УДК 004.896 + 004.056.5 Вестник УрФО № 2(40) / 2021, с. 44–58

Рагозин А. Н.

DOI: 10.14529/secur210205

ФОРМИРОВАНИЕ ПРОГНОЗА МНОГОКОМПОНЕНТНЫХ ВРЕМЕННЫХ РЯДОВ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ЦИФРОВОЙ ФИЛЬТРАЦИИ И ПРОГНОЗИРУЮЩЕГО АВТОКОДИРОВЩИКА С ЦЕЛЬЮ ОБНАРУЖЕНИЯ АНОМАЛИЙ В РАБОТЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ КИБЕРАТАК

Эффективность современных сложных автоматизированных систем управления технологическими процессами (АСУ ТП) складывается из показателей качества формирования в подобных системах управленческих решений и воздействий, а также способности сохранения устойчивого функционирования в условиях сильной неопределенности изменяющейся внешней среды, например, в следствии воздействия кибератак, как на информационном уровне, так и на кибернетическом уровне в АСУ ТП. Динамические временные ряды данных, отражающие процессы, протекающие в современных сложных АСУ ТП представляют результат взаимодействия многих подсистем и поэтому являются сложными многокомпонентными временными рядами. С целью обнаружения аномалий и повышения качества прогнозирования динамических многокомпонентных временных рядов данных, наблюдаемых с сенсоров в АСУ ТП, предлагается формировать прогноз в различных временных масштабах (краткосрочный, среднесрочный, долго-

срочный) развивающейся ситуации в АСУ ТП. При возникновении аномалий в работе АСУ ТП будут происходить структурные изменения в сигнале ошибки формируемого прогноза, в результате анализа этих структурных изменений ошибки прогноза, собственно происходит детектирование (обнаружение) аномалий в наблюдаемых процессах АСУ ТП. Структурный анализ многокомпонентного временного ряда и соответственно формирование архитектуры искусственной нейронной сети позволяют формировать прогноз в различных временных масштабах. Предлагаемый подход формирования прогноза в различных временных масштабах, позволит обнаруживать в множестве наблюдаемых временных рядов данных АСУ ТП аномалии раздельно по их различным динамическим характеристикам, что повышает эффективность управления устойчивостью функционирования АСУ ТП в условиях воздействия кибератак.

Ключевые слова: *цифровая фильтрация, искусственная нейронная сеть, многокомпонентный прогноз, прогнозирующий автоэнкодер, автоматизированная система управления технологическими процессами, кибератаки.*

Ragozin A. N.

FORMATION OF A FORECAST OF MULTICOMPONENT TIME SERIES OF DATA USING DIGITAL FILTERING METHODS AND A PREDICTIVE AUTOENCODER IN ORDER TO DETECT ANOMALIES IN THE OPERATION OF AUTOMATED CONTROL SYSTEMS FOR TECHNOLOGICAL PROCESSES UNDER THE INFLUENCE OF CYBERATTACKS

The effectiveness of modern complex automated process control systems (APCS) consists of the quality indicators of the formation in such systems of managerial decisions and influences,

as well as the ability to maintain stable functioning in conditions of strong uncertainty in a changing external environment, for example, because of the impact of cyberattacks, as at the information level and at the cybernetic level in the APCS. Dynamic time series of data reflecting the processes occurring in modern complex APCS represent the result of the interaction of many subsystems and therefore are complex multicomponent time series. In order to detect anomalies and improve the quality of forecasting dynamic multicomponent time series of data observed from sensors in the APCS, it is proposed to form a forecast at various time scales (short-term, medium-term, long-term) of the developing situation in the APCS. In the event of anomalies in the operation of the automated process control system, structural changes will occur in the error signal of the generated forecast; as a result of the analysis of these structural changes in the forecast error, in fact, anomalies are detected in the observed processes of the APCS. Structural analysis of a multicomponent time series and, accordingly, the formation of the architecture of artificial neural networks make it possible to form a forecast at different time scales. The proposed approach to the formation of a forecast in different time scales will allow detecting anomalies in the set of observed time series of APCS data separately according to their different dynamic characteristics, which increases the efficiency of managing the stability of the functioning of the APCS under cyberattacks.

Keywords: *digital filtering, artificial neural network, multicomponent forecast, predictive autoencoder, automated process control system, cyberattacks.*

Введение

Эффективность управления информационной безопасностью в современных сложных автоматизированных системах управления технологическими процессами (АСУ ТП) складывается из показателей качества формирования в подобных системах управленческих решений и воздействий, а также способности сохранения устойчивого функционирования в условиях сильной неопределённости изменяющейся внешней среды, например, в следствии воздействия кибератак, как на информационном уровне, так и на кибернетическом уровне в АСУ ТП. Воздействие кибератак проявляется в виде аномалий (неожидаемого изменения свойств) динамических рядов данных, отражающих работу АСУ ТП. Важной является задача оперативного обнаружения аномалий в работе АСУ ТП в условиях воздействия кибератак.

Современные АСУ ТП состоят из многих подсистем, поэтому процессы, протекающие в них и отражаемые в наблюдаемых потоках данных, являются сложными многокомпонентными процессами. Потоки данных в таких сложных автоматизированных системах можно упорядочить во временные ряды данных и, соответственно осуществлять прогноз сложных многокомпонентных временных рядов данных в различных временных масштабах (краткосрочный, среднесрочный, долгосрочный). Для реализации прогноза в различных временных масштабах необходим структурный анализ многокомпонентного временного ряда и соответственно, формирование масштабируемого прогноза [1, 2].

Атаки вызывают аномалии (то есть, неожидаемое изменение) в поведении наблюдаемых процессов (в динамике наблюдаемых временных рядов данных) при работе АСУ ТП. Технология прогнозирования играет важную роль при построении систем обнаружении (детектирования) аномалий в динамических потоках данных АСУ ТП [3-5]. Предлагаемый подход формирования прогноза в различных временных масштабах, позволит обнаруживать в множестве наблюдаемых временных рядов данных АСУ ТП аномалии раздельно по их различным динамическим характеристикам, что повышает эффективность управления устойчивостью функционирования АСУ ТП в условиях сильной неопределённости изменяющейся внешней среды, а также, в следствии воздействия кибератак на АСУ ТП.

Методы прогнозирования динамических рядов данных, рассмотрены в работах [6-10].

Методы обнаружения аномалий с использованием искусственных нейронных сетей (ИНС) рассмотрены в работах [11-19].

Из анализа российских и зарубежных источников следует, что задача формирования масштабируемого прогноза на различных временных интервалах по наблюдаемым сложным многокомпонентным временным рядам в настоящее время не имеет завершенного решения. В настоящей работе рассматриваются этапы и результат построения про-

гноза многокомпонентных временных рядов, наблюдаемых в АСУ ТП.

