Ирина С. Гефнер[1], Сергей М. Коваленко[2], Александр С. Суховерхов[3],
Сергей В. Соловьев[4]
[1]Федеральная служба по техническому и экспортному контролю,
ул. Старая Басманная, 17, Москва, 105175, Россия
[2,3,4]Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю,
ул. 9 Января, 280а, Воронеж, 394020, Россия
[1]e-mail: igefner@yandex.ru, https://orcid.org/0000-0003-2747-0857
[2]e-mail: skovalenko90@yandex.ru, https://orcid.org/0000-0001-8584-7945
[3]e-mail: mostom84@mail.ru, https://orcid.org/0000-0002-5557-0719
[4]e-mail: gniii_ptzi_3_upr@mail.ru, https://orcid.org/0000-0002-3983-2408

МЕТОДИЧЕСКИЙ ПОДХОД К ВЫЯВЛЕНИЮ ДЕСТРУКТИВНЫХ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ НА РАСПРЕДЕЛЕННУЮ СИСТЕМУ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

DOI: http://dx.doi.org/10.26583/bit.2020.1.10

Аннотация. Целью статьи является совершенствование методического обеспечения оценивания возможности реализации последовательности информационных воздействий на распределенную систему управления, приводящих к аварийным ситуациям. Решается проблема оценки возможности реализации последовательности информационных воздействий на распределенную систему управления, приводящих к аварийным ситуациям. Предлагается методический подход к выявлению последовательностей информационных воздействий, приводящих к аварийной ситуации на промышленных объектах, основанный на применении метода временных различий машинного обучения с подкреплением. Оценивается эффективность применения рассматриваемого методического подхода по сравнению с методом равновероятного перебора. Приводится пример реализации методического подхода в отношении технологического процесса, применяемого на промышленных объектах.

Ключевые слова: промышленный объект, аварийная ситуация, последовательность информационных воздействий, распределенная система управления.
Для цитирования: ГЕФНЕР, Ирина С. et al. МЕТОДИЧЕСКИЙ ПОДХОД К ВЫЯВЛЕНИЮ ДЕСТРУКТИВНЫХ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ НА РАСПРЕДЕЛЕННУЮ СИСТЕМУ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ. Безопасность информационных технологий, [S.l.], v. 27, n. 1, p. 111-118, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1258>. Дата доступа: 06 mar. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.1.10.

Irina S. Gefner[1], Sergey M. Kovalenko[2], Alexandr S. Sukhoverkhov[3], Sergey V. Solovyov[4]
[1]Federal Service for Technical and Export Control of Russia,
Staraya Basmannaya Str., 17, Moscow, 105175, Russia
[2,3,4]State research and testing Institute of problems of technical protection of information of the FSTEC,
on January 9 Str., 280a, Voronezh, 394020, Russia
[1]e-mail: igefner@yandex.ru, https://orcid.org/0000-0003-2747-0857
[2]e-mail: skovalenko90@yandex.ru, https://orcid.org/0000-0001-8584-7945
[3]e-mail: mostom84@mail.ru, https://orcid.org/0000-0002-5557-0719
[4]e-mail: gniii_ptzi_3_upr@mail.ru, https://orcid.org/0000-0002-3983-2408

A methodological approach to identifying destructive information actions on a distributed process control system

DOI: http://dx.doi.org/10.26583/bit.2020.1.10

Abstract. The aim of this study is to improve the methodological support for evaluating a possibility of implementing a sequence of information actions on a distributed control system leading to emergency

situations. The problem of evaluating a possibility of implementing a sequence of information actions on a distributed control system leading to emergency situations is solved. A methodological approach is proposed to identify information actions sequences leading to an emergency situation at industrial facilities, based on the use of the method of time differences of machine learning with reinforcement. The effectiveness of the considered methodological approach in comparison with the method of equal probability search is estimated. An example of the implementation of the methodological approach in relation to the technological process used at industrial facilities is given.
Keywords: industrial facility, an emergency situation, information actions sequence, distributed control system.
For citation: GEFNER, Irina S. et al. A methodological approach to identifying destructive information actions on a distributed process control system. IT Security (Russia), [S.l.], v. 27, n. 1, p. 111-118, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1258>. Date accessed: 06 mar. 2020. DOI:http://dx.doi.org/10.26583/bit.2020.1.10.

