ПРОГНОЗИРОВАНИЕ СБОЕВ И ОТКАЗОВ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ УПРАВЛЕНИЯ НА ОСНОВЕ МОДЕЛЕЙ ПРОГНОЗИРОВАНИЯ ВРЕМЕННЫХ РЯДОВ

Андрюхин Е.В.[1], *Ридли М.К.*[2], *Правиков Д.И.*[3]

В статье рассмотрены модели гетерогенных систем АСУ ТП. Проведен анализ подходов к обеспечению информационной безопасности на уровне программируемого логического контроллера. Определено, что для восстановления данных используются моделирование пространственных отношений и представление состояний системы в виде временного ряда. Представление системы в виде временного ряда позволяет учитывать такие характеристики системы, как сезонность, тренд и периодичность. В результате исследования предложена методика, являющаяся функциональным расширением методики обработки данных, предлагаемой ГОСТ Р МЭК 61508-2, и основанная на модели Хольта-Винтерса. Преимуществом предложенной модели является возможность резко реагировать на значительные изменения в структуре ряда, но быстро возвращать дисперсию к обычным значениям. Данное свойство позволяет настроить контролируемую систему даже в условиях сильно зашумленных рядов. Как результат, предложенная методика позволяет выявлять аномалии в системах управления посредством краткосрочных прогнозов для состояний систем, представленных в виде временного ряда.

Ключевые слова: *прогнозирование, распределенные системы управления, промышленный сетевой трафик, аномалии.*

DOI: *10.21681/2311-3456-2019-3-24-32*

Описание проблемы

Информационные системы относятся к ключевым в зависимости от их назначения в соответствии с перечнем критически важных сегментов информационной инфраструктуры (КСИИ). В свою очередь, критически важными сегментами признаются сегменты, нарушение штатного режима функционирования которых может нарушить функции управления чувствительными для Российской Федерации процессами, в том числе и системы управления потенциально опасными объектами, водоснабжением, энергоснабжением и др [1]. Таким образом, к КСИИ относятся автоматизированные системы управления технологическими процессами (АСУ ТП), а также системы промышленного интернета вещей (IIoT), включающие в себя, в том числе, объекты критической информационной инфраструктуры [2].

При проектировании типовой архитектуры систем управления основной функцией является – осуществлять воздействие на управляемый процесс, объект контроля и управления. Для этого необходимо реализовать подачу входного сигнала, его обработку и выдачу. При необходимости может быть реализовано устройство обратной связи, вычислительное устройство, преобразующее значения входов в значения выходов, а также управляющий механизм [3].

Архитектура, представленная в ISA/IEC 62443, является нейтральной точкой для создания гетерогенных систем АСУ ТП. Такая эталонная модель включает пять уровней [4]. Нулевой уровень содержит компоненты, обеспечивающие функционирование процесса: датчики и исполнительные механизмы. Первый уровень осуществляет локальное управление процессом, а также функции защиты и безопасности. На нем функционируют контроллеры, выполняющие функции логического управления технологическим процессом. Второй уровень осуществляет управление и мониторинг физических процессов. На нем находятся средства мониторинга и сбора данных, а именно – система SCADA. Если на предприятии присутствует необходимость управлять распределенными процессами, то часть функций SCADA уходит на третий уровень. Третий уровень позволяет осуществить операционное управление производством, а четвертый – предприятием. Обычно при рассмотрении функциональной безопасности АСУ ТП ограничиваются нулевым, первым и вторым уровнями. Для рассмотрения информационной безопасности необходимо учитывать все представленные уровни, а также их возможности взаимодействия в обход последовательности уровней. Необходимость учёта способом взаимодействия компонентов АСУ ТП также подтверждается указаниями доктрины Industry 4.0, приводящей к гибридизации архитектур Интернета Вещей и АСУ ТП. В итоге получается система, в которой функции мониторинга и сбора данных выполняются при помощи облачных технологий [5]. В ноябре 2018 ENISA выпустило документ «Good Practices for Security of Internet of Things in the context of Smart Manufacturing», в котором собраны практики обеспечения кибербезопасности для IIoT, а также выполнена классификация и описание возможных угроз, применительно к области IIoT [6]:

1 Андрюхин Евгений Владимирович, эксперт-исследователь, ЗАО «Перспективный мониторинг», г. Москва, Россия. E-mail: Andryukhin.Evg@amonitoring.ru

2 Ридли Михаил Кристофорович, инженер, Московский авиационный институт, г. Москва, Россия.

3 Правиков Дмитрий Игоревич, кандидат технических наук, директор НОЦ Новые информационно-аналитические технологии, РГУ нефти и газа (НИУ) имени И.М. Губкина. г. Москва, Россия. E -mail: dip@gubkin.pro

- эксплуатация с нарушением установленных режимов (осознанная и случайная) – манипуляции, производимые с данными и устройствами;
- прослушивание/перехват – сбор информации как в пассивном, так и активном режимах;
- непреднамеренное повреждение – ошибки конфигурирования, администрирования, внедрения;
- остановка работы системы – перебои в работе, связанные с потерей электропитания, либо нарушением коммуникаций;
- катастрофы – разрушительные внешние воздействия природного и техногенного характера;
- физические атаки – вывод из строя оборудования вследствие физического воздействия;
- сбои/отказы работы – происходят по причине случайных сбоев/отказов компонентов, а также из-за проблем в разработке программного обеспечения;
- нарушения, относящиеся к области общего права – отклонения от требований закона и контрактов.

Большинство решений, направленных на обеспечение безопасности компонентов АСУ ТП, ставят своей задачей поддержание необходимого уровня функциональной безопасности. Это связано, в первую очередь, с требованиями обеспечения безопасности жизнедеятельности, связанной с рисками для здоровья и жизни людей, а также окружающей среды [7]. Функциональная безопасность напрямую связана с надежностью аппаратной составляющей, и здесь осталось немного нерешенных задач. Электроника способна безотказно работать годами, а, если этого недостаточно, то всегда есть возможность резервирования. Однако программная составляющая, на которую возлагается управление функции безопасности, остается под угрозой: резервирование не решит проблем обеспечения надежности и безопасности, поскольку программные отказы будут проявляться во всех резервированных каналах.

