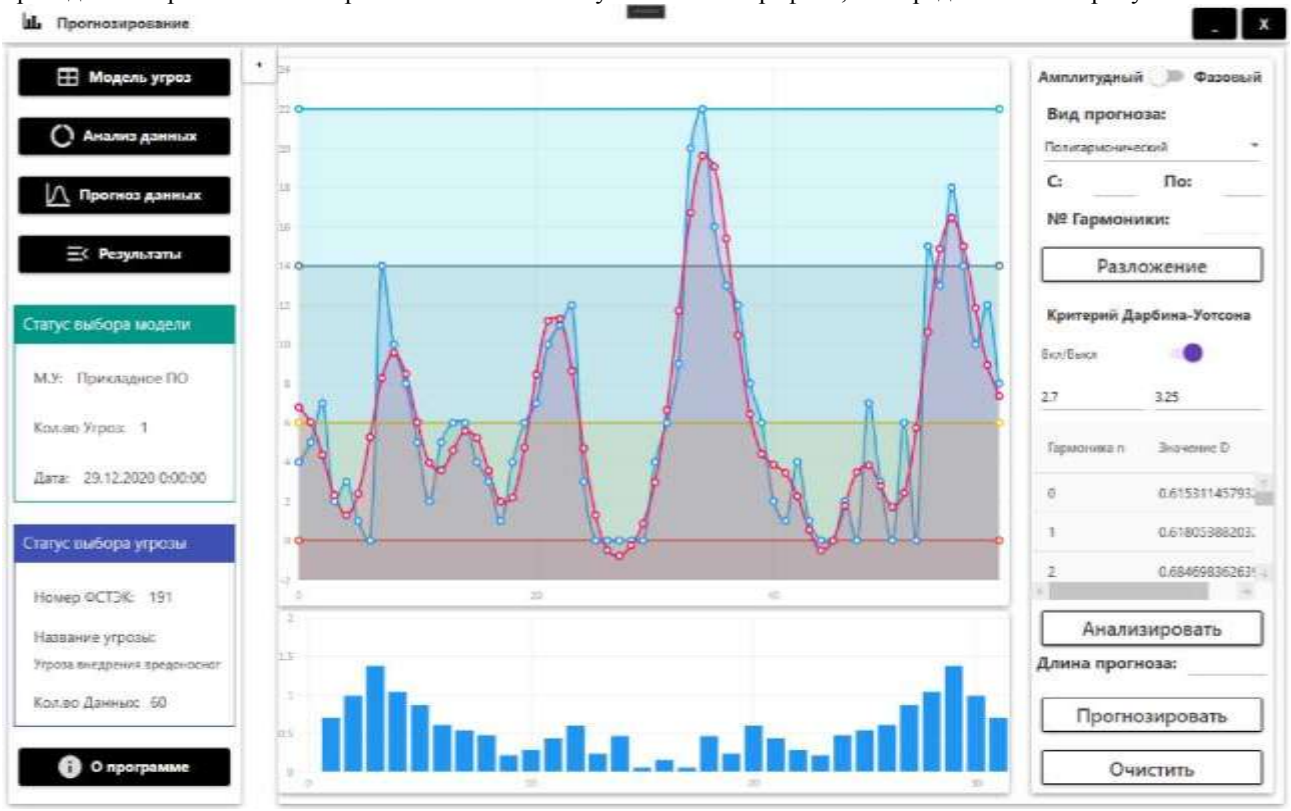

Рис. 5. Статистические данные прогнозного ряда угрозы внедрения вредоносного кода в прикладное программное обеспечение

Стоит отметить, что изначальный критерий с промежутком от 1.75 до 2.25 был скорректирован для улучшения качества прогнозного ряда. Используя обученную модель прогнозирования, проведем построение прогноза на 5 дней вперед, а именно начало рабочей недели следующего месяца, как представлено на рисунке 6.