Введение

В настоящее время вопросам обеспечения безопасного функционирования промышленных объектов уделяется повышенное внимание. Фактом, подтверждающим значимость таких объектов с точки зрения обеспечения безопасности их функционирования, является введение в действие с 1 января 2018 г. Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Согласно данному нормативному документу значимость таких объектов определяется последствиями, которые могут наступить в результате нарушения функционирования критической информационной инфраструктуры (КИИ). С учетом этого актуальным является определение таких последствий.

В настоящее время внимание уделяется в основном вопросам защиты автоматизированных систем управления технологическим процессом от несанкционированного доступа (НСД), при этом сами последствия нарушения функционирования промышленного объекта в результате осуществления нарушителем НСД не рассматриваются.

Определение последствий нарушения функционирования промышленного объекта представляет собой сложную и трудоемкую задачу, решение которой базируется на оценке взаимосвязанности и влияния на ход технологического процесса (ТП) большого количества технологического оборудования и их параметров работы (давления, температуры, положений клапанов и др.), управляемого через распределенную систему управления (РСУ). Решение этой задачи экспертными методами, основанными только на опыте и квалификации технологов, практически невозможно. Как показывает опыт, экспертно можно оценить влияние и взаимосвязь не более 10 единиц оборудования (колонн, клапанов, насосов). Увеличение объема рассматриваемого оборудования приводит к получению некорректных результатов оценивания последствий и ошибочному определению уровня значимости КИИ.

Предлагаемый методический подход

Предлагаемый методический подход позволяет выявлять последовательности информационных воздействий, приводящие к аварийной ситуации, в отношении функционирования промышленного объекта на основе оценки влияния параметров работы его взаимосвязанного технологического оборудования на основе моделирования с использованием программных средств типа Simulink [1], Hysys [2], PetroSIM [3], которые позволяют моделировать технологический процесс в пошаговом режиме.

Методический подход состоит в следующем.

На первом этапе определяется критический элемент (колонна, печь и т.д.), его параметры (давление, температура и т.д.), а также значение параметра (критическое значение), при котором наступает аварийная ситуация. При этом под критическим элементом понимается элемент промышленного объекта, физическое разрушение которого становится возможным при достижении критического значения критического параметра и приводит к возникновению аварийной ситуации. Если критических элементов несколько, то подход следует применить к каждому из них отдельно. Предполагается, что аварийная ситуация наступает тогда и только тогда, когда параметр выбранного критического элемента достигает критического значения.

Далее в модели выбираются исполнительные механизмы в соответствии с регламентом работы оборудования, которые могут быть использованы для достижения аварийной ситуации. Выбор исполнительных механизмов осуществляется исходя из возможностей потенциального нарушителя по изменению их состояния через распределенную систему управления. Примерами исполнительных механизмов являются регулирующие и отсечные клапаны, насосы, аппараты воздушного охлаждения и другое оборудование.

На втором этапе реализуется основная процедура, состоящая в формировании последовательности действий, приводящих к аварийной ситуации:

– открытие/закрытие регулирующего клапана на минимально возможную величину;
– открытие/закрытие отсечного клапана;
– включение/выключение насоса;
– включение/выключение аппаратов воздушного охлаждения;
– включение/выключение других исполнительных механизмов;
– возможность ничего не делать.

Реализация указанной процедуры может осуществляться с применением метода простого перебора, относящегося к классу методов поиска решения исчерпыванием всевозможных вариантов. Однако, решение поставленной задачи данным методом практически нереализуемо из-за большого количества всевозможных комбинаций управляющих воздействий, количество которых может достигать десятки тысяч, и отсутствия учета динамики ТП.

В связи с этим для решения этой задачи предлагается использование метода временных различий машинного обучения с подкреплением [4–9], который парирует указанные недостатки. Суть метода временных различий машинного обучения с подкреплением заключается в пошаговой оценке текущего состояния модели и совершаемых действий относительно предыдущих состояний модели с последующей корректировкой применяемой стратегии.