Ошибки, внесенные на этапе формирования спецификации требований, как и ошибки эксплуатации (некорректную эксплуатацию в терминах ИБ корректно было бы совместить с модификацией существующих систем), составляющие большую часть всех аварий, корректно определять и избегать при помощи функции ИБ. ФБ опирается на опыт теории надежности и проверенные практикой принципы, ИБ многогранна и постоянно развивается, как по части новых методов и типов уязвимостей, так и по части борьбы с ними.

Для управления рисками применяется принцип «защиты в глубину», который заключается в том, что в системе должен применяться набор разнотипных методов защиты. Такой принцип позволяет не предоставить злоумышленнику полный доступ ко всем данным сразу, если взломан хотя бы один из периметров защит. При таком подходе в качестве злоумышленника может выступать заинтересованное лицо, инцидент или авария на исследуемом объекте. Например, если на атомном энергоблоке какой-то из параметров выходит за установленные пределы, то включаются локальные технологические защиты и блокировки. Если это не помогло – осуществляется аварийный останов процесса, а развитие нежелательного процесса отслеживается до его полной ликвидации.

Если спроецировать эти группы требований на область информационной безопасности, то картина получится приблизительно та же. Таким образом, можно предположить, что для обеспечения информационной безопасности и функциональной безопасности достаточно применять одни и те же контрмеры, ведь функциональные ошибки, вызванные недостатками ПО и системной составляющей, приводят к уязвимостям, которые могут быть как использованы злоумышленником, так и стать причиной инцидента.

Одним из потенциальных рисков является перехват управления на уровне физических устройств, при котором злоумышленник может заставить систему выполнять функции, небезопасные для технологического процесса. В этом случае информационная и функциональная безопасность являются двумя сторонами одного явления. Свойство информационной безопасности должно обеспечить целостность, доступность и конфиденциальность данных системы управления. Свойство функциональной безопасности должно обеспечить корректное выполнение функций системы управления по переводу объекта управления в безопасное состояние.

Тем не менее, в области Интернета Вещей нет упоминаний о функциональной безопасности. Для Интернета Вещей именно от реализации функций безопасности зависит возможность получения доступа к данным (функция ИБ), либо к управляющим функциям физических устройств (функция ФБ). Поэтому ФБ не рассматривается как отдельное свойство, а рассматриваются только различные типы угроз и атак.

Анализ систем управления

Программируемый логический контроллер (ПЛК) это тип цифрового компьютера, целью которого является обеспечение автоматизации процесса. Логические контроллеры быстро работают в режиме реального времени, мгновенно реагируя на инструкции, отправляемые другими участниками процесса [8]. Принципиально важно помнить, что программа ПЛК выполняется не постоянно, а циклически, каждые несколько миллисекунд. Другое важное обстоятельство – время цикла ПЛК и время работы внешних устройств изначально никак не связаны. Например, к моменту, когда на СКАДА-сервере будет получена информация о температуре, ПЛК совершит десятки, а то и сотни циклов.

Внутри такого типа контроллера находится центральный процессор, который выполняет инструкции по управлению, найденные в программах пользователя, и инструкции самодиагностики, а также взаимодействует с другими устройствами в сети. ПЛК функционирует в постоянном цикле, выполняя следующие шаги: опрашивает входы, выполняет программный цикл, записывает выходы.

Память внутри контроллера не бесконечная и имеет свои размеры. У ПЛК память ввода-вывода определяет максимальное количество внешних модулей ввода-вывода (например, 4 мегабайта для памяти программы, 300 килобайт для памяти ввода-вывода, 1 мегабайт памяти переменных), а задачу сохранения значений программы между выключениями питания контроллера берет на себя функционал retain-переменных [9]. Контроллеры программируются при помощи различных языков и средств разработки, однако, любая программа, исполняемая на ПЛК, может быть представима в виде цифровой схемы с использованием логических элементов, используемых в цифровой логике [10].

Проблемы, связанные с ошибками в системах коммуникации между сенсорами, центрами обработки и хранения данных, а также системой контроля, часто приводят к возникновению типовых сетевых ошибок, таких как пропуск пакета или получение некорректных данных. Данные, полученные сенсором, могут быть как некорректными изначально, вследствие физического дефекта сенсора, например, по причине деградации состояния оборудования, так и претерпеть изменения во время передачи по каналам связи. В промышленных сетях для таких случаев используется специальное архитектурное решение – дуальная конфигурация. Такая конфигурация позволяет нескольким каналам независимо выполнять одну и ту же функцию, фактически, выполняя функцию резервирования. Наиболее частыми решениями по резервированию являются дублирование (резервирование на нагруженный резерв с кратностью 1 к 2) и троирование (резервирование на нагруженный резерв с кратностью 1 к 3). Недостатком является то, что наличие дуальных конфигураций в сетях существенно повышает избыточность и не позволяет добиваться устойчивости к систематическим отказам и отказам по общей причине. ГОСТ Р МЭК 61508-4 предлагает использовать различные физические методы и подходы к проектированию для повышения устойчивости к отказам, систематическим ошибкам и ошибкам с общей причиной, выделяя отдельный признак системы, называемый разнообразием (также встречается как «диверсификация»). На практике подобное разнообразие средств достижения необходимого уровня безопасности либо невозможно к выполнению, либо требует высоких финансовых затрат [11-13]. Также, в рамках ГОСТ Р МЭК 61508-4 указано, что отказоустойчивость аппаратных средств N означает, что отказ N+1 может привести к потере функции безопасности[4]. Иными словами, если некоторый компонент подсистемы непосредственно приводит к одному или более последующих отказов, то вся подсистема рассматривается как один отказ. При этом ГОСТ Р МЭК 61508-6 указывает не учитывать средства, которые могли бы управлять влиянием ошибок. ГОСТ Р МЭК 61508-2 предлагает использовать «ad-hoc» решения, основанные на бинарной логике работы исключительно выбранного набора инструментов[5]. Такая модель предлагает проводить диагностическое тестирование с целью обнаружения отказов, либо несоответствия результатов и переводить выходной сигнал в безопасное состояние в соответствии с выбранным решением по резервированию, причем для обнаружения несоответствия между каналами каждый сигнал может определять состояние другого канала независящим от другого канала способом. В качестве такого способа могут быть рассмотрены типовые методы анализа потоков данных: на основе передаваемых сигналов и на основе модели поведения системы.

