http://dx.doi.org/10.35596/1729-7648-2025-31-2-77-83

УДК 004.8+159.942.33

ПРИМЕНЕНИЕ СИСТЕМ «УМНЫЙ ГОРОД» В МОНИТОРИНГЕ И УПРАВЛЕНИИ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТЬЮ

Е. М. КОСАРЕВА, Д. В. ЛИХАЧЕВСКИЙ, Т. В. КАЗАК, Д. Р. ТИУНЧИК

Белорусский государственный университет информатики и радиоэлектроники (Минск, Республика Беларусь)

Аннотация. В статье обосновано применение систем «умный город» в качестве инструмента мониторинга и управления общественной безопасностью. Описан метод распознавания и оценки потенциальных антропогенных угроз «умного города». Проведено обоснование выбора факторов, лежащих в основе оценки потенциальной опасности лиц, с учетом специфики применения метода в автоматизированных интеллектуальных системах предиктивной аналитики и интеллектуального видеонаблюдения в «умном городе». Описаны результаты разработки прототипа интеллектуальной системы. Проведена оценка точности ее работы.

Ключевые слова: психоэмоциональное состояние, распознавание эмоций, антропогенные угрозы, «умный город», сверточные нейронные сети, интеллектуальное видеонаблюдение, предиктивная аналитика.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Применение систем «умный город» в мониторинге и управлении общественной безопасностью / Е. М. Косарева [и др.] // Доклады БГУИР. 2025. Т. 31, № 2. С. 77–83. http://dx.doi.org/10.35596/1729-7648-2025-31-2-77-83.

APPLICATION OF SMART CITY SYSTEMS IN PUBLIC SAFETY MONITORING AND MANAGEMENT

EKATERINA M. KOSAREVA, DMITRY V. LIKHACHEVSKY, TAMARA V. KAZAK, DANIIL R. TIUNCHIK

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Abstract. The article substantiates the use of “smart city” systems as a tool for monitoring and managing public safety. A method for recognizing and assessing potential anthropogenic threats to a “smart city” is described. The choice of factors underlying the assessment of the potential danger of individuals is substantiated, taking into account the specifics of the method’s application in automated intelligent systems of predictive analytics and intelligent video surveillance in a “smart city”. The results of developing a prototype of an intelligent system are described. The accuracy of its operation is assessed.

Keywords: psycho-emotional state, emotion recognition, anthropogenic threats, “smart city”, convolutional neural networks, intelligent video surveillance, predictive analytics.

Conflict of interests. The authors declare no conflict of interests.

For citation. Kosareva E. M., Likhachevsky D. V., Kazak T. V., Tiunchik D. R. (2025) Application of Smart City Systems in Public Safety Monitoring and Management. *Digital Transformation.* 31 (2), 77–83. http://dx.doi.org/10.35596/1729-7648-2025-31-2-77-83 (in Russian).

Введение

Возникновение новых парадигм общественного развития влечет за собой качественные изменения во всех сферах функционирования белорусского государства. С 2021 г. в Беларуси взят курс на развертывание процессов цифровой трансформации. Сегодня концепция цифровой трансформации реализуется в рамках Программы социально-экономического развития Республики Беларусь на 2021–2025 гг. (далее – Программы). В соответствии с Программой, одной из задач является создание отраслевых и региональных цифровых платформ, а также внедрение технологии «умных городов» во всех регионах страны, в первую очередь в областных центрах [1].

При внедрении «умных городов» первостепенную важность имеют сопутствующие системы обеспечения безопасности, которые обрабатывают поступающие данные в режиме реального времени. И они уже используются для прогнозирования мест и времени возможных преступлений [2]. Кроме того, сами по себе «умные города» могут выступать в качестве средства повышения уровня общественной безопасности [3].

Автоматизация процесса распознавания потенциальных антропогенных угроз при помощи «умных городов» ведет к переходу от фиксации совершенных правонарушений к аналитике реального времени и предиктивной аналитике, которые позволяют выявить и предотвратить антропогенные угрозы до момента их реализации. Согласно [4], ключевую роль в распознавании антропогенных угроз играют оценка текущего психоэмоционального состояния потенциально опасного лица, а также идентификация его предшествующего криминального опыта. Обе эти задачи могут быть успешно решены при помощи интеллектуальных систем видеонаблюдения, активно применяющихся в «умных городах» [5].

В статье описан метод оценки потенциальной опасности лица с учетом специфики его применения в системе интеллектуального видеонаблюдения, а также проведена оценка точности интеллектуальной системы, реализующей данный алгоритм.