По результатам анализа информационных источников [4, 6, 10–13] данный метод широко применяется для решения задач оптимального управления технологическими процессами. В отличие от других методов машинного обучения (например, методов Монте-Карло) метод временных различий с одной стороны является интерактивным и полностью инкрементным, что позволяет учитывать динамику технологического процесса, а с другой – не требует завершения эпизодов для обучения.

На третьем этапе реализации методического подхода анализируются полученные последовательности действий, реализация которых приводит к аварийной ситуации.

Целью методического подхода является выявление хотя бы одной последовательности информационных воздействий, приводящей к аварийной ситуации. В связи с этим вопросы полноты определения всех возможных последовательностей

информационных воздействий, приводящей к аварийной ситуации, не рассматривались. В большинстве случаев достаточно определить возможность наступления аварийной ситуации (найти хотя бы одну последовательность) и лишь затем оптимизировать найденные последовательности исходя из выбранных критериев (самая короткая, самая быстрая, с наименьшим влиянием на другие параметры технологического процесса и т.д.).

Исходными данными для реализации методического подхода являются:

– модель технологического процесса;

– критический параметр и его значение, при котором наступает аварийная ситуация, указанное в технической документации;

– перечень действий, которые можно использовать для достижения аварийной ситуации, определяемых экспертно технологами или разработчиками автоматизированной системы управления.

Алгоритм реализации метода временных различий машинного обучения с подкреплением выявления последовательностей информационных воздействий, приводящих к аварийной ситуации на промышленном объекте в виде блок-схемы приведен на рис. 1.