Метод анализа потоков данных на основе передаваемых сигналов является низкоуровневым и требует применения эвристических методов на основе статистических данных, полученных с конкретного сенсора [14-16]. Обычно, эти методы основаны на проверке либо значения сигналов, либо оценке отклонения характеристик сигнала от ожидаемых. С одной стороны, задача проверки сигнала по значениям может быть сведена к задаче проверки выхода номинала значения за верхний и нижний порог: в случае, если значение не попадает в множество допустимых – сигнал некорректен. С другой стороны, методы, основанные на оценке изменений характеристик сигнала, могут определять некорректный сигнал без привязки к точным характеристикам, исключительно на основе поведения полученной кривой: по сильным отклонениям (скачки на графике), либо отсутствии отклонений (спрямление).

Методы анализа, основанные на построении модели поведения системы, позволяют вычислить разницу между предсказанным значением, полученным вследствие анализа работы системы, и реальным значением, полученным в течение работы системы. Разница между предсказанным и фактическим значениями сравнивается с некоторым значением, выбранным как пороговое. В случае, если разница превышает пороговое значение – предполагается, что на сенсоре произошла ошибка, иначе – система работает корректно [17]. Также, для методов на основе модели поведения системы могут быть добавлены процедуры, позволяющие оценить значения временной и пространственной избыточности.

Методика обработки данных сенсора, предложенная ниже, является функциональным расширением методики, предлагаемой ГОСТ Р МЭК 61508-2. Задачей предлагаемого метода является валидация и восстановление данных на основе результатов обработки промежуточных результатов (метаданных):

- среднее время получения метаданных в течение сессии между двумя объектами сети;
- среднее значение изменения метаданных (длина пакетов, длина сессии);
- изменение значения относительно ожидаемых метаданных (прогнозные значения);
- изменение значения относительно соседних компонентов, с которыми сенсор осуществляет взаимодействие (если осуществляет), либо находится в дуальной конфигурации.

Для восстановления данных используются следующие типы моделирования: моделирование пространственных отношений и представление состояний системы в виде временного ряда. Представление системы в виде временного ряда позволяет учитывать такие характеристики системы, как сезонность, тренд и периодичность. Учитывая то, что целью производства является механическое повторение действий, направленное на выполнение небольшой поставленной задачи, данные с сенсора также должны быть упорядочены по циклу, или близкими к

4 ГОСТ Р МЭК 61508-4-2012 URL: http://docs.cntd.ru/document/1200102418
5 ГОСТ Р МЭК 61508-2-2012 URL: http://docs.cntd.ru/document/1200100344

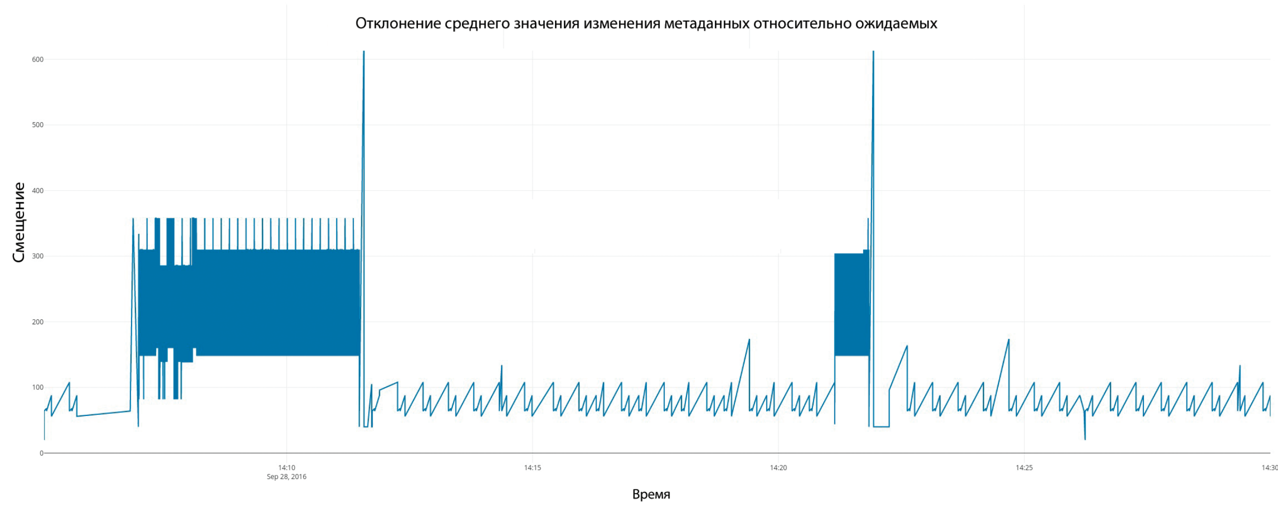

Рис. 1 График зависимости среднего значения изменения метаданных относительно ожидаемых метаданных

повторяющимся. В случае моделирования на основе построения пространственных отношений, создается матрица пространственных весов для описывания соотношений, которые существуют между объектами в наборе. Для решения задачи валидации данных может быть использована модель ARIMA (модель пространственных отношений на основе метода наименьших квадратов), а для решения задачи восстановления данных может быть использована модель Хольта-Винтерса (моделирование в виде временного ряда) [18].

Применение методики

Модель Хольта-Винтерса принадлежит к классу методов экспоненциального сглаживания и позволяет делать краткосрочные прогнозы для предоставленного временного ряда [19]. В отличие от сглаживания, модель Хольта-Винтерса выявляет тренды и экстраполирует их на дальнейшие данные, что, в силу характеристик промышленного трафика, может существенно уточнить прогнозные данные [20]. В основе метода находится гипотеза о том, что исследуемый временной ряд может быть представлен как сумма основного значения и двух значений: тренда и коэффициента сезонности, причем, коэффициент сезонности скоррелирован на период сезона (1):

$$y_{(t+1)}=a_t+b_t+c_{(t+1-m)}, \qquad (1)$$

где a_t – основное значение, b_t – значение тренда, $c_{(t+1-m)}$ – значение сезонности, m – период сезона, t – момент времени.