Метод оценки антропогенных угроз

Антропогенные угрозы представляют собой группу потенциальных угроз «умного города», которые являются результатом реализации социальной опасности отдельных лиц или групп. Социальная опасность личности развивается чаще всего до момента совершения деяния. Постепенное формирование такой опасности обычно проявляется в асоциальном поведении конкретного лица – административных, дисциплинарных правонарушениях, безнравственных действиях, не имеющих пока еще характера преступления [6]. Таким образом, крайне важно применять инструменты предиктивной аналитики для распознавания лиц с высоким уровнем социальной опасности для предотвращения реализации антропогенных угроз [5]. Внедрение «умных городов» позволяет автоматизировать эти процессы, обеспечивая при этом более высокую точность и скорость распознавания по сравнению с неавтоматизированными методами.

С учетом специфики средств реализации интеллектуальной системы распознавания в качестве основы для оценки потенциальной опасности предлагается использовать те параметры, которые возможно однозначно представить в виде числовой величины или зафиксировать с помощью средств видеонаблюдения. Кроме того, выбранные параметры в совокупности должны наиболее полно определять уровень потенциальной опасности лица.

В рамках предлагаемой методики оценка потенциальной опасности лица может производиться на основании психоэмоционального состояния, а также наличия/отсутствия предыдущего криминального опыта. Привлечение к уголовной ответственности в прошлом является основной предпосылкой реализации социальной опасности лица. Это обусловлено психологической сущностью рецидива, определяющей повышенную опасность личности виновного. Отсюда следует, что при оценке потенциальной опасности лица данный фактор имеет больший вес. Задача оценки этого фактора сводится к решению задачи идентификации личности. Идентификация личности человека производится при помощи алгоритма распознавания лиц и сопоставления полученного вектора признаков с имеющейся базой данных лиц. Нейронная сеть, решающая задачу идентификации личности, позволяет получить бинарное значение фактора криминального прошлого лица: 1 – лицо совершало противоправные поступки, 0 – подобный опыт отсутствует.

Согласно исследованию [4], внешние проявления психологических состояний, ведущих к реализации социальной опасности, по своей мимической структуре соответствуют таким эмо-

циям, как гнев, страх и нейтральная. Применимо к автоматизированной системе данный фактор может быть оценен посредством нейронной сети, решающей задачу распознавания эмоций в видеопотоке. В результате решения данной задачи будет получен вектор процентов соответствия выражения лица каждой из эмоций, из которого будут выделены значения интересующих эмоций. Значение фактора проявления специфических признаков (MSS – Manifestation of Specific Signs) в психологическом профиле рассчитывается по формуле

$$\mathrm{MSS} = \frac{\sum v_i}{100}, \tag{1}$$

где v_i – степень проявления эмоции (гнева, страха и нейтральной).

В отличие от предшествующего криминального опыта, фактор текущего психоэмоционального состояния имеет меньший вес при расчете общего показателя потенциальной опасности. Это объясняется тем, что в контексте интеллектуальной системы психоэмоциональное состояние оценивается только по внешним признакам, что может частично снизить достоверность результатов. В табл. 1 приведены весовые коэффициенты для каждого из факторов, определяющих потенциальную опасность лица.

Таблица 1. Весовые коэффициенты для факторов оценки
Table 1. Weighting factors for evaluation factors

Фактор	Весовой коэффициент α_i
Привлечение к уголовной ответственности в прошлом	0,6
Проявление специфических признаков (MSS) в психологическом профиле	0,4

Интегральный показатель потенциальной опасности (PHI – Potential Hazard Indicator) лица рассчитывали по формуле

$$\mathrm{PHI} = \sum_{\alpha_i y_j}, \tag{2}$$

где α_i – нормированный весовой коэффициент; y_j – значение фактора.

Результатом оценки является численный показатель $\mathrm{PHI} \in [0; 1]$, который может быть представлен в процентном соотношении. PHI, колеблющийся в интервале от 0,35 до 0,60, свидетельствует о высокой потенциальной опасности лица [4]. Описанный метод лежит в основе прототипа автоматизированной системы распознавания потенциальных антропогенных угроз.

Модель для оценки факторов потенциальной опасности антропогенных угроз

Для оценки факторов потенциальной опасности лица обученная модель, лежащая в основе интеллектуальной системы, решает две задачи: оценки психоэмоционального состояния лица и распознавания лица (определение наличия/отсутствия предыдущего криминального опыта). Разработанная система состоит из следующих функциональных блоков:

– входной видеопоток от камеры;
– блок детекции лиц (dlib);
– модуль распознавания эмоций (дообученная модель FER + постобработка);
– модуль сравнения лиц (face descriptors с порогом 0,6);
– интерфейс визуализации.