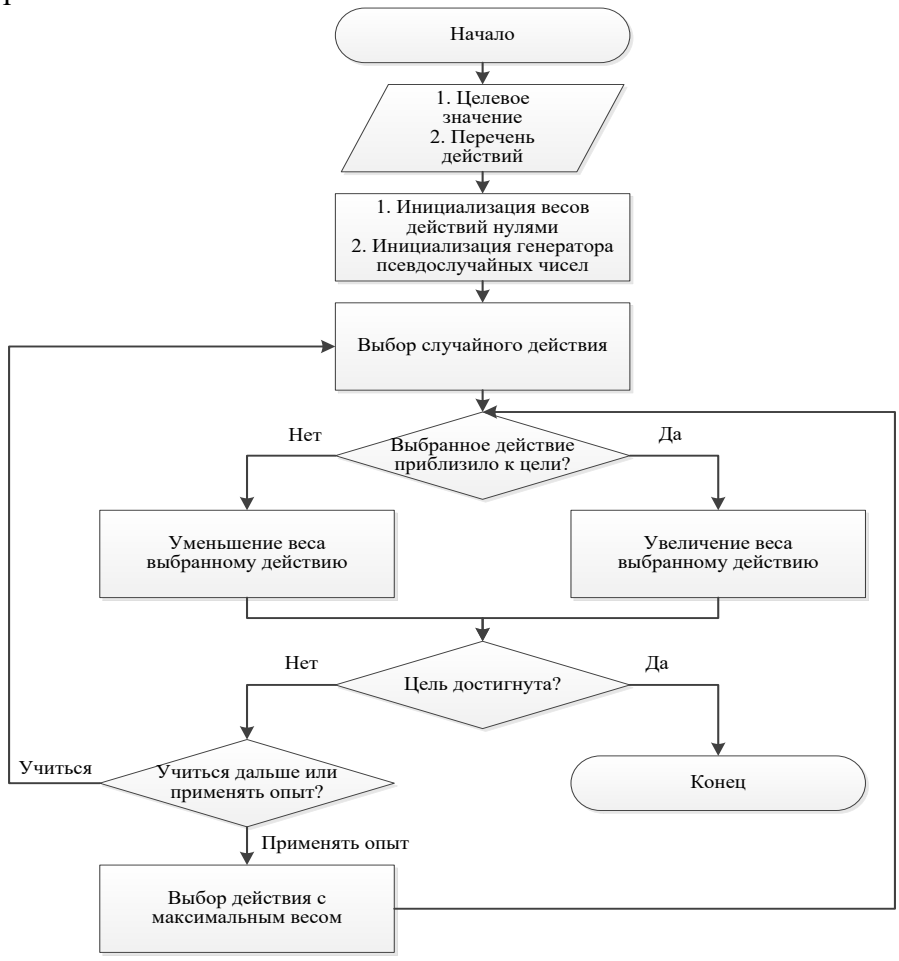

Рис. 1. Блок-схема алгоритма метода временных различий машинного обучения с подкреплением выявления последовательностей информационных воздействий, приводящих к аварийной ситуации на промышленном объекте

(Fig. 1. Block diagram of the algorithm of the time differences method of machine learning with the reinforcement to identify information actions sequences that lead to an emergency situation at industrial facilities)

Указанный алгоритм может выполняться в двух режимах:

– режим обучения;

– режим применения накопленного опыта.

В режиме обучения выполняются действия по изменению параметров ТП и оценивается отклик системы на эти действия путем сравнения изменившихся значений критических параметров ТП со значениями критических параметров ТП до выполнения действий. По результатам оценки повышается вес у действий, приближающих значение критического параметра к цели, и понижается вес, в противном случае. По мере получения достаточной информации о системе (вес какого-либо действия превысил порог) происходит переключение в режим применения накопленного опыта. В режиме применения накопленного опыта выполняются действия, имеющие максимальный вес.

Для реализации режима обучения требуется возможность выполнения равновероятных случайных действий.

Апробация методического подхода проводилась на модели установки стабилизации нефти на объекте подготовки нефти. В ходе реализации методического подхода было смоделировано три вычислительных блока – блок генерации псевдослучайных чисел, блок логики и блок памяти предыдущих состояний.

Блок генерации псевдослучайных чисел, позволяет осуществлять случайное действие. В связи с отсутствием в среде моделирования встроенного генератора случайных чисел были разработаны генераторы псевдослучайных чисел (ГПСЧ) на основе значений параметров технологического процесса. Оценка равномерности получаемого распределения на основе критериев хи-квадрат и тестов NIST [14, 15] подтвердила хорошие статистические свойства разработанных ГПСЧ.

Блок памяти предыдущих состояний позволяет вести учет динамики технологического процесса на возмущающие воздействия. В ходе апробации блок памяти сохранял девять предшествующих состояний модели. Количество хранимых предшествующих состояний связано с ограничениями среды моделирования.

Блок логики, используя информацию из блоков генерации псевдослучайных чисел и памяти предыдущих состояний, оценивает совершаемые действия, обновляет их веса, и на основе получаемой информации осуществляет новый выбор действий вплоть до достижения цели - аварийной ситуации.

Обновление весов проводилось в соответствии с формулой:

$$V_{i+1} = V_i + \sum_{j=1}^{9} \alpha_{i-j} * r_{i-j}\,, \qquad \text{при } i > 10,$$

где V_{i+1} - новое значение веса выполненного действия;

V_i – первоначальное значение веса выполненного действия;

r_{i-j} – получаемое вознаграждение на текущем шаге *i*, относительно шага *j*;

α_{i-j} – коэффициент значимости вознаграждения, рассчитываемого для шага *(i-j)*, $\alpha \in [0; 1]$.

Коэффициенты значимости вознаграждения α_{i-j} определяются экспертно из соображения, что информационные воздействия, реализованные на шаге $i - j_1$, имеют большую значимость (коэффициент принимает большее значение), чем информационные воздействия, реализованные на шаге $i - j_2$ для $\forall j_1 < j_2$.

Под вознаграждением понимается степень приближения значения критического параметра к значению, при котором достигается аварийная ситуация. Вознаграждение рассчитывается по формуле:

$$r_{i-j} = T_i - T_{i-j},$$

где T_i - значение критического параметра на текущем шаге *i*;

T_{i-j} – значение критического параметра на шаге *i-j*.