Поскольку новое значение является скорректированным на сезонный коэффициент текущим значением и зависит от изменения линии тренда, прогноз тренда прибавляется к основному значению (2):

$$a_t=\alpha(y_t-c_{(t-m)})+(1-\alpha)(a_{(t-1)}+b_{(t-1)}) \qquad (2)$$

Оценка тренда равна разности между текущим и предыдущим значением базового значения (3):

$$b_t=\beta(a_t-a_{(t-1)})+(1-\beta)b_{(t-1)} \qquad (3)$$

Оценка сезонности равна разности между текущим значением и предшествующей базовой компонентой, соответствующей сезонности с учетом цикла (4):

$$c_t=\gamma(y_t-a_t)+(1-\gamma)c_{(t-m)} \qquad (4)$$

В первых точках ряда расчет прогноза не осуществляется, так как не существует достаточного количества предшествующих экспериментальных значений. Базовое значение считается равным наблюдаемому значению, а тренд считается линейным и рассчитывается как разность текущего и прошлого базового значения.

Для вычисления точки ряда, начиная с которой целесообразно начинать расчёт предсказаний, достаточно использовать критерий «минимизация квадратов отклонений расчётных значений от фактических». Начиная с полученной точки базовое значение рассчитывается с учетом тренда и сезона по формулам выше. Поскольку для расчета изменения величины строится прогноз ее значения на истории предыдущих измерений и последнего значения, количество значений может быть выбрано так, чтобы достигать необходимого уровня выявления аномалий.

Для проверки гипотезы применимости модели Хольта-Винтерса был рассмотрен промышленный трафик, полученный из внутренней сети нефтеперерабатывающего завода. ПЛК, трафик с которого был собран, выполняет задачу нагрева сырья для последующего разделения его на фракции. На образце трафика, помимо нескольких полных циклов корректной работы, запечатлен момент атаки, направленной на изменение значения переменной на ПЛК с целью перевода процесса на следующий этап. Для анализа предоставленного образца будут последовательно применены методы, которые позволят реализовать модель Хольта-Винтерса. На рис.1 предоставлен график зависимости среднего значения изменения метаданных относительно ожидаемых метаданных от времени в момент, когда была проведена атака (~14:21):

На графике просматривается циклическая структура, присущая промышленным сетям. Также легко заметить, что данные сильно зашумлены. Отдельно рассмотрим момент атаки, поскольку именно для него будет осуществляться прогнозирование (рис.2):

9 National Cyber Strategy of the United States, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

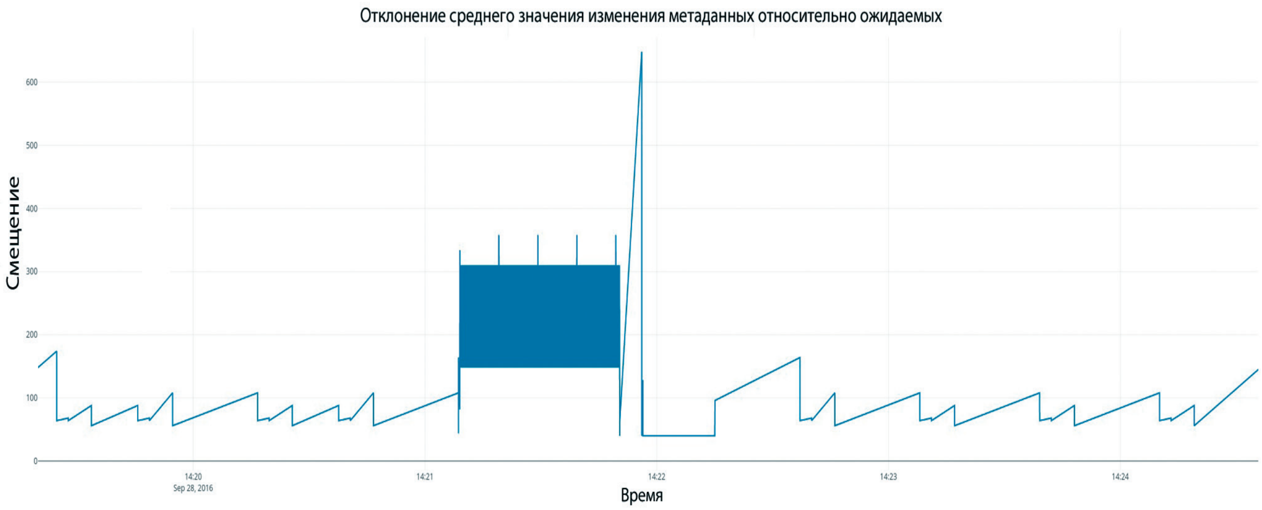

Рис.2 График зависимости среднего значения изменения метаданных относительно ожидаемых метаданных в момент атаки

Добавим прогнозирование на основе скользящей средней: предположим, что будущее значение системы зависит от среднего её предыдущих значений. Несмотря на то, что такой прогноз долгосрочным сделать не получится, однако, с учетом сильной зашумленности данных, сглаживание исходного ряда может помочь более явно увидеть закономерности. На графике ниже предоставлен результат прогноза с учетом доверительного интервала при сглаживании по секундам (рис.3) и минутам (рис.4):