1. Этапы построения прогноза многокомпонентного динамического временного ряда АСУ ТП

Динамические потоки данных, наблюдаемые в АСУ ТП представляют собой многокомпонентные временные ряды данных.

Для построения многокомпонентного (масштабируемого) прогноза в различных временных масштабах необходима реализация первого этапа – применение технологии цифровой обработки сигналов (ЦОС) для разложения сложного многокомпонентного временного ряда на отдельные базовые компоненты (структурный анализ многокомпонентного временного ряда, для наблюдаемого множества всех временных рядов, отражающих работу АСУ ТП).

При реализации второго этапа, происходит формирование архитектуры модульной ИНС для формирования прогноза в соответствии со структурой прогнозируемого многокомпонентного временного ряда (для каждого отдельного временного ряда, из наблюдаемого множества всех временных рядов, отражающих работу АСУ ТП). При этом, для каждой базовой компоненты прогнозируемого многокомпонентного временного ряда, в соответствии с их динамическими характеристиками формируются отдельные прогнозы с различным по длительности временным горизонтом. Более «медленные и инерционные» базовые компоненты допускают в результате более длительной автокорреляции, соответственно более длительный прогноз на больший интервал времени вперёд.

При реализации третьего этапа, по полученным прогнозам, отдельных базовых компонент с различным временным горизонтом, формируется завершённый масштабируемый прогноз на различных временных интервалах, то есть прогноз исходного многокомпонентного временного ряда. Самый дальний горизонт прогнозирования исходного многокомпонентного временного ряда определяется самой медленной базовой компонентой. Самый ближний горизонт прогнозирования исходного многокомпонентного временного ряда определяется параметрами самой быстрой базовой компоненты.

Возможности сформированного масштабируемого прогноза в различных временных масштабах для обнаружения в множестве наблюдаемых временных рядов данных АСУ ТП аномалий раздельно по их различным динамическим характеристикам рассмотрены в работах [3, 5].

2. Формирование структуры прогнозирующего модуля для построения прогноза динамического временного ряда данных АСУ ТП

Для формирования прогноза, каждой отдельной компоненты прогнозируемого многокомпонентного временного ряда в работе [20] предложен и рассмотрен прогнозирующий автокодировщик (автоэнкодер, РАЕ), позволяющий, кроме восстановления на выходе РАЕ входного сигнала, или части входного сигнала, также формировать на выходе РАЕ прогнозируемые отсчеты входного сигнала на заданное количество временных шагов «вперед». Показано [20], что использование РАЕ повышает точность результата прогнозирования исследуемого сигнала.

На рисунках 1-3 представлены типовые структуры ИНС автокодировщиков (автоэнкодеров, АЕ)).

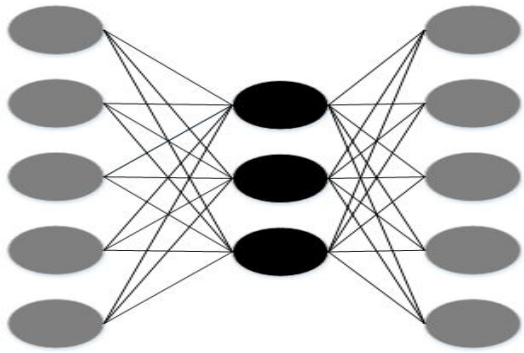

Рис. 1. Типовая структура ИНС автокодировщика (автоэнкодера, АЕ)

Типовой автокодировщик (автоэнкодер) (рис.1) реализуется в виде ИНС прямого распространения, восстанавливающей входной сигнал на выходе ИНС, при этом размер внутреннего слоя ИНС меньше размерности входного и выходного (восстановленного) сигнала.

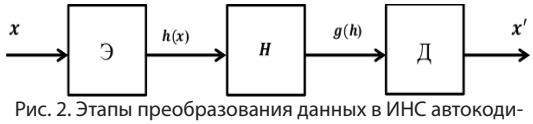

Рис. 2. Этапы преобразования данных в ИНС автокодировщике

На рисунке 2 отображены этапы преобразования данных в автокодировщике. На структурной схеме (рис.2) обозначено: входной сигнал x, выходной сигнал x', представляющий собой копию входного сигнала x. Авто-

кодировщик состоит из двух частей: энкодера и декодера. Энкодер переводит входной сигнал x в его представление (сжатый код): $h = g(x)$, а декодер восстанавливает сигнал x по его коду: $x = f(h)$ Обобщённая структурная схема автоэнкодера, содержащая несколько скрытых слоёв, представлена на рисунке 3.

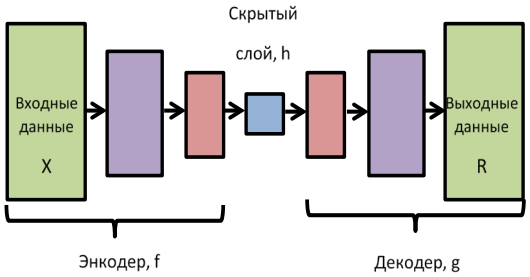

Рис. 3. Обобщённая структурная схема автокодировщика, содержащая несколько скрытых слоёв

Задача ИНС автоэнкодера, состоит в восстановлении, с сохранением наиболее важных свойств, входных данных x в качестве выходных данных x'.

Возможно модифицировать задачу выполняемую ИНС автокодировщика, добавив требование, чтобы кроме отображения входных данных x, в выходные данные x', с сохранением наиболее важных свойств входных данных x, дополнительно, также формировать в выходных данных x', прогнозируемые значения входных данных x. Предполагается, что возможность ИНС автокодировщика (автоэнкодера) при этом отбирать наиболее важные свойства входных данных x, приведёт к повышению качества формируемого прогноза входных данных x, содержащегося в восстанавливаемых автокодировщиком выходных данных x'.

На рисунке 4 отображено преобразование типовой структуры автокодировщика (AE) в структуру прогнозирующего автокодировщика (PAE). Белыми кружками обозначены добавленные прогнозируемые отсчёты входного сигнала x, сформированные в выходном сигнале x'.

На рис. 5а отображена структура прогнозирующего автокодировщика с формированием не симметричного прогноза входного сигнала, на рис. 5б отображено формирование только прогноза входного сигнала, при этом структура (рис. 5б) вырождается в структуру стандартного предиктора, формирующего на выходе только прогнозные значения входного сигнала.