Реализуемость методического подхода проверялась на примере исследования аварийной ситуации в печи, используемой на установке стабилизации нефти. В технической документации указано, что авария в печи возникает при ее нагреве до 1000 °С.

Клапаны, используемые для достижения аварии, приведены на мнемосхеме (рис. 2).

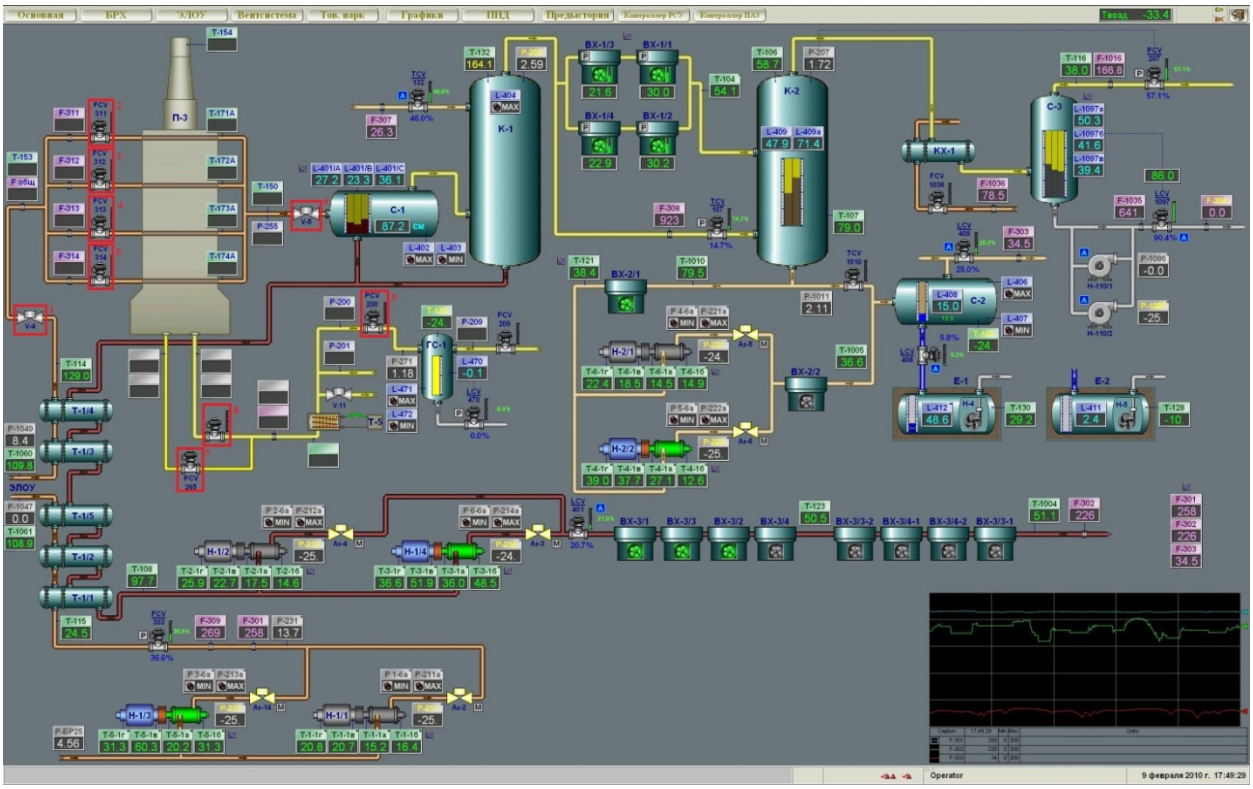

Рис. 2. Мнемосхема установки стабилизации нефти с выбранными клапанами, используемыми для поиска аварийной ситуации
(Fig. 2. Mnemonic diagram of an oil stabilization unit with selected valves used to search for an emergency situation)