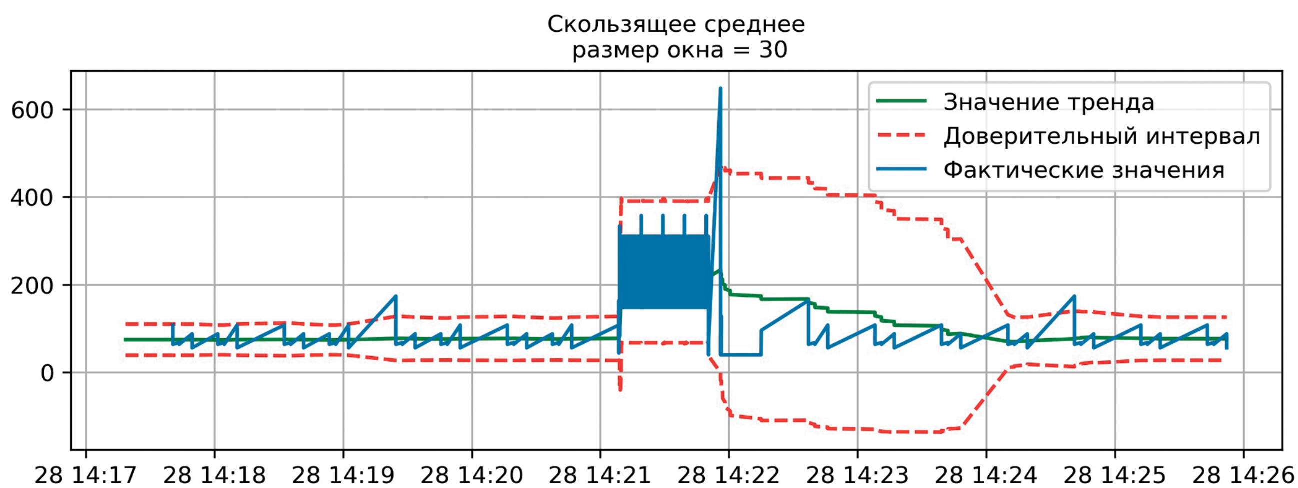

Рис. 3 Скользящее среднее со сглаживанием по секундам

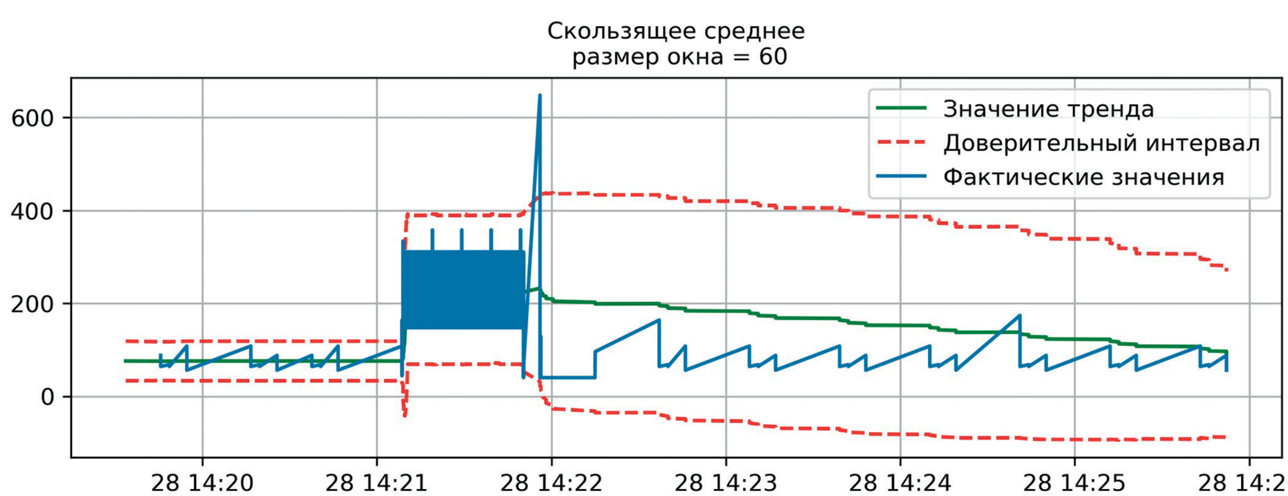

Рис. 4 Скользящее среднее со сглаживанием по минутам

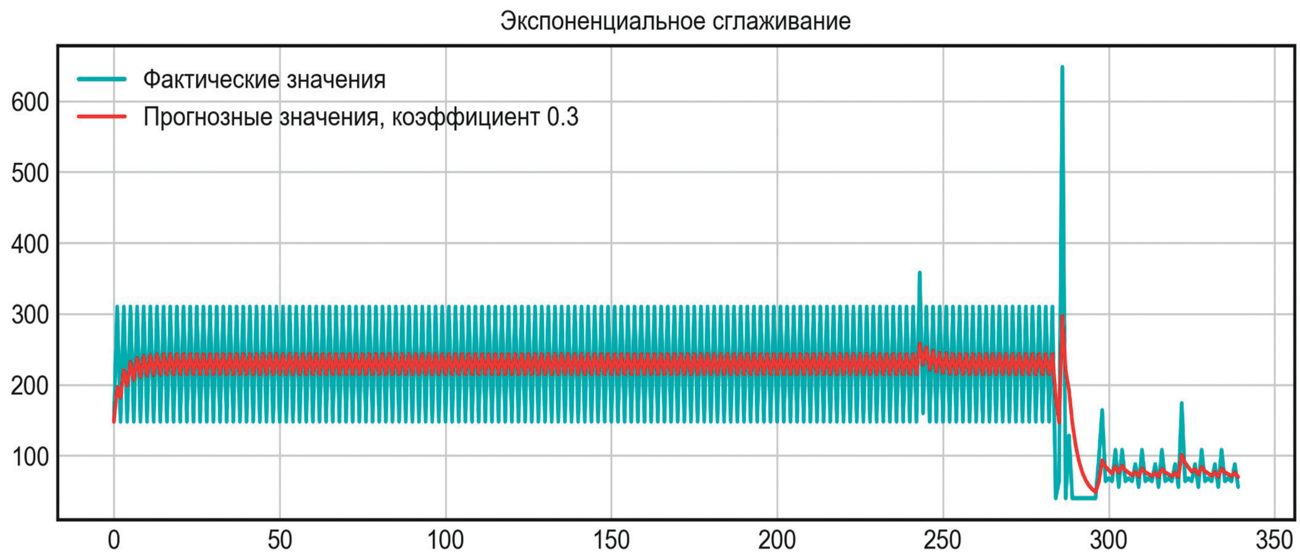

Рис. 5 Простое экспоненциальное сглаживание

Осуществим прогнозирование на основе экспоненциального сглаживания: вместо взвешивания последних значений ряда, будем взвешивать все наблюдения, при этом экспоненциально уменьшая веса по мере углубления в исторические данные. В качестве прогнозируемого значения $\hat{y}_t$ будет рассматриваться средневзвешенная между текущим истинным y_t и предыдущим прогнозируемым значением $\widehat{y_{t-1}}$. Для учета значимости последних истинных значений необходимо использовать сглаживающий фактор α. Чем меньше значение α, тем сильнее сглаживается ряд. Таким образом, формула для вычисления экспоненциального среднего выглядит следующим образом (5):

$$\hat{y}_t = \alpha * y_t + (1 - \alpha) * \widehat{y_{t-1}} \quad (5)$$

На рис.5 видно, что прогнозное значение повторяет фактические значения, однако, в данный момент прогноз может быть только на одну точку вперед. Для получения возможности точного прогноза следующей точки с сохранением сглаживания ряда необходимо разбить ряд на две составляющие – уровень и тренд и представлять систему в качестве набора функций. Под уровнем понимается среднее значение временного ряда. Тренд — это изменение временного ряда от одного периода к другому. Определим тренд, наложим линию тренда на базовый уровень. С учетом сезонной составляющей можно получить модель прогнозирования. Для выполнения задачи учета веса при сглаживании вводится сглаживающий коэффициент β. Дополнив формулу экспоненциального сглаживания, получим формулу (6) для вычисления двойного экспоненциального сглаживания (рис.6):

$$l_x = \alpha y_x + (1 - \alpha)(l_{x-1} + b_{x-1})$$

$$b_x = \beta(l_x - l_{x-1}) + (1 - \beta)b_{x-1}$$

$$\widehat{y_{x+1}} = l_x + b_x \quad (6)$$

Также, как указывалось ранее, необходимо добавить учет сезонности. Термин «сезон» используется для обозначения периода времени до того, как поведение начнет повторяться. Сезонная компонента будет объяснять