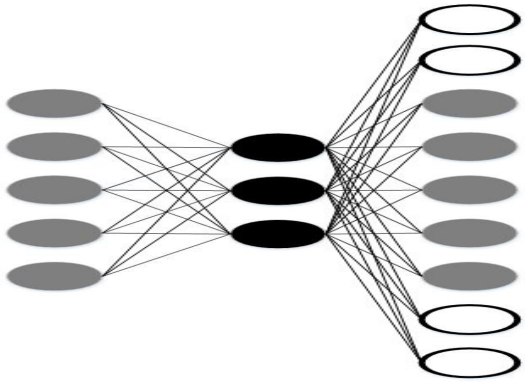

Рис. 4. Структура ИНС прогнозирующего автокодировщика (PAE)

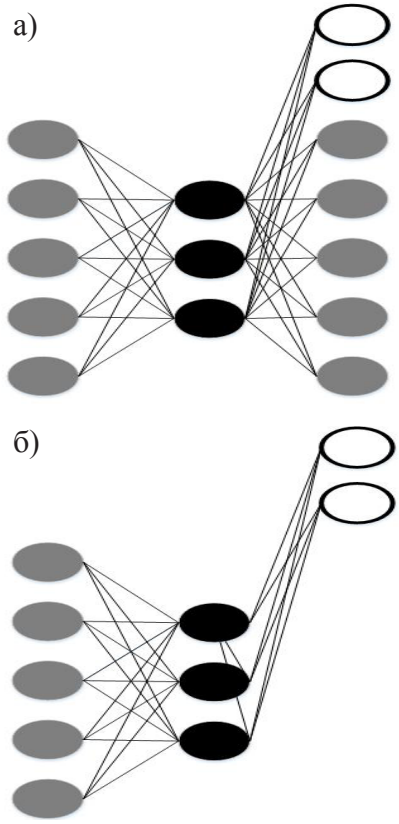

Рис. 5. Структура прогнозирующего автокодировщика с формированием не симметричного прогноза входного сигнала (а), структура стандартного предиктора входного сигнала (б)

Возможно сформировать модифицированную структуру прогнозирующего автокодировщика с формированием прогноза и одновременно с частичным восстановлением входного сигнала (то есть, части входного сигнала) (рис.6а), также с требованием реализовать дополнительное отображение входного сигнала в некоторый выходной сигнал с заданными свойствами (рис. 6б, заштрихованные кружки).

На рис. 7 представлена обобщённая

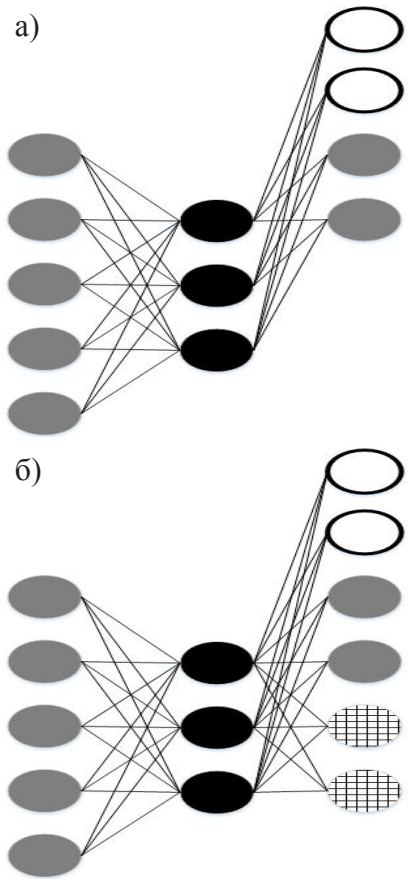

Рис. 6. Модифицированные структуры прогнозирующего автокодировщика

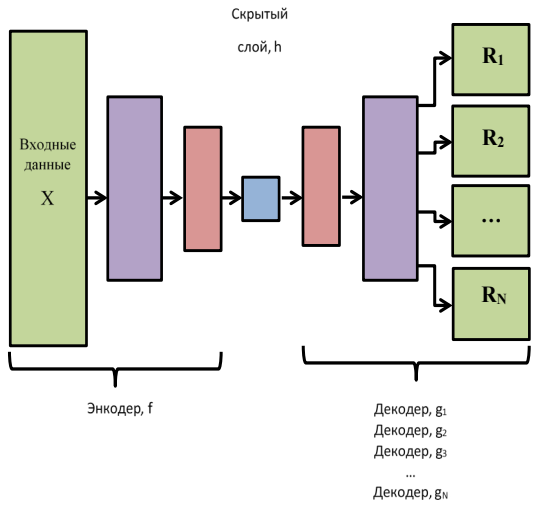

Рис. 7. Обобщённая структурная схема модифицированного автокодировщика, содержащая несколько скрытых слоёв

структура модифицированного прогнозирующего автокодировщика, содержащая несколько скрытых слоёв, результат модификации – одновременное формирование на выходе модифицированного автокодировщика различных отображений входного сигнала: полностью всего входного сигнала (что, является функцией стандартного автокодировщика) или только части входного сигнала, также требуемых прогнозных значений входного сигнала, также дополнительно возможно требование формирования набора различных отображений входного сигнала в требуемые выходные сигналы с заданными свойствами.

Модификация прогнозирующего автокодировщика, представленная на рис.7 позволяет реализовать управление качеством формируемого прогноза входного сигнала за счёт требования одновременной реализации множества дополнительных отображений входного сигнала, формируемых на выходе прогнозирующего автокодировщика (автоэнкодера, PAE) в требуемые выходные сигналы, обладающие различными требуемыми свойствами.

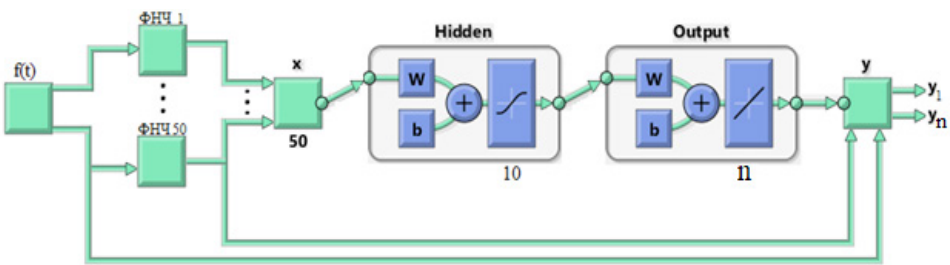

Рис. 8. Структурная схема прогнозирующего модуля: блок ЦОС и прогнозирующий блок с использованием ИНС

В работе [20] для прогнозирования сигналов предлагается применять прогнозирующий модуль, представленный на рис. 8, состоящий из последовательно соединенных блока ЦОС и прогнозирующего блока с использованием ИНС.