Схематично структура системы представлена на рис. 1.

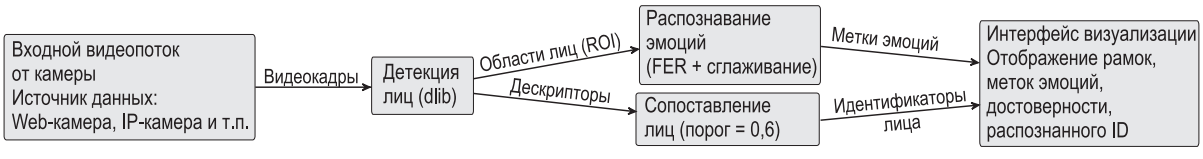

Рис. 1. Блок-схема потока данных
Fig 1. Data flow diagram

Логика работы системы для распознавания эмоций строится на последовательной обработке входного видеопотока и работает по следующему алгоритму.

1. Определение лица в кадре. Выделяется регион изображения, содержащий лицо, с помощью детектора лиц. Сначала видеопоток захватывается с камеры (для этого применяется модуль camera.py, в котором паттерн Singleton гарантирует, что камера создается и управляется единственным экземпляром объекта). Далее каждое изображение кадра передается на детектор лиц, основанный на dlib: библиотеке, предоставляющей метод get_frontal_face_detector(), который находит координаты лиц в кадре.

2. Считывание и классификация эмоции. Используется нейронная сеть, которая возвращает вектор вероятностей по каждому классу эмоций. Особый интерес представляют отрицательные эмоциональные состояния (гнев, страх) и нейтральное выражение лица, поскольку они коррелируют с потенциально «опасным» профилем (агрессия, ригидность, возбудимость). Для каждого обнаруженного лица формируется вырезанный фрагмент (ROI – Region of Interest) и передается в модуль распознавания эмоций FER. Дообученная модель FER, лежащая в основе данного модуля, использует сверточные фильтры для анализа изображения, извлекает высокоуровневые признаки (изгибы губ, положение глаз, нахмуренность бровей и т. д.) и на выходе выдает вектор вероятностей для каждого класса эмоций. Затем выбирается эмоция с наибольшим значением вероятности в качестве итоговой. Дополнительно, чтобы избежать скачкообразных изменений, применяется сглаживание (post-processing).

3. Сопоставление с базой данных. Происходит сравнение выделенного лица с записями в базе, где хранятся сведения о лицах, представляющих потенциальную угрозу по установленным критериям. Помимо определения эмоции, система параллельно решает задачу идентификации лиц. Для этого используется механизм генерации дескрипторов лиц (face descriptors), который также предоставляет dlib. Сформированное векторное представление (128-мерный вектор) сравнивается с заранее вычисленными дескрипторами эталонных лиц, хранящихся в локальной базе. Если евклидово расстояние между векторами не превышает заданный порог (например, 0,6), система считает, что лицо уже присутствует в базе, и выводит соответствующую информацию. Так достигаются одновременная идентификация человека и определение его эмоционального состояния.

4. Расчет показателя потенциальной опасности лица. На основании полученной информации вычисляется интегральный PHI. Если PHI превышает пороговое значение 0,6, то система классифицирует человека как потенциально опасного. В пользовательском интерфейсе визуализируется итоговый процент опасности: низкий (до 0,6) – зеленым цветом, высокий (более 0,6) – красным. Для иллюстрации работы системы на рис. 2 представлен скриншот интерфейса системы.