При проведении экспериментальных исследований по выявлению последовательностей деструктивных информационных воздействий, осуществляемых через распределенную систему управления технологическим процессом, с применением предлагаемого методического подхода проводился учет действий, выполняемых алгоритмом, записываемых в файл формата Excel. Во всех найденных последовательностях к аварийной ситуации приводило полное открытие клапана № 1 (рис. 2). В режиме обучения постепенно происходило повышение веса действию «открытие клапана № 1» из-за связанного с ним повышения температуры в печи, после чего осуществлялся переход в режим применения накопленного опыта, где происходило полное открытие этого клапана. В среднем для обнаружения аварии алгоритму требовалось ~3500 шагов, что соответствует ~1,5 часам работы модели в режиме реального времени. Результаты экспериментальных исследований представлены в табл. 1

Таблица 1. Результаты экспериментальных исследований

№	Метод прямого перебора		Метод временных различий	
	Результат	Количество шагов	Результат	Количество шагов
1	Авария не найдена	10000	Авария найдена	7912
2	Авария не найдена	10000	Авария найдена	695
3	Авария не найдена	10000	Авария не найдена	10000
4	Авария не найдена	10000	Авария найдена	445
5	Авария не найдена	10000	Авария не найдена	10000
6	Авария не найдена	10000	Авария не найдена	10000
7	Авария не найдена	10000	Авария найдена	4512
8	Авария не найдена	10000	Авария не найдена	10000
9	Авария не найдена	10000	Авария не найдена	10000
10	Авария не найдена	10000	Авария найдена	3728

Результаты экспериментальных исследований подтверждают эффективность предлагаемого методического подхода в сравнении с методом прямого перебора возможных информационных воздействий.

Таким образом, в результате применения предлагаемого методического подхода установлено, что наиболее быстро (за 20–25 с) аварийная ситуация в печи, используемой на установке стабилизации нефти, достигается за счет полного (на 100%) открытия клапана № 1. Остальные последовательности действий (например, последовательное открытие клапанов № 7, № 8, № 9, № 1) приводят к аварийной ситуации за более длительное время (в среднем за 1,5–2 часа). Анализ найденных последовательностей позволяет определить наиболее быстро реализуемые, а значит наиболее опасные последовательности действий, приводящих к аварийным ситуациям, и, тем самым, выявлять наиболее опасные угрозы информационной безопасности, направленные на реализацию указанных последовательностей действий на промышленных объектах.

Заключение

Предлагаемый подход позволяет находить последовательности информационных воздействий, приводящих к аварийным ситуациям на промышленных объектах. Выявление таких последовательностей позволяет определить критические места в распределенной системе управления промышленным объектом, в отношении которых успешная реализация угроз безопасности информации может привести к аварийной ситуации на промышленном объекте.

Методический подход апробирован на модели установки стабилизации нефти, подтверждена его более высокая эффективность по сравнению с методом прямого перебора.

Дальнейшим направлением исследований является расширение номенклатуры установок на промышленных объектах, в отношении которых осуществляются различные угрозы безопасности информации, реализуемые через распределенную систему управления этими установками, а также выявление особенностей функционирования технологических установок, необходимых для учета при реализации разработанного методического подхода.

СПИСОК ЛИТЕРАТУРЫ:

1. Simulink – Simulation and Model-Based Design – MATLAB & Simulink: URL: https://www.mathworks.com/products/simulink.html (дата обращения: 12.02.2020).
2. Aspen HYSYS: URL: https://www.aspentech.com/products/engineering/aspen-hysys (дата обращения: 12.02.2020).
3. Petro-SIM | Process Simulation Software | KBC: URL: https://www.kbc.global/software/process-simulation-software/ (дата обращения: 12.02.2020).

