КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ
COMPUTER SIMULATION HISTORY

УДК 519.24
DOI 10.18413/2687-0932-2020-47-2-354-361

О САМООБУЧАЮЩИХСЯ МАШИННЫХ СИСТЕМАХ В ПРОЦЕССЕ АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ БАНКОМАТОВ

ABOUT SELF-LEARNING MACHINE SYSTEMS IN THE PROCESS OF AUTHORIZATION OF USERS OF ATMs

М.В. Бирюков, Н.А. Климова, Т.В. Гостищева
M.V. Biryukov, N.A. Klimova, T.V. Gostishcheva

Белгородский университет кооперации, экономики и права,
Россия, 308023, г. Белгород, ул. Садовая, д. 116а

Belgorod University of Cooperation, Economics &Law ,116a, Sadovaya Street, Belgorod, 308023, Russia

E-mail: briu@ya.ru, natalya.zadorojnaia@yandex.ru, gtv432@mail.ru

Аннотация
Целью данной статьи является дополнение комплекса мер безопасности, направленных на предотвращение мошеннических действий в процессе авторизации клиентов банкоматов и платежных терминалов. Необходимость исследования проблемы безопасности банкоматов в процессе авторизации клиентов обусловлена тем, что процент мошенничеств и хищений средств банкоматов не снижается, и на каждое средство повышения безопасности появляются меры противодействия мошенников. В связи с тем, что временной интервал между появлением нового мошеннического алгоритма и появлением средства противодействия ему все еще высок, мы видим необходимость создания и внедрения самообучающихся машинных алгоритмов в процессе авторизации клиентов банкоматов. В работе предложен алгоритм создания программного обеспечения онлайн-мониторинга авторизации клиентов на базе искусственного интеллекта. В ходе исследования использовались общенаучные методы (наблюдение, сравнение); экономико-статистические методы обработки данных (группировка, сравнение, анализ воздействия на бизнес (BIA)), анализ причин и следствий, техническое обслуживание, направленное на обеспечение надежности. Результатом исследования является алгоритм создания ПО, анализирующего легитимность авторизации клиентов банкоматов, обоснование целесообразности его применения.

Abstract
The purpose of this article is addition of security measures, which aimed at preventing fraud in ATM customers authorizing and payment terminals. Necessityof the ATM security problems studingin ATM users authorization is due to the fact that the percentage of fraud and embezzlement of ATMs is not reduced, and countermeasures are introduced for each means of improving security. Due to the fact that the time interval between the emergence of a new fraudulent algorithm and the appearance of a countermeasure to it is still high, we see the need to create and implement self-learning machine algorithms in the process of authorizing ATM clients.The article proposes an algorithm for creating software for online monitoring of client authorization based on artificial intellect. The study used general scientific methods (observation, comparison); economic statistical data processing methods (grouping, comparison, business impact analysis (BIA)), cause and effect analysis, maintenance activities designed to ensure reliability. The result of the study is an algorithm for creating software that analyzes the legitimacy of authorization of ATM customers, the rationale for the expediency of its use.

Ключевые слова: информационная безопасность; банковские карты; искусственный интеллект; платёжные системы; авторизация; самообучающиеся машины.
Keywords: information security; bank cards;artificial intelligence; payment systems; authorization; self-learning machines.

Введение

Необходимость исследования проблемы использования банковских карт обусловлена тем, что они являются важнейшей тенденцией развития технологии безналичных расчетов в банковской сфере. Банковские карты предоставляют как физическим, так и юридическим лицам множество преимуществ. Среди этих преимуществ можно выделить удобство, надежность, практичность, минимальные временные затраты и экономия живого труда [Вахитов, Силич, 2010]. Рынок пластиковых карт переживает важный момент своего развития. От элитных, доступных лишь высокооплачиваемым категориям населения, пластиковые карты превращаются в достаточно демократичное средство расчетов. Производство банковских карт позволяет интегрироваться в мировую систему банковских услуг, поднять деловой имидж банка, завоевать рынок и привлечь клиентуру, дает возможность овладеть новейшими банковскими технологиями, увеличить скорость расчетов, исключить ошибки и злоупотребления со стороны банковских служащих [Гладких, 2010].