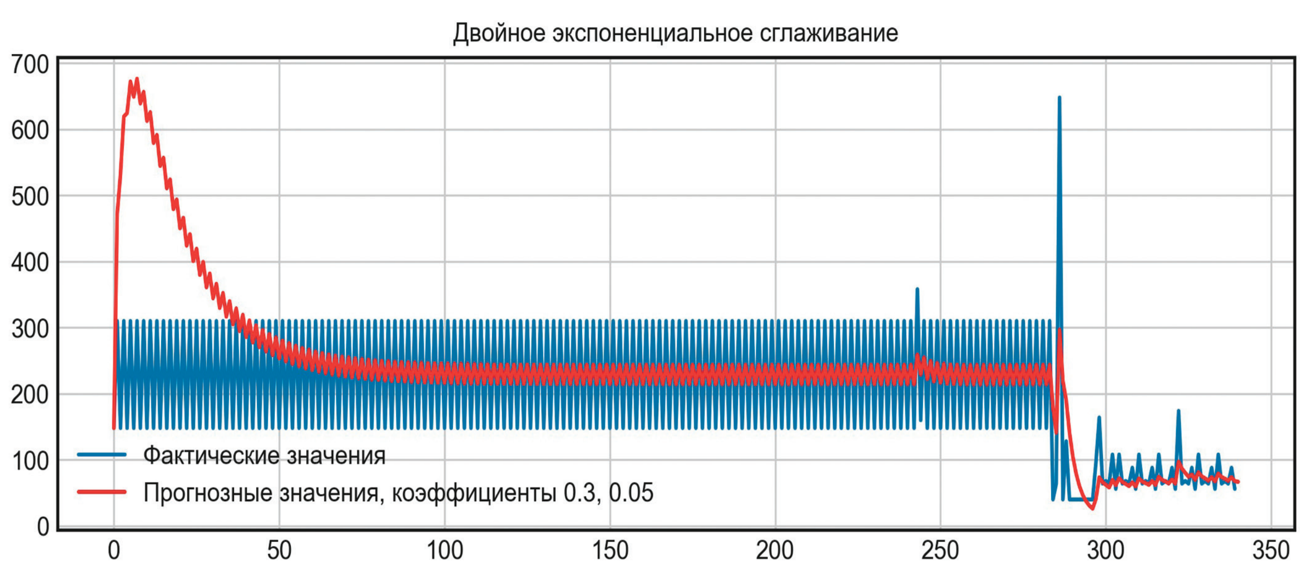

Рис.6 Двойное экспоненциальное сглаживание

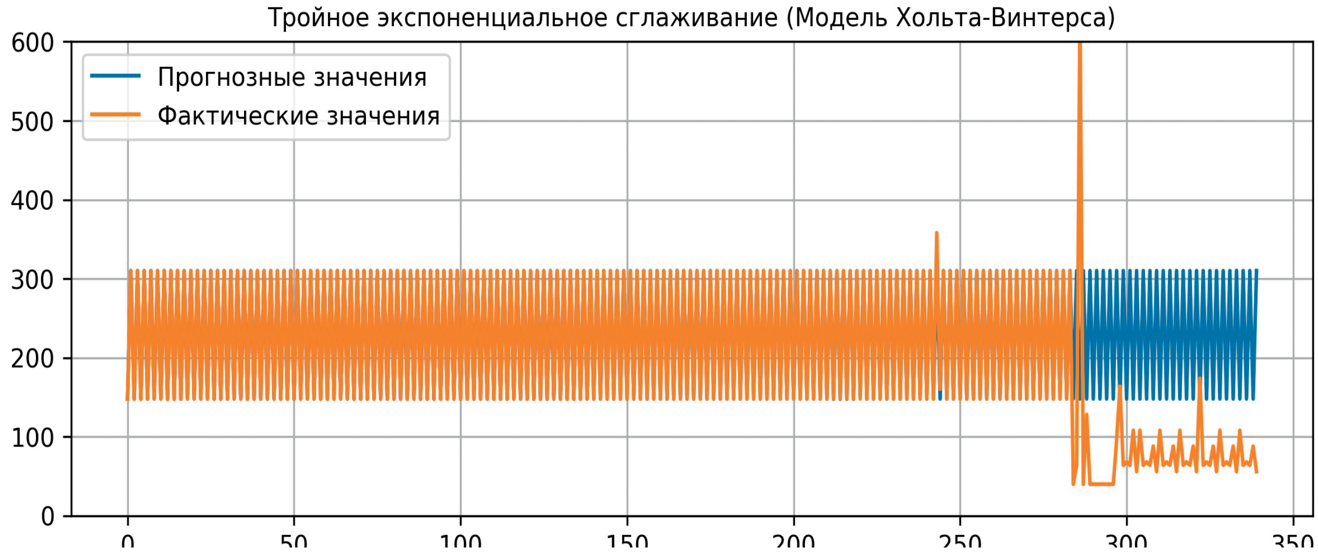

Рис. 7 Прогноз процесса на основе модели Хольта-Винтерса

колебания вокруг уровня и тренда, а характеризоваться длиной сезона – периодом.

На рис.7 видно, что модель описывала временной ряд до тех пор, пока не была проведена атака, что привело к аномальным снижениям, вышедшим за пределы доверительных интервалов (рис.8).