В прогнозирующем модуле (рис. 8) блок ЦОС состоит из гребенки цифровых фильтров нижних частот с конечной импульсной характеристикой (КИХ-ФНЧ). При этом на выходе гребенки КИХ-ФНЧ формируется набор отфильтрованных компонентов входного сигнала, далее, подаваемые на вход ИНС [20]. Целевыми отсчетами, подаваемыми на выход

ИНС при машинном обучении прогнозирующего модуля, являются целевые (прогнозируемые) отсчеты входного сигнала (впоследствии, итоговые результаты прогноза), Также, дополнительными целевыми отсчетами, подаваемыми на выход ИНС при машинном обучении прогнозирующего модуля являются дополнительные отсчеты, в виде выборки заданной длины из отсчетов исходного входного сигнала (то есть, со входа блока ЦОС), плюс дополнительно выборки заданной длины из отсчетов сигнала с входа ИНС (то есть, с выхода блока ЦОС). Дополнительно подаваемые на выход ИНС (при машинном обучении) целевые отсчёты, требуют кроме формирования требуемого прогноза, также дополнительное восстановление на выходе ИНС части исходного входного сигнала и части отсчётов сигналов с выхода гребенки КИХ-ФНЧ блока ЦОС. Прогнозирующий модуль, представленный на рис. 8 реализован в соответствии с модифицированной структурой прогнозирующего автокодировщика (автоэнкодера, PAE), отображённого на рис. 6б. Более подробное описание и исследование прогнозирующего модуля, (рис. 8) приведено в работе [20].

3. Результаты исследования качества формируемого прогноза прогнозирующим модулем, реализованным в виде модифицированного прогнозирующего автокодировщика (автоэнкодера)

Проведём сравнение качества прогноза исследуемого сигнала, формируемого стандартным предиктором исследуемого сигнала (рис. 5б) и модифицированным прогнозирующим автокодировщиком (автоэнкодером, PAE) (рис. 6б). Реализация с использованием ИНС (используется блок ЦОС на входе ИНС) стандартного предиктора исследуемого сигнала (рис. 5б) приведена на рис. 9. Реализация с использованием ИНС (используется блок ЦОС на входе ИНС) модифицированного прогнозирующего автоэнкодера (PAE) (рис. 6б) приведена на рис. 8.

На рис. 10 отображены две зависимости максимального количества прогнозируемых отсчётов сигнала (максимальной дальности прогноза), при условии не превышения ошибки прогноза заданной максимальной величины ошибки прогноза (среднеквадратичное отклонение (СКО) результата прогноза), от величины верхней частоты спектра прогнозируемого сигнала, для случаев использования стандартного предиктора (рис. 9) (пунктирная линия, рис. 10) и модифицированного прогнозирующего автокодировщика (автоэнкодера, PAE) (рис. 8) (чёрная линия, рис. 10), соответственно. Обучение ИНС производилось методом Левенберга-Маркварда на выборке сигнала длиной 5000 отсчетов, при этом распределение входных данных: подгонка – 70%, контроль – 15%, тестирование – 15%. Задаваемая максимальная величина ошибки прогноза на интервале тестирования соответствовала СКО=0.25. Верхняя частота спектра прогнозируемого сигнала формировалась фильтрацией исходного сигнала с использованием КИХ-ФНЧ с изменяемой частотой среза. На рис. 10 изменяемая частота среза КИХ-ФНЧ по оси абсцисс отображается в виде обратной величины – периода среза КИХ-ФНЧ, задаваемого в нормированных временных отсчётах.

На рис. 10 увеличение периода среза КИХ-ФНЧ по оси абсцисс соответствует уменьшению верхней частоты спектра прогнозируемого сигнала с выхода КИХ-ФНЧ, что повышает инерционность и увеличивает интервал автокорреляции прогнозируемого сигнала, соответственно, при этом увеличивается (как видно из рис. 10) дальность максимального прогноза при задаваемой фиксированной величине максимальной ошибки прогноза.

В результате сравнения, представленных на рис. 10 двух зависимостей дальности прогноза сигнала (при фиксированной ошибке прогноза сигнала) от верхней частоты спектра сигнала (пунктирная линия на рис. 10 – стандартный предиктор (рис. 9), чёрная линия на рис. 10 – модифицированный прогно-

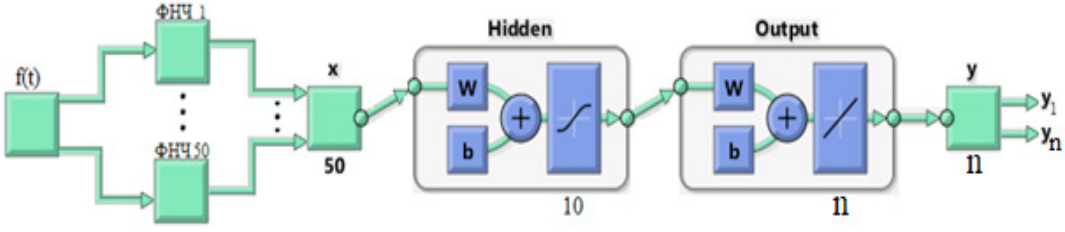

Рис. 9. Структурная схема прогнозирующего модуля: блок ЦОС и прогнозирующий блок с использованием ИНС

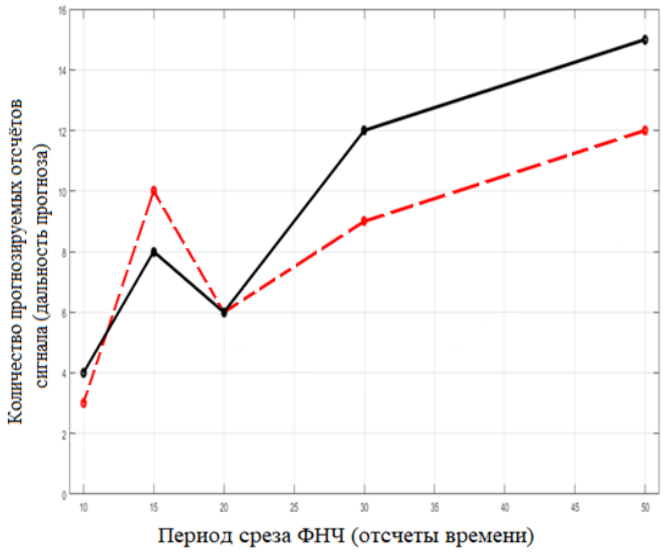

Рис. 10. Зависимость дальности прогноза сигнала от верхней частоты среза прогнозируемого сигнала

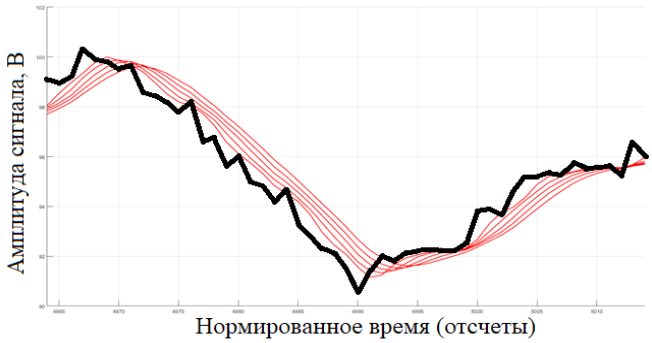

Рис. 11. Пять базовых компонент (тонкие линии) исходного сигнала (жирная чёрная линия), полученных с выходов гребёнки из пяти цифровых КИХ-ФНЧ

зирующий автокодировщик (автоэнкодер, PAE) (рис. 8)) следует вывод, что применение архитектуры PAE, то есть модификация прогнозирующего автокодировщика, представленная на рис.7 и реализованного в виде структуры, представленной на рис. 8, позволяет увеличить точность формируемого прогноза входного сигнала.