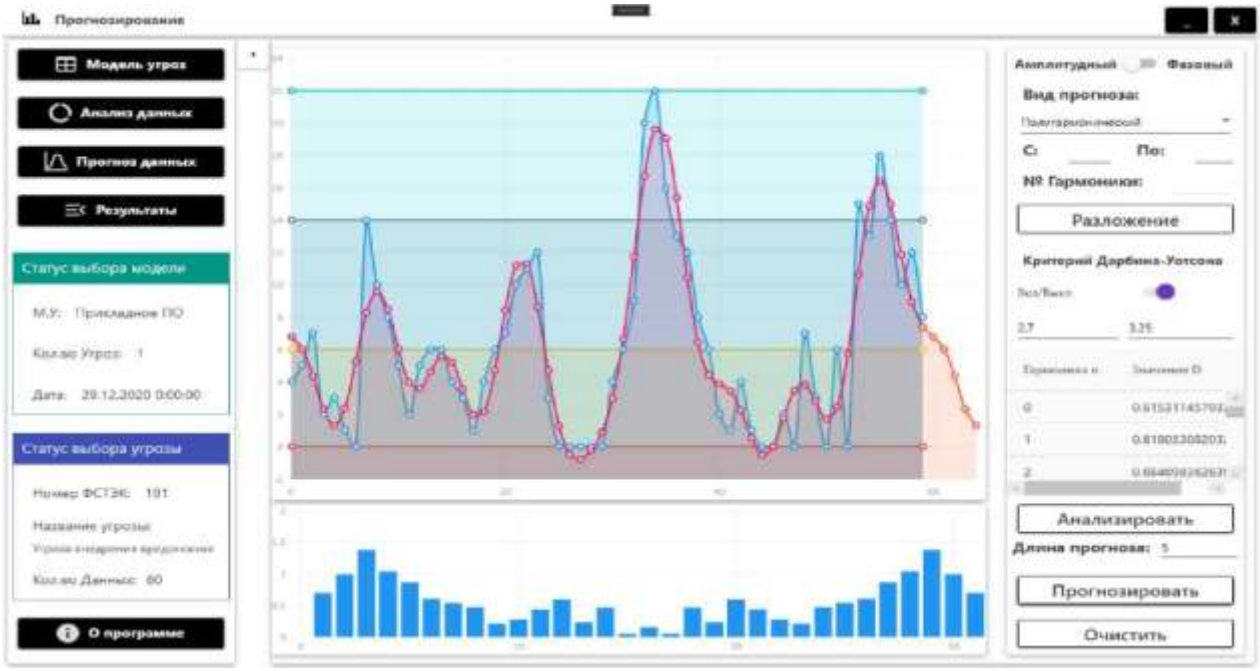

Рис. 6. Статистические данные прогнозного ряда угрозы внедрения вредоносного кода в прикладное программное обеспечение

Из проведенного построения прогноза на первую рабочую неделю следующего месяца видно, что локальный тренд временного ряда направлен вниз и стоит ожидать уменьшения количества попыток внедрения вредоносного кода в прикладное программное обеспечение.

В качестве достоинств работы стоит отметить использование метода прогнозирования полигармоническим полиномом узкоспециализированные сезонные ряды, возможность гибко настраивать модель под конкретный ряд в зависимости от внешних условий, где находятся собранные статистические данные, ошибка при построении прогноза составила 12.33%. В качестве недостатков работы можно отметить неспособность корректно работать с временными рядами, в которых не прослеживается сезонность. Любой временной ряд можно разложить на гармонические компоненты, однако, не любой ряд подается точному прогнозированию данных.

В заключение хочется отметить, что прогнозирование угроз на прикладные программные продукты особо актуально на сегодняшний день. Потому что атаки на прикладное ПО дают максимальный ущерб как промышленным организациям, так и финансовым, где применяется подобное программное обеспечение, особенно угроза внедрения вредоносного кода. Так как именно внедрение вредоносного кода дает полный или частично-максимальный контроль над прикладной системой, что позволяет нарушителям использовать ее в своих целях, примером может служить выставление ложных ордеров на биржах с целью обвала рыночного актива, или выявления проблем и поломок в системах нефтепровода при подъеме нефтяной жидкости.

Список литературы / References

1 *Гулов В.П.* Алгоритм прогнозирования вероятности реализации угроз несанкционированного доступа к информации технологических медицинских информационных систем / Гулов Владимир Павлович, Скрыпников А.В., Хвостов В.А., Пелешенко Е.И. Воронеж: Издательство: Printing house "Maestro", 2016. С. 31-35.

2 *Десницкий В.А.* Модель защиты программного обеспечения на основе механизма "удаленного доверия" / Десницкий В.А., Котенко И.В. Санкт-Петербург: Издательство: Министерство науки и высшего образования *РФ (Санкт-Петербург), 2008. С. 26-31.*

3 *Жигулин Г.П.* Мониторинг ресурсов и прогнозирования поля угроз системы защиты информации. Санкт-Петербург: Издательство: Федеральное государственное казенное военное образовательное учреждение высшего образования "Краснодарское высшее военное училище имени генерала армии С.М. Штеменко" Министерства обороны Российской Федерации (Краснодар), 2010. С. 78-87.

4 *Лебедев С.С.* Разработка методов и средств комплексной оценки качества систем защиты программного обеспечения. Москва: Издательство: Московский автомобильно-дорожный государственный технический университет (МАДИ) (Москва), 2007. С. 84-89.

5 *Соловьев С.В.* Применение экспертных методов при прогнозировании угроз безопасности информации с использованием баз данных уязвимостей / Соловьев С.В., Мамута В.В. Воронеж. Издательство: Воронежский государственный технический университет (Воронеж), 2014. С. 460-463.

6 *Mlynarczyk M.* Analysis and si promien - comparison of the functionality of the software for the assessment of contamination / Mlynarczyk M., Maciejewski P., Szerszen M. Варшава: Издательство: Centrum Naukowo-Badawcze Ochrony Przeciwpozarowej im. Jozefa Tuliszkowskiego - Panstwowy Instytut Badawczy (Юзефув), 2015. С. 133-138.