Однако пластиковые карты, являясь удобным способом доступа к деньгам на карточном счете, неизбежно становятся и объектом внимания злоумышленников [Акулич, 2011]. Так, например, по данным аналитического центра Zecurion, за январь – июнь 2018 года злоумышленники похитили с помощью скимминга 1000 млн рублей, с помощью фишинга – 170 млн рублей. **Целью** данной статьи является дополнение комплекса мер безопасности, направленных на предотвращение мошеннических действий по банковским картам клиентов с помощью дополнительных средств анализа аутентификации клиентов.

В ходе исследования использовались общенаучные **методы** (наблюдение, сравнение); экономико-статистические методы обработки данных (группировка, сравнение, анализ воздействия на бизнес (BIA)), анализ причин и следствий, техническое обслуживание, направленное на обеспечение надежности.

Результатом исследования является алгоритм создания ПО, анализирующего легитимность авторизации клиентов банкоматов, обоснование целесообразности его применения.

Целесообразность использования систем самообучающегося интеллекта в банковской сфере

К 2019 году в большинстве отраслей бизнеса и коммерции растет доля применения технологий на базе самообучающихся машинных систем или искусственного интеллекта (далее ИИ). За последние 5 лет доля финансирования ИИ-отрасли в мире увеличилась десятикратно и подошла к отметке в 3,5 млрд долларов [Жихарев и др., 2014]. Лидерами финансирования ИИ-отрасли является КНР и США, ощутимые прорывы в области самообучающихся систем и их внедрения в коммерческую отрасль произошли в Японии, Южной Корее и ряде стран Западной Европы. На сегодняшний день в области ИИ происходит эволюционный и революционный скачок, результатом которого станет вытеснение традиционных технологий и алгоритмов, используемых в бизнесе, на ИИ-технологии [Ефимов, Якимов, 2009]. В перспективе ближайших пяти лет речь идет о 30-процентном замещении вспомогательных бизнес-структур, в том числе автоматизации ряда профессий и полного отказа от человеческого труда в ряде направлений. На сегодняшний день риски апробации и внедрения ИИ-технологий становятся меньше каждый месяц, т. к. от накопительного и экспериментального процесса данная технология пришла к качественному и более «точечному» применению. Сформировалась так называемая база универсальных ИИ-алгоритмов, чье применение возможно в разнообразных сферах с несущественными

преобразованиями. Так например, разработанный в 2015 году российской компанией N-Tech.Lab алгоритм FaceN предложил универсальную систему распознавания лиц, применение которой возможно в подавляющем количестве систем авторизации пользователей. Красноречивым примером может быть разработка отечественной компании DigitalGenius, позволяющая полностью автоматизировать переписку, информационный чат между клиентами и компанией [Жихарев и др., 2016].

Если говорить о финансовых выгодах применения в сфере банковского обслуживания, то они неоспоримы в силу того, что единообразные вложения в создание ИИ-алгоритма позволят использовать полученный продукт неограниченное количество времени без дальнейших затрат на амортизацию, при этом сокращая расходы на персонал, аренду помещений и избегая рисков человеческого фактора. На данный момент стоимость разработки оригинального ИИ-алгоритма колеблется в широком диапазоне, где одна и та же услуга может быть оценена с разностью в 10 раз [Егоров и др., 2018], в силу большого предложения от разработчиков компаний различных стран. Так разработка уникального распознавателя лиц может стоить до 100 тыс. долларов США, а распознаватель лиц, компилирующий уже созданные алгоритмы, может обойтись и в 1000 долларов [Жихарев, Маторин, 2014]. Стоимость ИИ-алгоритма определяется рядом факторов, среди которых:

1. Уникальность разработки;
2. Необходимость переоснащения технического оборудования;
3. Объем вводимых данных для анализа ИИ. [Бегунов и др., 2010]

ИИ-алгоритмы, использующие прошлые разработки и не требующие технологического дооборудования, минимальны в цене (сотни долларов), их предложение существенно превышает спрос.