4. Формировании прогноза многокомпонентных временных рядов данных с использованием методов цифровой фильтрации и модифицированного прогнозирующего автокодировщика (автоэнкодера)

При формировании прогноза многокомпонентных временных рядов данных применяется технология ЦОС для разложения сложного многокомпонентного временного ряда на отдельные базовые компоненты (то есть, структурный анализ многокомпонентного временного ряда). Отфильтрованные базовые компоненты исходного сигнала формируются в результате прохождении сигнала через гребёнку цифровых ФНЧ и в получении на выходе набора отфильтрованных компонентов исходного сигнала. При таком подходе производится компонентное разложение исходного сигнала и последовательная фильтрация шумов с использованием параллельного набора цифровых ФНЧ.

На рис. 11 представлен результат структурного анализа многокомпонентного временного ряда, при этом исходный временной ряд данных (жирная чёрная линия, рис. 11) разложен на пять базовых компонент (тонкие линии, рис. 11), полученных с выходов гребенки из пяти цифровых КИХ-ФНЧ с периодами среза, равными величинам 7, 10, 13, 16, 19 отсчётов времени, соответственно. Период среза ФНЧ определяется как обратная величина частоты среза ФНЧ.

На рис. 12 представлен результат формирования архитектуры модульной ИНС для формирования прогноза в соответствии со структурой прогнозируемого многокомпонентного временного ряда. В данном примере на рис. 12 представлена архитектура мо-

дульной ИНС из пяти прогнозирующих модулей, представленных на рис. 8.

С использованием архитектуры модульной ИНС из пяти прогнозирующих модулей (рис. 8) и технологии «машинного обучения» для каждой из пяти базовых компонент исходного сигнала (рис. 11, тонкие линии), в соответствии с их динамическими характеристиками, формируются пять отдельных прогнозов с различным по длительности временным горизонтом.

На рис. 13 – 17 представлены сформированные пять отдельных прогнозов с различным по длительности временным горизонтом на 2, 3, 4, 5, 6 временных отсчётов вперед, для каждой из пяти базовых компонент (рис. 11, тонкие линии), соответственно. Также, на рис. 13 – 17 отображены доверительные интервалы (полосы) прогноза вперед для каждой из пяти базовых компонент, рассчитываемые в виде СКО каждой отфильтрованной базовой компоненты относительно исходного сигнала (рис. 11, жирная черная линия).

Более медленные и инерционные базовые компоненты (рис. 11, тонкие линии), допускают в результате более длительной автокорреляции, соответственно более длительный прогноз на больший интервал времени вперед, при этом доверительный интервал (полоса) прогноза каждой отфильтрованной базовой компоненты отражает прогнозное изменение исходного сигнала (рис. 11, жирная чёрная линия) в пределах доверительного интервала прогноза для каждой базовой компоненты (рис. 11, тонкие линии).

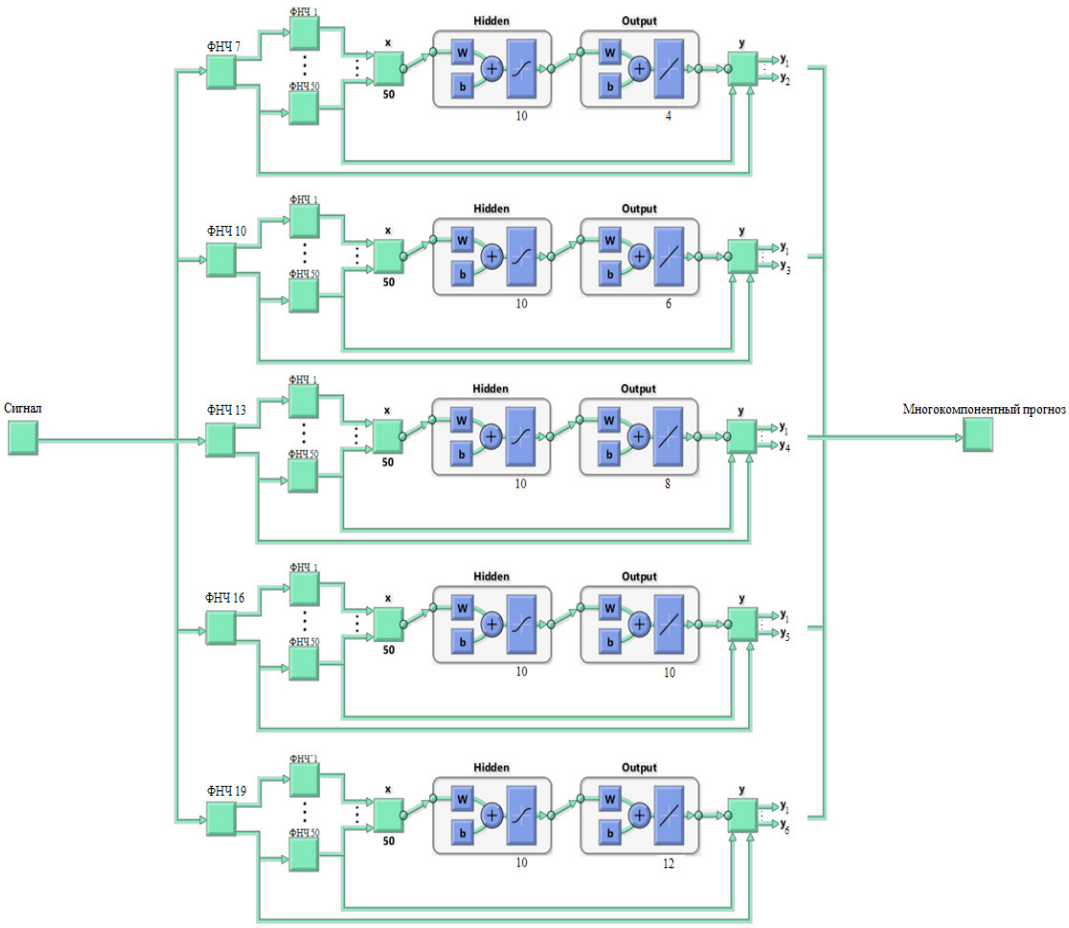

Рис. 12. Архитектуры модульной ИНС из пяти прогнозирующих модулей (рис. 8), формирующей многокомпонентный прогноз наблюдаемого временного ряда