4. Саттон Р.С., Барто Э.Г. Обучение с подкреплением: Пер. с англ. М.: БИНОМ. Лаборатория знаний, 2011. – 399 с.
5. Комашинский В.И., Смирнов Д.А. Нейронные сети и их применение в системах управления и связи: М.: Горячая линия – Телеком, 2003. – 94 с.
6. Deep Learning: URL: https://www.deeplearningbook.org (дата обращения: 12.02.2020).
7. Что не так с обучением с подкреплением (Reinforcement Learning)? / Хабр.: URL: https://habr.com/ru/post/437020/ (дата обращения: 12.02.2020).
8. Введение в обучение с подкреплением для начинающих: URL: https://proglib.io/p/reinforcement-learning/ (дата обращения: 12.02.2020).
9. Обучение с подкреплением для самых маленьких / Хабр.: URL: https://habr.com/ru/post/308094/ (дата обращения: 12.02.2020).
10. Вьюгин В.В. Математические основы теории машинного обучения и прогнозирования: М.: 2013. – 387 с.
11. Домингос П. Верховный алгоритм. Как машинное обучение изменит наш мир. – М.: Манн, Иванов и Фербер, 2016. – 336 с.
12. Trevor Hastie, Robert Tibshirani, Jerome H. Friedman The Elements of Statistical Learning: Data Mining, Inference, and Prediction. - Springer Science & Business Media, 2001. – 533 с.
13. Хайкин С. Нейронные сети: полный курс, 2-е издание.: Пер. с англ. – М.: Издательский дом «Вильямс», 2006. – 1104 с.
14. Критерий согласия Пирсона χ2 (Хи-квадрат) - statanaliz.info: URL: https://statanaliz.info/statistica/proverka-gipotez/kriterij-soglasiya-pirsona-khi-kvadrat/ (дата обращения: 12.02.2020).
15. NIST SP 800-22: Documentation and Software - Random Bit Generation | CSRC: URL: https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software (дата обращения: 12.02.2020).

REFERENCES:

[1] Simulink – Simulation and Model-Based Design – MATLAB & Simulink. URL: https://www.mathworks.com/products/simulink.html (accessed: 12.02.2020).
[2] Aspen HYSYS URL: https://www.aspentech.com/products/engineering/aspen-hysys (accessed: 12.02.2020).
[3] Petro-SIM | Process Simulation Software | KBC. URL: https://www.kbc.global/software/process-simulation-software/ (accessed: 12.02.2020).
[4] Sutton Richard S., Barto Andrew G. Reinforcement Learning: An Introduction. The MIT Press, 2014. – 338 p.
[5] Komashinskiy V.I., Smirnov D.A. Neural networks and their application in control and communication systems: M.: Goryachaya liniya, Telekom, 2003 – 94 p. (in Russian).
[6] Deep Learning. URL: https://www.deeplearningbook.org (accessed: 12.02.2020) (in Russian).
[7] What's wrong in machine learning with reinforcement (Reinforcement Learning)? / Habr.: URL: https://habr.com/ru/post/437020/ (accessed: 12.02.2020) (in Russian).
[8] Introduction to machine learning with reinforcement for beginners. URL: https://proglib.io/p/reinforcement-learning (accessed: 12.02.2020) (in Russian).
[9] Machine learning with reinforcement for the youngest Habr.: URL: https://habr.com/ru/post/308094/ (accessed: 12.02.2020) (in Russian).
[10] Viyugin V.V. Mathematical foundations of machine learning and forecasting theory: M.: 2013. – 387 p. (accessed: 12.02.2020) (in Russian).
[11] Domingos P. The Supreme algorithm. How machine learning will change our world. M.: Mann, Ivanov i Ferber, 2016. – 336 p. (accessed: 12.02.2020) (in Russian).
[12] Trevor Hastie, Robert Tibshirani, Jerome H. Friedman The Elements of Statistical Learning: Data Mining, Inference, and Prediction. Springer Science & Business Media, 2001. – 533 p.
[13] Haykin S. Neural Networks: A Comprehensive Foundation, Second Edition. – Prentice Hall, Inc., 2006. – 823 p.
[14] Pearson's consent criterion χ2 (chi-square test) - statanaliz.info. URL: https://statanaliz.info/statistica/proverka-gipotez/kriterij-soglasiya-pirsona-khi-kvadrat/ (accessed: 12.02.2020) (in Russian).
[15] NIST SP 800-22: Documentation and Software - Random Bit Generation | CSRC. URL: https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software (accessed: 12.02.2020) (in Russian).

Поступила в редакцию – 04 февраля 2020 г. Окончательный вариант – 29 февраля 2020 г.
Received – February 04, 2020. The final version – February 29, 2020.