Красноречиво выглядят перспективы использования ИИ в финансовой сфере (рис.1) на период ближайших пяти лет.

Рис. 1. Оценка влияния технологии ИИ в течении пяти лет в финансовой сфере (% респондентов)
Fig. 1. Assessment of the impact of AI technology for five years in the financial sector (% of respondents)

ИИ-технологии могут применяться (в ряде стран уже применяются) в следующих сферах банковского обслуживания:

1. Чат-боты и робоэдвайзинг (автоматизированные справочные системы);
2. IoT (InternetofThings) (автоматизация приобретения услуг и товаров);
3. Антифрод. Нейтрализация внешних и инсайдерских угроз;
4. Повышение операционной эффективности;
5. Оптимизация коллекторской деятельности;
6. Повышение надежности авторизации клиентов [Гаврилова, 2016].

На последнем пункте данного списка мы более подробно остановимся в следующей части нашей работы.

Использование ИИ для выявления мошеннических действий пользователей банкоматов

Безусловно, лучшей авторизацией клиента является незаметная для него авторизация. Кроме стандартной паролевой (ввод пин-кода) авторизации клиентов банкомата существует и активно используется ряд биометрических способов подтверждения личности:

- Сканирование сетчатки глаза;
- Авторизация по отпечатку пальца или ладони;
- Анализ венозного рисунка;
- Трехмерное сканирование лица;
- Голосовая авторизация и пр. [Дюк и др., 2011].

Любой способ биометрической авторизации имеет несложные способы его обхода [Асадуллаев, 2017]. На сегодняшний день возможно воссоздать трехмерную копию лица с помощью 3D-принтера и существующего программного обеспечения, создающего 3D-маску по ряду двумерных фотографий (которые, как правило можно скопировать из аккаунтов социальных сетей). Именно поэтому остро стоит разработка универсального ИИ для авторизации пользователя и, что важнее, анализирующего поведение клиента в режиме настоящего времени [Жихарев и др., 2015a].

Алгоритм самообучающегося ИИ авторизации клиентов банкоматов должен «самообучиться» таким образом, чтобы смог в режиме реального времени анализировать видеопоток с камер слежения и делать выводы о типичном и подозрительном поведении пользователя. На первом этапе работы для создания «библиотеки» подозрительного поведения ИИ необходимо предоставить видео с записями прошлых мошенничеств. Используя существующие методы распознавания контуров человека нужно предоставить возможность ИИ проанализировать поведение субъектов видео у банкомата, приведшие к мошенничеству или хищению средств из банкомата [Жихарев и др., 2015b]. Таким образом алгоритм ИИ создаст библиотеку подозрительной активности клиентов. На втором этапе разработки необходимо измерить эффективность алгоритма. Для этого нужно предоставить ряд неизвестных до этого видеозаписей мошенничеств и статистически измерить, в каком проценте из них ИИ посчитает поведение субъектов подозрительным. Общая схема этапов работы над алгоритмом ИИ представлена на рис. 2. Проанализировав результаты можно будет делать выводы об эффективности алгоритма и необходимости его дальнейшей доработки.