В таблице 1 приведены результаты расчета СКО ошибки прогноза (для каждой из пяти базовых компонент, рис. 11, тонкие линии) с различным по длительности временным горизонтом на 2, 3, 4, 5, 6 временных отсчётов вперед,

Далее, по полученным пяти отдельным прогнозам с различным временным горизонтом базовых компонент исходного сигнала (рис.18, жирная черная линия), формируется

Рис. 13. Результат прогнозирования первой компоненты с временным горизонтом на 2 отсчёта вперёд

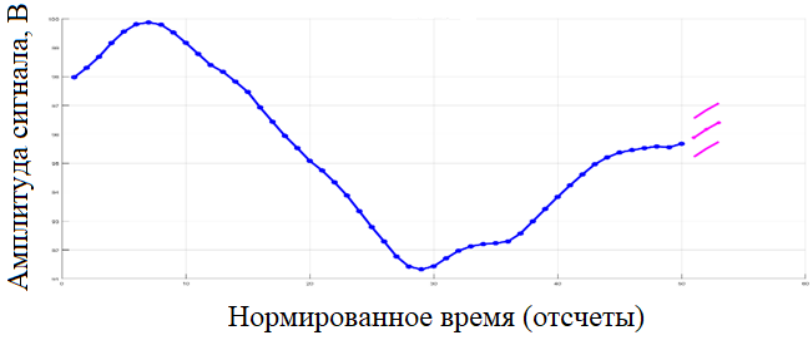

Рис. 14. Результат прогнозирования второй компоненты с временным горизонтом на 3 отсчёта вперёд

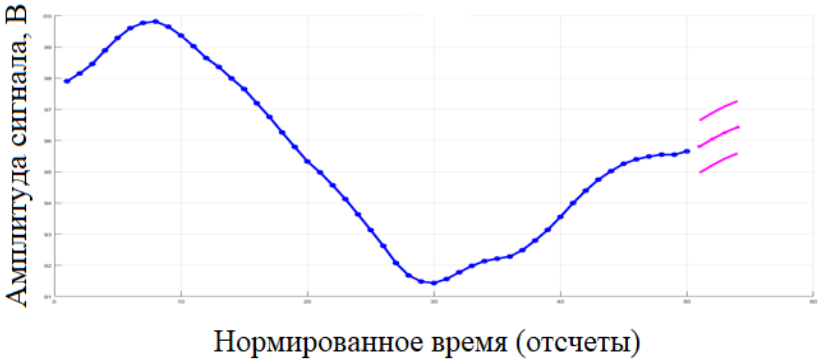

Рис. 15. Результат прогнозирования третьей компоненты с временным горизонтом на 4 отсчёта вперёд

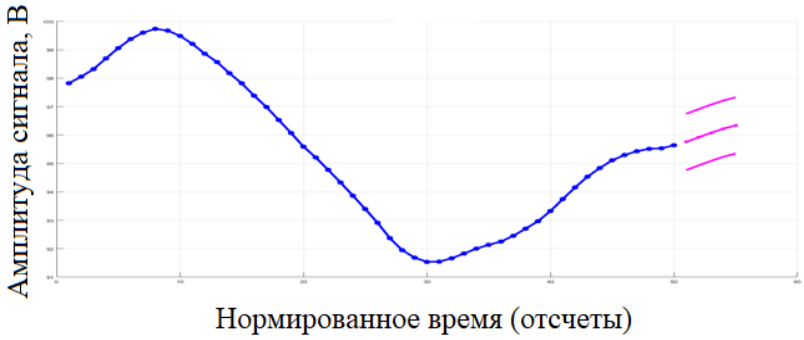

Рис. 16. Результат прогнозирования четвёртой компоненты с временным горизонтом на 5 отсчётов вперёд

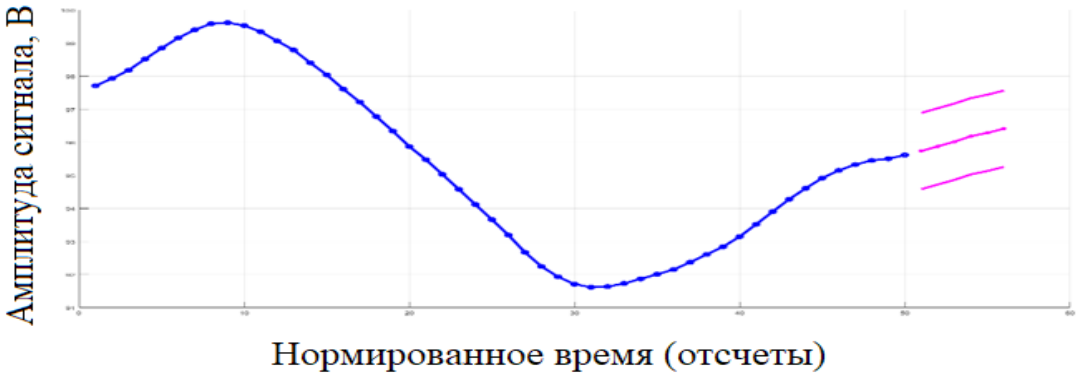

Рис. 17. Результат прогнозирования пятой компоненты с временным горизонтом на 6 отсчётов вперёд

Таблица 1

СКО сигналов на разных периодах среза ФНЧ

Период среза ФНЧ, (количество временных отсчётов).	Длительность временного горизонта, (количество временных отсчётов).	СКО
7	2	0,1777332
10	3	0,1898771
13	4	0,2009997
16	5	0,2156947
19	6	0,2249945

завершенный масштабируемый прогноз на различных временных интервалах (рис.18, тонкие линии).

Из отображенного результата прогноза (рис. 18, тонкие линии прогноза) следует, что самый ближний горизонт прогнозирования исходного многокомпонентного временного ряда (рис.18, жирная черная линия) определяется параметрами самой быстрой базовой компонентой (прогноз базовой компоненты, плюс доверительный интервал (полоса) прогноза базовой компоненты). Самый дальний горизонт прогнозирования исходного многокомпонентного временного ряда (рис.18, жирная черная линия) определяется самой медленной базовой компонентой и имеет максимальную ширину полосы прогноза (ширину доверительного интервала прогноза).