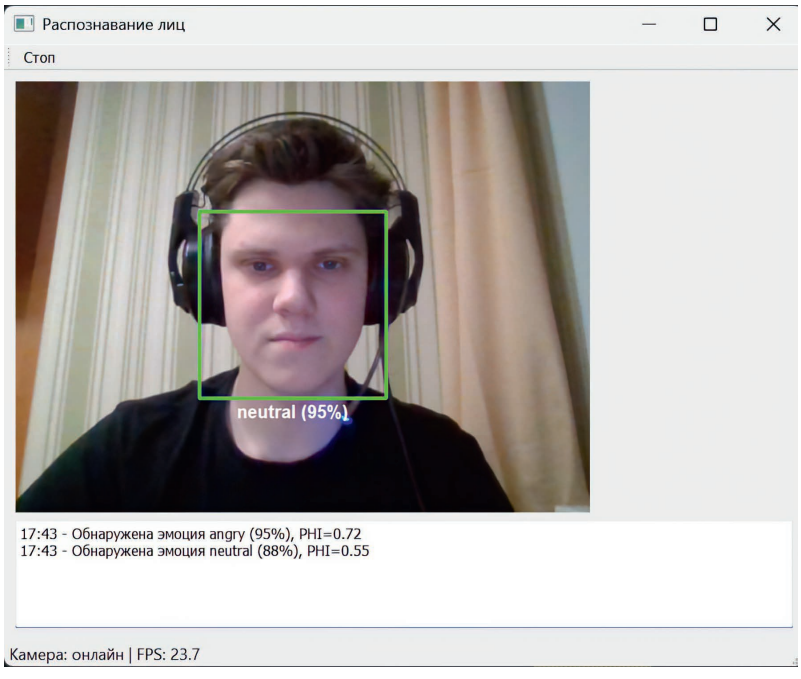

Рис. 2. Интерфейс программного средства
Fig. 2. Software interface

Для проверки точности работы интеллектуальной системы формировалась тестовая выборка из примерно 300 изображений, в которой сбалансированно представлены все семь классов эмоций. Каждое изображение «размечивалось» вручную, т. е. было указано, какая эмоция на самом деле представлена на изображении. Процесс тестирования включал следующие шаги:

– автоматическая детекция лиц в каждом тестовом изображении;

– распознавание эмоции;

– сопоставление предсказания и эталонной разметки;

– подсчет метрик (Accuracy, Precision, Recall, F1-score).

Для идентификации лиц использовалась отдельная методика сравнения дескрипторов. В демонстрационной среде модель сравнивала полученные векторы с примерами. Если евклидово расстояние оказывалось меньше 0,6, лицо считалось идентифицированным.

В исходном виде FER поставляется с предобученными весами, полученными на крупных публичных датасетах (включающих десятки тысяч изображений людей с выраженными эмоциями). Однако для уточнения модели под конкретные условия в настоящем исследовании была сформирована дополнительная выборка, включающая около 300 фотографий с различными эмоциями. Эти изображения были либо сняты в условиях офисного освещения, либо взяты из публичных источников с целью повысить вариативность (разные ракурсы, возрастные группы, цветовая гамма и т. д.). Для проведения fine-tuning выборку разбивали на три части:

– обучающая (training) – около 70 % изображений;

– валидационная (validation) – 20 %;

– тестовая (test) – 10 %.

При этом для валидации и теста особое внимание уделялось тому, чтобы в набор попали как «простые» фото (лицо анфас, нормальное освещение), так и более «сложные» (разные наклоны головы, мимика, аксессуары вроде очков). Тем самым обеспечивалась большая обобщающая способность модели. Дообучение модели проводилось согласно следующему алгоритму:

– загрузка предобученой модели (FER);

– заморозка части слоев (base_layers);

– разморозка последних слоев и обучение на своих данных с постепенной корректировкой весов;

– указание оптимизатора (например, Adam) и функции потерь (categorical crossentropy);

– разбиение данных на обучающую и валидационную выборки, обучение в течение 10 эпох с использованием EarlyStopping, чтобы не допустить переобучения;

– сохранение итоговой модели.

На практике выбор количества эпох и гиперпараметров зависит от объема данных и аппаратных возможностей. В рассматриваемом случае при использовании около 300–500 собственных изображений достаточно 5–10 эпох, чтобы донастроить высшие слои нейронной сети.

На рис. 3 изображены кривые обучения (training accuracy vs. validation accuracy) и кривые потерь. Данные графики иллюстрируют, как модель «учится» и после какой эпохи достигается плато точности.

По результатам анализа эффективности работы двух ключевых модулей системы – идентификации лиц (dlib-дескрипторы) и распознавания эмоций (модель FER с дообучением) – были сделаны следующие выводы:

– тестовая выборка (300 изображений) позволила зафиксировать точность распознавания эмоций на уровне 87–90 % при дообучении (fine-tuning) базовой модели FER на локальном датасете, учитывающем различные углы съемки и условия освещения;

– наиболее часто ошибки наблюдались при распознавании классов fear и surprise, чьи мимические паттерны схожи;

– в задаче идентификации лиц точность достигала 92 % для фронтального ракурса и снижалась до 80–85 % при значительных поворотах головы.

Система, реализованная на современном аппаратном обеспечении, обрабатывает видеопоток с практической скоростью в реальном времени. Это важно для анализа потенциальной опасности, поскольку дает возможность одновременно учитывать все факторы потенциальной опасности лица, что подтверждает актуальность применения предложенной методики в рамках «умного города».