По нашим оценкам для разработки и создания данного алгоритма требуется база видеозаписей мошенничеств (которую возможно создать лишь существующим банкам и МВД РФ), насчитывающую более 1000 записей (для обеспечения погрешности в 0,1 %), сервер для написания и хранения кода, а также банкоматы, оснащенные достаточными вычислительными мощностями для работы алгоритма в режиме реального времени. Основным алгоритмом при написании программного продукта будет самостоятельный анализ видеозаписей при помощи утилиты распознавания контуров человека на предмет типичных поведенческих шаблонов. При этом алгоритму заранее будет известно – запечатлено ли на видеозаписи будущее хищение или это штатное обналичивание средств. Таким образом, алгоритм должен накопить «библиотеку признаков правонарушений» и в дальнейшем в режиме онлайн должен сопоставлять данные признаки с реальным потоком видео с целью прогнозирования поведения клиента. В случае негативного прогноза алгоритм в кратчайшие сроки

(до 8–10 секунд, для этого соответствующий софт должен быть установлен в ОС банкомата, в случае удаленного сканирования временной интервал может быть излишним, ввиду зависимости от интернет-трафика) блокирует или отменяет операции клиента и сообщает о дальнейшей невозможности работы терминала.

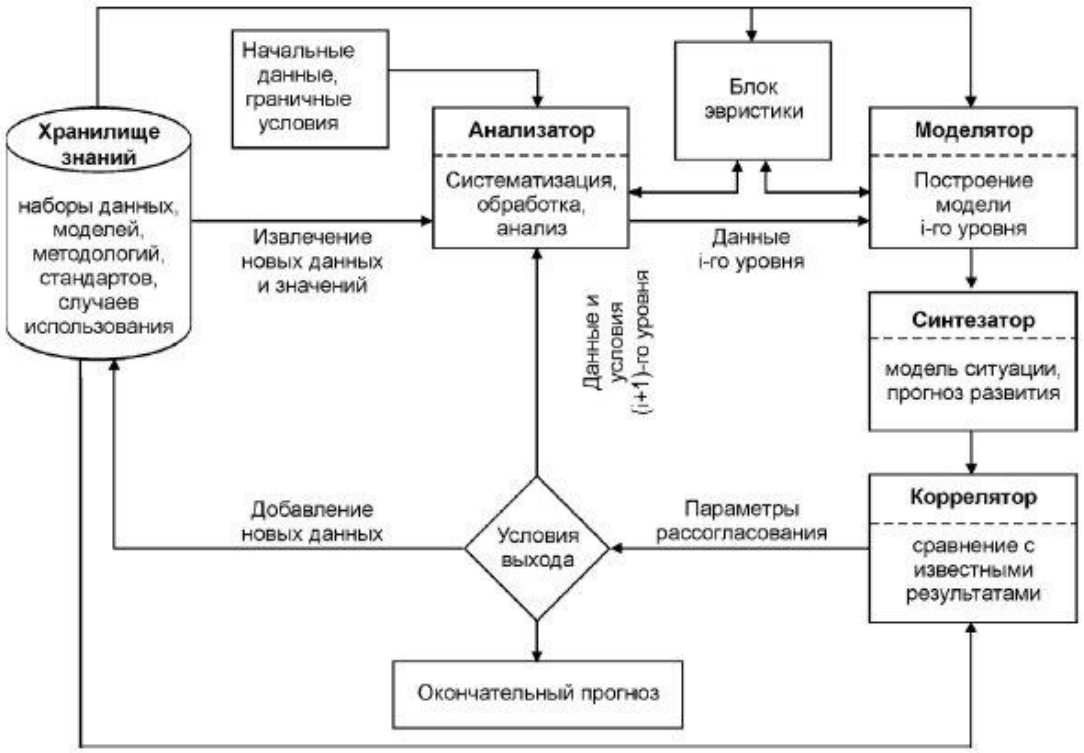

Рис. 2. Схема работы алгоритма ИИ, анализирующего авторизацию клиентов банкоматов
Fig. 2. The scheme of operation of the AI algorithm, analyzing the authorization of ATM customers

На сегодняшний день оценить стоимость затрат на создание и апробацию подобного алгоритма можно лишь с высокой степенью приблизительности, и это сумма порядка 50–100 тысяч долларов. Однако необходимость разработки подобного ПО очевидна и является лишь вопросом скорейшего времени. Для разработки данного алгоритма самым ценным ресурсом является библиотека видеозаписей, сделанных с банкоматов и запечатлевших не менее 1000 фактов мошенничества. Стоимость оборудования для написания алгоритма не превышает нескольких тысяч долларов. Необходим персонал в виде штата программистов (5–10 человек), имевших опыт написания ИИ ПО, и временной ресурс от месяца до полугода для тестирования и апробации ПО.