Заключение

Преимуществом такой модели также является возможность резко реагировать на значительные изменения в структуре ряда, но быстро возвращать дисперсию к обычным значениям. Такое свойство позволит настроить систему даже в условиях сильно зашумленных рядов.

Недостатком модели является необходимость в ряде данных, состоящем как минимум из трех периодов: по первому периоду рассчитываются сезонные коэффициенты, по второму – строится сама модель, по третьему – подбираются оптимальные коэффициенты сглаживания для сезонной компоненты. Для модели были получены расчеты ошибки первого и второго рода: 6.75% и 2.23% соответственно. Было замечено, что сбои чаще приводят к последовательностям срабатываний, в отличие от случаев, вызывающих ошибки первого рода, большая часть из которых содержат единичные срабатывания. Эта особенность будет исследована и учтена в дальнейшем.

Рис. 8 Аномалии, выявленные в момент атаки при прогнозировании на основе модели Хольта-Винтерса

Литература

1. Костогрызов А.И. Эффективное управление рисками для критически и стратегически важных объектов РФ // ИТ-Стандарт. 2015. № 2 (3). С. 1-8.
2. Ванцева И.О., Зырянова Т.Ю., Медведева О.О. Влияние Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» на владельцев критических информационных структур // Вестник УрФО. Безопасность в информационной сфере. 2018. № 1 (27). С. 71-76.

3. Старостин А.А., Лаптева А.В. Технические средства автоматизации и управления. Екатеринбург: Изд-во Урал. ун-та, 2015. – 168 с.
4. Phinney T. IEC 62443: Industrial network and system security [Электронный ресурс] // Honeywell, 2018. URI: https://www.isa.org/pdfs/autowest/phinneydone/ (дата обращения к ресурсу: 17.12.2018)
5. Anam Sajid, Haider Abbas, Kashif Saleem. Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges [Электронный ресурс] // IEEE Xplore, 31 марта 2016. URI: https://ieeexplore.ieee.org/document/7445139 (дата обращения к ресурсу: 17.12.2018)
6. Enisa. Good Practices for Security of Internet of Things in the context of Smart Manufacturing. [Электронный ресурс] // Enisa, ноябрь 2018. URI: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot?fbclid=IwAR1q-chv88kZRsIESHtGTEwbA0Mbx8mb9hV1Euqy-Y–IHVYvLuFhGuvi6o (дата обращения к ресурсу: 17.12.2018)
7. Leveson N. G. Engineering a Safer World. [Электронный ресурс] // Massachusetts Institute of Technology, 2009. URI: http://sunnyday.mit.edu/safer-world.pdf (дата обращения к ресурсу: 17.12.2018)
8. Курнасов Е.В., Разумовский Ю.А. Программируемые контроллеры систем автоматизации и управления. Часть 1. Москва, 2014. 95 с.
9. Егоров А.А. Промышленные контроллеры: прошлое, настоящее и будущее. Программируемые логические контроллеры: история создания // Автоматизация и IT в энергетике. 2018. № 6 (107). С. 36-50.
10. Альтерман И.З., Шалыто А.А. Формальные методы программирования логических контроллеров // “Промышленные АСУ и контроллеры”, 2005, №11, с. 49– 52.
11. Гетьман А.И., Маркин Ю.В., Обыденков Д.О., Падарян В.А., Тихонов А.Ю. Подходы к представлению результатов анализа сетевого трафика. Труды ИСП РАН, том 28, вып. 6, 2016, стр. 103-110. DOI: 10.15514/ISPRAS-2016-28(6)-7
12. Гетьман А., Маркин Ю., Обыденков Д., Падарян В. Архитектура системы глубокого разбора сетевого трафика // Системный администратор. 2018. № 1-2 (182-183). С. 83-87.
13. Гетьман А.И., Маркин Ю.В., Евстропов Е.Ф., Обыденков Д.О. Обзор задач и методов их решения в области классификации сетевого трафика // Труды Института системного программирования РАН, 2017. Вып.29 (3), С.117-150. https://doi.org/10.15514/ISPRAS-2017-29(3)-8
14. Маркин Ю.В. Методы и средства углубленного анализа сетевого трафика // автореферат дис. кандидата технических наук / Ин-т систем. программирования. Москва, 2017
15. Машечкин И.В., Петровский М.И., Царёв Д.В. Методы машинного обучения для анализа поведения пользователей при работе с текстовыми данными в задачах информационной безопасности // Вестник Московского университета. Серия 15: Вычислительная математика и кибернетика. 2016. № 4. С. 33-39.
16. Mashechkin I.V., Petrovskiy M.I., Popov D.S., Tsarev D.V. Applying text mining for data loss prevention // Programming and Computer Software. 2015. Т. 41. № 1. С. 23-30.
17. Лукашин Ю.П. Адаптивные методы краткосрочного прогнозирования временных рядов [Электронный ресурс] // Финансы и статистика, 2003. URI: https://biznesbooks.com/components/com_jshopping/files/demo_products/lukashin-yu-p-adaptivnye-metody-prognozirovaniya.pdf (дата обращения к ресурсу: 17.12.2018)
18. Селиверстова А.В. Сравнительный анализ моделей и методов прогнозирования // Современные научные исследования и инновации. 2016. № 11 (67). С. 241-248.
19. Тарджуманян А.А. Прогнозирование по методам тройного экспоненциального сглаживания Хольта-Винтерса // Молодежный научно-технический вестник. 2015. № 4. С. 50.
20. Поздняков А.С. Применение метода Хольта-Винтерса при анализе и прогнозировании динамики временных рядов // Проблемы организации и управления на транспорте Сборник научных трудов студентов, магистрантов, аспирантов, молодых ученых и их научных руководителей (материалы межвузовской научно-практической конференции). 2017. С. 57-64.

PREDICTION OF FAULTS AND FAILURES IN DISTRIBUTED CONTROL SYSTEMS BASED ON TIME SERIES FORECASTING MODELS

Andryukhin E.V.[6], Ridli M.A.[7], Pravikov D.I.[8]

The article considers models of heterogeneous systems of automated process and production control systems. Approaches to providing information security at the programmable logic controller level are analyzed. It is determined that spatial relationship modeling and representation of system states as a time series are used for data recovery. Representation of a system as a time series helps take account of the system’s characteristics, such as seasonality, trend and frequency. A procedure is proposed based on the study findings, which is a functional extension of the data processing procedure proposed by the national standard GOST R IEC 61508-2 and uses the Holt-Winters model. The proposed model’s advantage is the ability to respond sharply to significant changes in the series structure and quickly return the variance to normal values. This property allows the controlled system to be set up even in highly noisy series. As a result, the proposed procedure makes it possible to identify anomalies in control systems by means of short-term forecasts for the states of systems represented as a time series.