На рис. 19, более детально показан временной участок, соответствующий многоком-

Рис. 18. Сформированный прогноз исходного многокомпонентного временного ряда

понентному прогнозу (отображен на рис. 18, тонкие линии), также добавлен временной участок исходного прогнозируемого сигнала (рис. 18, жирная черная линия).

На рис. 19 отображено: сформированный многокомпонентный прогноз (пунктирные линии) исходного сигнала, добавлена жирная черная линия – продолжение исходного прогнозируемого сигнала на область сформированного многокомпонентного прогноза. Из рис. 19 следует, что сформированный многокомпонентный прогноз задает доверительную область прогноза исследуемого сигнала.

5. Заключение.

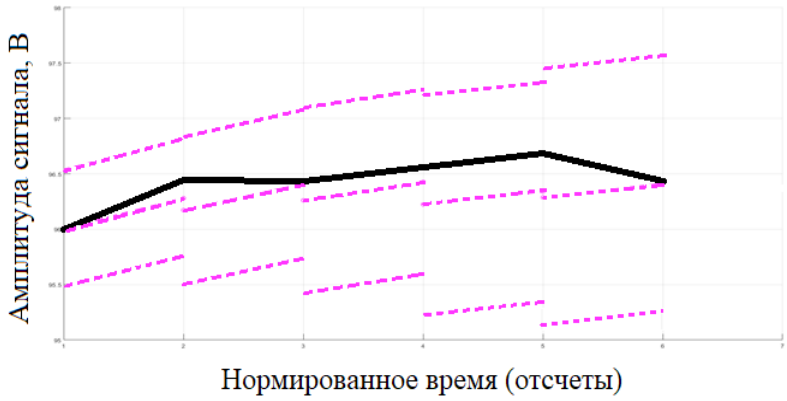

Рис. 19. Многокомпонентный прогноз (пунктирные линии) временного участка исходного сигнала (жирная чёрная линия)

Процессы, протекающие в АСУ ТП и отражаемые в наблюдаемых потоках данных, являются сложными многокомпонентными процессами, что существенно усложняет формирование их прогнозов. Для реализации многокомпонентного прогноза предлагается применять технологию ЦОС для разложения сложного многокомпонентного временного ряда на отдельные базовые компоненты (структурный анализ многокомпонентного временного ряда), также предлагается формировать модульную архитектуру ИНС для осуществления прогноза, в соответствии со структурой прогнозируемого многокомпонентного временного ряда.

При возникновении аномалий в работе АСУ ТП будут происходить структурные изменения в сигнале ошибки формируемого прогноза, в результате анализа этих структурных изменений ошибки прогноза, собственно происходит детектирование (обнаружение) аномалий в наблюдаемых процессах АСУ ТП. Предлагаемый подход формирования прогноза для каждой отдельной базовой компоненты прогнозируемого многокомпонентного временного ряда, в соответствии с их динамическими характеристиками, позволит обнаруживать в множестве наблюдаемых временных рядов данных АСУ ТП аномалии раздельно по их различным динамическим характеристикам, что повышает эффективность управления устойчивостью функционирования АСУ ТП в условиях воздействия кибератак.

При формировании многокомпонентного прогноза временных рядов данных АСУ ТП предлагается применять ИНС – модифицированный прогнозирующий автокодировщик (автоэнкодер, PAE). В проведённом исследовании показано, что ИНС – модифицированный прогнозирующий автокодировщик (автоэнкодер, PAE) позволяет увеличить точность формируемого прогноза входного сигнала, что важно при реализации обнаружения (детектирования) аномалий по результатам анализа структурных изменений, возникающих в сигнале ошибки формируемого прогноза исследуемого сигнала.

Литература

1. A. Ragozin, V.Telezhkin, P.Podkorytov, «Prediction of Aggregate Multicomponent Time Series in Industrial Automated Systems Using Neural Network», Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2019, 13-15 March, 2019, Hong Kong, pp. 17-19.

2. A. N. Ragozin, V. F. Telezhkin, P. S. Podkorytov. State Prediction in Control Systems via Compound Time Series: Neural Network Approach. EEE SoutheastCon 2019 Von Braun Center Huntsville, Alabama April 11th-14th, 2019. Pages 1–6.

3. A. N. Ragozin, V. F. Telezhkin, P. S. Podkorytov, «Forecasting Complex Multi-component Time Series within Systems Designed to Detect Anomalies in Dataflows of Industrial Automated Systems», SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks, September 2019, Article No.: 2, pp. 1–5.

4. A. N. Sokolov, A. N. Ragozin, I. A. Pyatnitsky, S. K. Alabugin, «Applying of Digital Signal Processing Techniques to Improve the Performance of Machine Learning-based Cyber Attack Detection in Industrial

Control System», SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks, September 2019, Article No.: 23, pp. 1–4.

5. Ragozin A. N. ; Osipov D. V. ; Tarasov I. S. ; Pletenkova A. D., Investigation of the Influence of the Preliminary Digital Filtering Method on the Accuracy of Sig-nal Prediction in Anomaly Detection Systems in Industrial Automatic Control Systems (IACS), 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT) 2020, 14-15 May, 2020, Yeka-terinburg, Russia,, pp. 1-4.

6. S. Tomonobu and T. Hitoshi, «One-hour-ahead load forecasting using neural network», IEEE Transactions on Power Systems, no. 1, pp. 21–24, 2002.

7. R. Huang, T. Huang, and Gadh, «Solar generation prediction using the ARMA model in a laboratory-level micro-grid», in IEEE Third International Conference on Smart Grid Communications, Sydney, 2012, pp. 528–533.

8. A. M. Abdurakhmanov, M. V. Volodin, E. Yu. Zybin, and V. N. Ryabchenko, «Methods for predicting power consumption in distribution networks (review)», Russian Internet Journal of Electrical Engineering, pp. 3–23, 2016.

9. A. N. Ragozin, A. A. Razumov, «Neural network forecasting with preliminary digital filtering of complex radio signals», in XVI International scientific and technicalconference Physics and technicalapplications of wave processes, Miass, 2018, pp. 285–290.

10. M. Granroth-Wilding and S. Clark, «What Happens Next? Event Prediction Using a Compositional Neural Network Model», AAAI, pp. 2727–2733, 2016.

11. Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid. SANS Industrial Control Systems, 23.

12. Xiao, Y. J., Xu, W. Y., Jia, Z. H., Ma, Z. R., & Qi, D. L. (2017). NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers. Frontiers of Information Technology & Electronic Engineering, 18(4), 519-534.