Использование контурного анализа в алгоритме авторизации

Уже два десятилетия применяются системы распознавания и визуальные интерпретаторы. Исходя из особенностей систем видеонаблюдения (невысокая частота кадров, стационарное расположение, низкое разрешение, отсутствие зума и пр.) для компиляции анализатора изображений оптимально использование метода активных контуров движущегося изображения Дж. Кэнни [Жихарев и др., 2013].

Растр границы $(\mathbf{x_0}, \mathbf{y_0})$, расположенный в примыкающей области $(\boldsymbol{x}, \boldsymbol{y})$, определяется как исходный $(\boldsymbol{x}, \boldsymbol{y})$ исходя из модуля градиента, если:

$$\nabla \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) - \nabla \boldsymbol{f}(\mathbf{x_0}, \mathbf{y_0}) \leq \mathbf{E},$$

где E – установленный положительный порог, и по вектору градиента, если

$$\boldsymbol{\alpha(x, y) - \alpha(x_0, y_0) \leq A},$$

где $\boldsymbol{\alpha(x, y) = arctg \frac{\partial x}{\partial y}}$, А – заданный порог поворота.

Растр в данной площади объединяется с центральным $(\boldsymbol{x, y})$, при выполнении критериев значения и сходства. Данный процесс циклично повторяется в каждом растре изображения с фиксированием предыдущих связанных растров при движении условного центра площади.

Алгоритм Кэнни включает в себя:

- размытие картинки в пределах выделенного контура для сокращения шума;
- градиентный поиск (отметка наличия границ при максимальном градиенте);
- подавление краев несвязанных с однозначно выявленными границами;
- определение потенциальных границ с помощью двойной пороговой фильтрации.

Главным недостатком метода Кэнни является невозможность задачи контуров при однородных цветах объектов или объектах с высокой градиентной составляющей.

Рис. 3. Пример определения контуров с помощью алгоритма Кэнни
Fig. 3. An example of determining the contours using the Canny algorithm

Для уменьшения вычислительной нагрузки и сокращения времени анализа нами предлагается с условным интервалом (утром, до начала «рабочего» дня, но при оптимальной освещенности) задавать кадр-эталон. Любые изображения в кадре, отличные от эталона, и должны подвергаться поведенческому анализу. Отличие кадров от эталонного дает возможность практически моментального выявления контуров новых объектов (в частности лиц, проходящих авторизацию, контуров тела и пр.) и применять к ним анализатор поведения, который будет сравнивать контурные маски и заданные поведенческие шаблоны правонарушений. Именно использование сравнения с эталонным изображением позволит безошибочно выявлять контуры объектов и нивелирует погрешности контуроопределения метода Кэнни.

Заключение

Из статистики известно, что в результате одного хищения банк теряет средства, сопоставимые с затратами на содержание банкомата и его стоимостью за несколько лет. Сумма среднего хищения банкомата в 2018 году составляла 150–200 тыс. руб. Исходя из этого, если поведенческий алгоритм позволит сократить процент хищений банкоматов хотя бы на 5–10 %, это позволит окупить его затраты к пятидесятому хищению. На сегодняшний день в РФ работает более 206 тысяч банкоматов, и по статистике каждый в среднем подвергается 2 попыткам взлома ежегодно. Следовательно, ПО подобного рода необходимо, а затраты на разработку и внедрение несопоставимы с возможными убытками. Если говорить о рисках, то главной возможной уязвимостью является сам программный продукт. С помощью внешнего изменения кода его работоспособность и функции можно изменить, но такие же риски несет

весь комплекс ПО банкоматов, т. е. в данном ключе риски остаются неизменны. Появление и внедрение программного обеспечения, анализирующего поведение клиентов, вопрос ближайших нескольких лет.