6 Evgeny Andryukhin, expert-researcher, “Advanced monitoring”, Moscow, Andryukhin.Evg@amonitoring.ru
7 Mihail Ridli, engineer, Moscow aviation institute, Moscow
8 Dmitry Pravikov, Ph.D., Director of the REC of new information and analytical technologies, Gubkin Russian State University of Oil and Gas (NRU), Moscow, dip@gubkin.pro

Keywords: *forecasting, distributed control systems, industrial network traffic, anomalies.*

References

1. Kostogryzov A.I. EHffektivnoe upravlenie riskami dlya kriticheski i strategicheski vazhnyh ob»ektov RF // IT-Standart. 2015. № 2 (3). S. 1-8.
2. Vanceva I.O., Zyryanova T.YU., Medvedeva O.O. Vliyanie Federal'nogo zakona «O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii» na vladel'cev kriticheskih informacionnyh struktur // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2018. № 1 (27). S. 71-76.
3. Starostin A.A., Lapteva A.V. Tekhnicheskie sredstva avtomatizacii i upravleniya. Ekaterinburg: Izd-vo Ural. un-ta, 2015. – 168 s.
4. Phinney T. IEC 62443: Industrial network and system security [EHlektronnyj resurs] // Honeywell, 2018. URl: https://www.isa.org/pdfs/autowest/phinneydone/ (data obrashcheniya k resursu: 17.12.2018)
5. Anam Sajid, Haider Abbas, Kashif Saleem. Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges [EHlektronnyj resurs] // IEEE Xplore, 31 marta 2016. URl: https://ieeexplore.ieee.org/document/7445139 (data obrashcheniya k resursu: 17.12.2018)
6. Enisa. Good Practices for Security of Internet of Things in the context of Smart Manufacturing. [EHlektronnyj resurs] // Enisa, noyabr' 2018. URl: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot?fbclid=IwAR1q-chv88kZRsIESHtGTEwbA0Mbx8mb9hV1Euqy-Y--IHVYvLuFhGuvi6o (data obrashcheniya k resursu: 17.12.2018)
7. Leveson N. G. Engineering a Safer World. [EHlektronnyj resurs] // Massachusetts Institute of Technology, 2009. URl: http://sunnyday.mit.edu/safer-world.pdf (data obrashcheniya k resursu: 17.12.2018)
8. Kurnasov E.V., Razumovskij YU.A. Programmiruemye kontrollery sistem avtomatizacii i upravleniya. CHast' 1. Moskva, 2014. 95 s.
9. Egorov A.A. Promyshlennye kontrollery: proshloe, nastoyashchee i budushchee. Programmiruemye logicheskie kontrollery: istoriya sozdaniya // Avtomatizaciya i IT v ehnergetike. 2018. № 6 (107). S. 36-50.
10. Al'terman I.Z., SHalyto A.A. Formal'nye metody programmirovaniya logicheskih kontrollerov // "Promyshlennye ASU i kontrollery", 2005, №11, s. 49– 52.
11. Get'man A.I., Markin YU.V., Obydenkov D.O., Padaryan V.A., Tihonov A.YU. Podhody k predstavleniyu rezul'tatov analiza setevogo trafika. Trudy ISP RAN, tom 28, vyp. 6, 2016, str. 103-110. DOI: 10.15514/ISPRAS-2016-28(6)-7
12. Get'man A., Markin YU., Obydenkov D., Padaryan V. Arhitektura sistemy glubokogo razbora setevogo trafika // Sistemnyj administrator. 2018. № 1-2 (182-183). S. 83-87.
13. Get'man A.I., Markin YU.V., Evstropov E.F., Obydenkov D.O. Obzor zadach i metodov ih resheniya v oblasti klassifikacii setevogo trafika // Trudy Instituta sistemnogo programmirovaniya RAN, 2017. Vyp.29 (3), S.117-150. https://doi.org/10.15514/ISPRAS-2017-29(3)-8
14. Markin YU.V. Metody i sredstva uglublennogo analiza setevogo trafika // avtoreferat dis. kandidata tekhnicheskih nauk / In-t sistem. programmirovaniya. Moskva, 2017
15. Mashechkin I.V., Petrovskij M.I., Caryov D.V. Metody mashinnogo obucheniya dlya analiza povedeniya pol'zovatelej pri rabote s tekstovymi dannymi v zadachah informacionnoj bezopasnosti // Vestnik Moskovskogo universiteta. Seriya 15: Vychislitel'naya matematika i kibernetika. 2016. № 4. S. 33-39.
16. Mashechkin I.V., Petrovskiy M.I., Popov D.S., Tsarev D.V. Applying text mining for data loss prevention // Programming and Computer Software. 2015. T. 41. № 1. S. 23-30.
17. Lukashin YU.P. Adaptivnye metody kratkosrochnogo prognozirovaniya vremennyh ryadov [EHlektronnyj resurs] // Finansy i statistika, 2003. URl: https://biznesbooks.com/components/com_jshopping/files/demo_products/lukashin-yu-p-adaptivnye-metody-prognozirovaniya.pdf (data obrashcheniya k resursu: 17.12.2018)
18. Seliverstova A.V. Sravnitel'nyj analiz modelej i metodov prognozirovaniya // Sovremennye nauchnye issledovaniya i innovacii. 2016. № 11 (67). S. 241-248.
19. Tardzhumanyan A.A. Prognozirovanie po metodam trojnogo ehksponencial'nogo sglazhivaniya Hol'ta-Vintersa // Molodezhnyj nauchno-tekhnicheskij vestnik. 2015. № 4. S. 50.
20. Pozdnyakov A.S. Primenenie metoda Hol'ta-Vintersa pri analize i prognozirovanii dinamiki vremennyh ryadov // Problemy organizacii i upravleniya na transporte Sbornik nauchnyh trudov studentov, magistrantov, aspirantov, molodyh uchenyh i ih nauchnyh rukovoditelej (materialy mezhvuzovskoj nauchno-prakticheskoj konferencii). 2017. S. 57-64.