13. Wang, W., Xie, Y., Ren, L., Zhu, X., Chang, R., & Yin, Q. (2018, May). Detection of data injection attack in industrial control system using long short term memory recurrent neural network. In 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 2710-2715). IEEE.

14. Kravchik, M., & Shabtai, A. (2018, October). Detecting cyber attacks in industrial control systems using convolutional neural networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy (pp. 72-83). ACM.

15. Muna, A. H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 41, 1-11

16. Potluri, S., Diedrich, C., & Sangala, G. K. R. (2017, September). Identifying false data injection attacks in industrial control systems using artificial neural networks. In 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (pp. 1-8). IEEE.

17. Yang, H., Chen, T., Guo, X., Wang, X., & Li, F. (2017, December). Research on intrusion detection of industrial control system based on OPSO-BPNN algorithm. In 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (pp. 957-961). IEEE.

18. Demertzis, K., Iliadis, L., & Spartalis, S. (2017, August). A spiking one-class anomaly detection framework for cyber-security on industrial control systems. In International Conference on Engineering Applications of Neural Networks (pp. 122-134). Springer, Cham.

19. Wu, Z., Albalawi, F., Zhang, J., Zhang, Z., Durand, H., & Christofides, P. (2018). Detecting and Handling Cyber-attacks in Model Predictive Control of Chemical Processes. Mathematics, 6(10), 173.

20. Рагозин А.Н. Применение цифровой обработки сигналов и нейронной сети при формировании прогноза временных рядов данных для целей обнаружения аномалий при автоматизированном управлении технологическими процессами. Вестник УрФО. Безопасность в информационной сфере., No 1 (35), 2020. – С. 24–34.

References

1. A. Ragozin, V.Telezhkin, P.Podkorytov, «Prediction of Aggregate Multicomponent Time Series in Industrial Automated Systems Using Neural Network», Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2019, 13-15 March, 2019, Hong Kong, pp. 17-19.

2. A. N. Ragozin, V. F. Telezhkin, P. S. Podkorytov. State Prediction in Control Systems via Compound Time Series: Neural Network Approach. EEE SoutheastCon 2019 Von Braun Center Huntsville, Alabama April 11th-14th, 2019. Pages 1–6.

3. A. N. Ragozin, V. F. Telezhkin, P. S. Podkorytov, «Forecasting Complex Multi-component Time Series within Systems Designed to Detect Anomalies in Dataflows of Industrial Automated Systems», SIN '19:

Proceedings of the 12th International Conference on Security of Information and Networks, September 2019, Article No.: 2, pp. 1–5.

4. A. N. Sokolov, A. N. Ragozin, I. A. Pyatnitsky, S. K. Alabugin, «Applying of Digital Signal Processing Techniques to Improve the Performance of Machine Learning-based Cyber Attack Detection in Industrial Control System», SIN '19: Proceedings of the 12th International Conference on Security of Information and Networks, September 2019, Article No.: 23, pp. 1–4.

5. Ragozin A. N. ; Osipov D. V. ; Tarasov I. S. ; Pletenkova A. D., Investigation of the Influence of the Preliminary Digital Filtering Method on the Accuracy of Sig-nal Prediction in Anomaly Detection Systems in Industrial Automatic Control Systems (IACS), 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT) 2020, 14-15 May, 2020, Yeka-terinburg, Russia,, pp. 1-4.

6. S. Tomonobu and T. Hitoshi, «One-hour-ahead load forecasting using neural network», IEEE Transactions on Power Systems, no. 1, pp. 21–24, 2002.

7. R. Huang, T. Huang, and Gadh, «Solar generation prediction using the ARMA model in a laboratory-level micro-grid», in IEEE Third International Conference on Smart Grid Communications, Sydney, 2012, pp. 528–533.

8. A. M. Abdurakhmanov, M. V. Volodin, E. Yu. Zybin, and V. N. Ryabchenko, «Methods for predicting power consumption in distribution networks (review)», Russian Internet Journal of Electrical Engineering, pp. 3–23, 2016.

9. A. N. Ragozin, A. A. Razumov, «Neural network forecasting with preliminary digital filtering of complex radio signals», in XVI International scientific and technicalconference Physics and technicalapplications of wave processes, Miass, 2018, pp. 285–290.

10. M. Granroth-Wilding and S. Clark, «What Happens Next? Event Prediction Using a Compositional Neural Network Model», AAAI, pp. 2727–2733, 2016.

11. Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid. SANS Industrial Control Systems, 23.

12. Xiao, Y. J., Xu, W. Y., Jia, Z. H., Ma, Z. R., & Qi, D. L. (2017). NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers. Frontiers of Information Technology & Electronic Engineering, 18(4), 519-534.

13. Wang, W., Xie, Y., Ren, L., Zhu, X., Chang, R., & Yin, Q. (2018, May). Detection of data injection attack in industrial control system using long short term memory recurrent neural network. In 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 2710-2715). IEEE.

14. Kravchik, M., & Shabtai, A. (2018, October). Detecting cyber attacks in industrial control systems using convolutional neural networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy (pp. 72-83). ACM.

15. Muna, A. H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 41, 1-11

16. Potluri, S., Diedrich, C., & Sangala, G. K. R. (2017, September). Identifying false data injection attacks in industrial control systems using artificial neural networks. In 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA) (pp. 1-8). IEEE.

17. Yang, H., Chen, T., Guo, X., Wang, X., & Li, F. (2017, December). Research on intrusion detection of industrial control system based on OPSO-BPNN algorithm. In 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (pp. 957-961). IEEE.

18. Demertzis, K., Iliadis, L., & Spartalis, S. (2017, August). A spiking one-class anomaly detection framework for cyber-security on industrial control systems. In International Conference on Engineering Applications of Neural Networks (pp. 122-134). Springer, Cham.

19. Wu, Z., Albalawi, F., Zhang, J., Zhang, Z., Durand, H., & Christofides, P. (2018). Detecting and Handling Cyber-attacks in Model Predictive Control of Chemical Processes. Mathematics, 6(10), 173.

20. Ragozin A.N. Application of digital signal processing and neural network in the formation of time series prediction for the purpose of anomaly detection in automated process control. Bulletin of the Urals Federal District. Securityintheinformationfield, Vol 1 (35), 2020. – P. 24–34.

РАГОЗИН Андрей Николаевич, кандидат технических наук, доцент кафедры защиты информации, доцент кафедры инфокоммуникационных технологий высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: ragozinan@susu.ru

RAGOZIN Andrey, Candidate of Sciences in Technology, Department of Information Security, Department of Information Technology Federal State Autonomous Educational Institution of Higher Education «South Ural State University (national research university)» Russia, 454080, Chelyabinsk, prsp. Lenina, 76. E-mail: ragozinan@susu.ru