Список литературы

1. Акулич И.Л. 2011. Математическое программирование в примерах и задачах: учебное пособие. СПб., Издательство «Лань», 352.

2. Асадуллаев Р.Г., Ломакин В.В., Белоконь Ю.Ю., Зайцева Т.В., Резниченко О.С. 2017. Модели и средства поддержки принятия решений в системах переподготовки кадров предприятия Научные ведомости Белгородского государственного университета. Экономика. Информатика. 23 (272), вып. 44: 148–158.

3. Бегунов Н.А., Клебанов Б.И., Рапопорт И.А. 2010. Объединение подходов интеллектуального анализа данных и имитационного моделирования для прогнозирования доходов бюджета. Автоматизация и современные технологии, 12: 37–40.

4. Вахитов А.Р., Силич В.А. 2010. Использование нечеткого логического вывода для интеллектуального анализа данных. Известия Томского политехнического университета, 317 (5): 171–174.

5. Гаврилова Т.А., Кудрявцев Д.В., Муромцев Д.И. 2016. Инженерия знаний. Модели и методы. М., Издательство «Лань», 324.

6. Гладких Н.А. 2010. Оптимизация систем электронного документооборота на основе интеллектуального анализа данных. В мире научных открытий, 4 (11): 122–123.

7. Дюк В.А., Флегонтов А.В., Фомина И.К. 2011. Применение технологий интеллектуального анализа данных в естественнонаучных, технических и гуманитарных областях. Известия российского государственного педагогического университета им. А.И. Герцена, 138: 77.

8. Егоров И.А., Маторин С.И., Жихарев А.Г. 2018. Системно-объектное имитационное моделирование химических загрязнений подземных вод в горнопромышленном кластере. Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика, 45 (3): 510–523.

9. Ефимов С.Н., Якимов Л.С. 2009. Применение технологии нейронных сетей для интеллектуального анализа данных. Сборник научных трудов по материалам международной научно-практической конференции. 2 (2): 64–70.

10. Жихарев А.Г., Болгова Е.В., Гурьянова И.В., Маматова О.П. 2014. О перспективах развития системно-объектного метода представления организационных знаний. Научные ведомости Белгородского государственного университета. Сер. История. Политология. Экономика. Информатика, 1 (172): 110–114.

11. Жихарев А.Г., Корчагина К.В., Бузов П.А., Акулов Ю.В., Жихарева М.С. 2016. Об имитационном моделировании производственно-технологических систем. Сетевой журнал «Научный результат», серия «Информационные технологии», 3 (3): 25–31.

12. Жихарев А.Г., Маторин С.И. 2014. Системно-объектное моделирование технологических процессов. Научные ведомости Белгородского государственного университета. Сер. История. Политология. Экономика. Информатика, 21 (192): 137–142.

13. Жихарев А.Г., Маторин С.И., Зайцева Н.О. 2015. Системно-объектное имитационное моделирование транспортных и технологических процессов. Научные ведомости Белгородского государственного университета. Сер. История. Политология. Экономика. Информатика,7 (204): 159–170.

14. Жихарев А.Г., Маторин С.И., Зайцева Н.О. 2015. Системно-объектный инструментарий для имитационного моделирования технологических процессов и транспортных потоков. Искусственный интеллект и принятие решений, 4: 95–103.

15. Жихарев А.Г., Маторин С.И., Маматов Е.М., Смородина Н.Н. 2013. О системно-объектном методе представления организационных знаний. Научные ведомости БелГУ. Сер. Информатика, 8 (151): 137–146.

References

1. Akulich I.L. 2011. Mathematical programming examples and problems: a tutorial. SPb., LanPublishingHouse, 352. (in Russian)

2. Asadullaev R.G., Lomakin V.V., Belokon Y.Y., Zaitseva T.V., Reznichenko O.S. 2017. Models and methods of decision support in the information systems for requalification of employees. BelgorodStateUniversityScientificBulletin. Economics. Informationtechnologies. 23 (272), Issue 44: 148–158.

3. Begunov N.A. Klebanov B.I., Rapoport I.A. 2010. Combining the approaches of data mining and simulation modeling to predict future revenues. Automationandmoderntechnologies, 12: 37–40. (in Russian)

4. Vakhitov A.R., Silich V.A. 2010. The use of fuzzy inference for data mining. ProceedingsofTomskpolytechnicuniversity, 317 (5): 171–174. (in Russian)

5. Gavrilova T.A., Kudryavtsev, D.V., Muromtsev D.I. 2016. Knowledge Engineering. Models and methods. M., PublishingHouse "LAN", 324. (in Russian)

6. Gladkich N.A. 2010. Optimization of electronic document management systems based on data mining. Intheworldofscientificdiscoveries, 4 (11): 122–123. (in Russian)

7. Duke V.A., Flegontov A.V., Fomin I.K. 2011. The application of data mining technology in scientific, technical and humanitarian fields. Bulletin of the Russian State Pedagogical University. A.I. Herzen. (138): 77. (in Russian)

8. Yegorov I.A., Matorin S.I., Zhikharev A.G. 2018. System-object simulation modeling of chemical pollution of groundwater in the mining cluster. Belgorod State University Scientific Bulletin. Ser. Economics. Information technologies, 45 (3): 510–523 (in Russian).

9. Efimov S.N., Yakimov L.S. 2009. Application of neural network technology for data mining. Collection of scientific works on the materials of the international scientific-practical conference. 2 (2): 64–70. (in Russian)

10. Zhiharev A.G., Bolgova E.V., Gur'yanova I.V., Mamatova O.P. 2014. On the prospects for the development of a system-object method for representing organizational knowledge. Belgorod State University Scientific Bulletin. Ser. History. Political science. Economics. Information technologies, 1 (172): 110–114.

11. Zhikharev A.G., Korchagina K.V., Buzov P.A., AkulovYu.V., Zhikhareva M.S. 2016. On simulation modeling of production and technological systems. Network journal "Scientific result", a series of "Information technology", 3 (3): 25–31 (in Russian).

12. Zhiharev A.G., Matorin S.I. 2014. System-object modeling of technological processes]. Belgorod State University Scientific Bulletin. Ser. History. Political science. Economics. Information technologies, 21 (192): 137–142.

13. Zhiharev A.G., Matorin S.I., Zajceva N.O. 2015. System-object simulation of transport and technological processes. Belgorod State University Scientific Bulletin. Ser. History. Political science. Economics. Information technologies, 7 (204): 159–170.

14. Zhikharev AG, Matorin S.I., Zaitseva N.O. 2015. System-Object Tools for Simulation Modeling of Technological Processes and Transport Flows. Artificial Intelligence and Decision Making, 4: 95–103 (in Russian).

15. Zhiharev A.G., Matorin S.I., Mamatov E.M., Smorodina N.N. 2013. On a system-object method for representing organizational knowledge. Belgorod State University Scientific Bulletin. Ser. Economics. Informationtechnologies, 8 (151):137–146.

Ссылка для цитирования статьи
For citation

Бирюков М.В., Климова Н.А., Гостищева Т.В. 2020. О самообучающихся машинных системах в процессе авторизации пользователей банкоматов. Экономика. Информатика. 47 (2): 354–361. DOI: 10.18413/2687-0932-2020-47-2-354-361.

Biryukov M.V., Klimova N.A., Gostishcheva T.V. 2020. About self-learning machine systems in the process of authorization of users of ATMs. Economics. Information technologies. 47 (2): 354–361 (in Russian). DOI: 10.18413/2687-0932-2020-47-2-354-361.