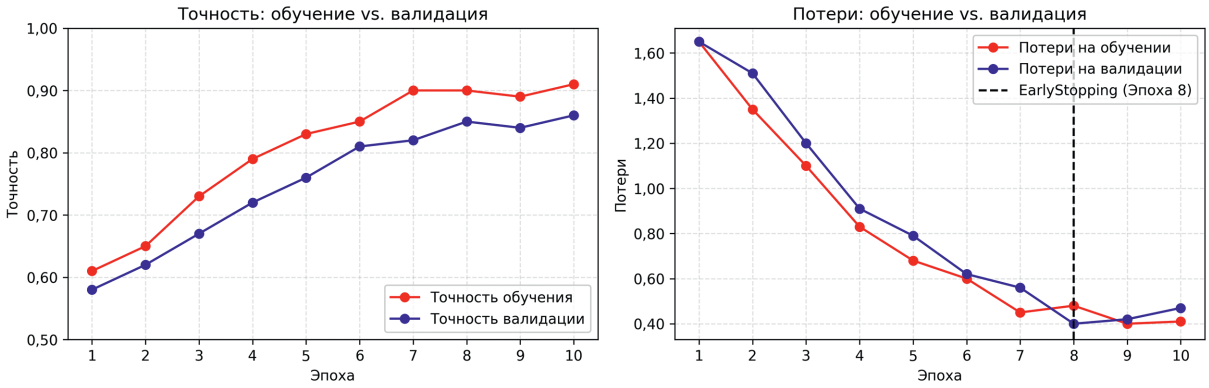

Рис. 3. Точность и потери при дообучении модели FER
Fig. 3. Accuracy and loss during retraining of the FER model

Заключение

1. «Умный город» как система мониторинга общественной безопасности позволяет существенно повысить уровень безопасности населения за счет применения технологий предиктивного распознавания потенциальных угроз, в том числе антропогенных.

2. Применение предлагаемой автоматизированной интеллектуальной системы позволяет одновременно оценивать несколько факторов, влияющих на реализацию социальной опасности с высокой точностью. Результаты экспериментов демонстрируют перспективность и практическую применимость данного подхода для систем интеллектуального видеонаблюдения и предиктивной аналитики в рамках «умного города».

Список литературы

1. Об утверждении Программы социально-экономического развития Беларуси на 2021–2025 годы: Указ Президента Республики Беларусь от 29 июля 2021 г. № 292 [Электронный ресурс]. Режим доступа: https://pravo.by/document/?guid=3871&p0=P32100292. Дата доступа: 01.04.2025.
2. Шаталова, В. В. Большие данные: как технологии Big Data меняют нашу жизнь / В. В. Шаталова, Д. В. Лихачевский, Т. В. Казак // BIG DATA и анализ высокого уровня: сб. науч. ст. VII Междунар. науч.-практ. конф., г. Минск, 19–20 мая 2021 г. Минск: Бестпринт, 2021. С. 188–192.
3. Косарева, Е. М. «Умный» город как система мониторинга общественной безопасности / Е. М. Косарева, Д. В. Лихачевский // Искусственный интеллект в Беларуси: III форум IT-Академграда, г. Минск, 10–11 окт. 2024 г. Минск: Объед. ин-т проблем информ. Нац. акад. наук Беларуси, 2024. С. 162–166.
4. Косарева, Е. М. Признаки потенциально опасных лиц как одной из угроз в системах «умного» города / Е. М. Косарева, Д. В. Лихачевский // Современные проблемы радиоэлектроники и телекоммуникаций: сб. науч. тр. № 7. М.-Севастополь: Изд-ва РНТОРЭС им. А. С. Попова, СевГУ, 2024.
5. Косарева, Е. М. Методы машинного обучения для распознавания потенциальных антропогенных угроз в системах «умного» города / Е. М. Косарева, Д. В. Лихачевский // Цифровая среда: технологии и перспективы. DETP 2024: сб. матер. II Междунар. науч.-практ. конф., г. Брест, 31 окт.–1 нояб. 2024 г. Брест: Брест. гос. техн. ун-т, 2024. С. 86–90.
6. Васильев, Л. В. Юридическая психология, 6-е изд. / Л. В. Васильев. СПб.: Питер, 2009.

Поступила 07.04.2025 Принята в печать 05.05.2025 Доступна на сайте 10.07.2025

References

1. On Approval of the Program for the Socio-Economic Development of Belarus for 2021–2025. *Decree of the President of the Republic of Belarus dated July 29, 2021 No 292*. Available: https://pravo.by/document/?guid=3871&p0=P32100292 (Accessed 1 April 2025) (in Russian).
2. Shatalova V. V., Likhachevsky D. V., Kazak T. V. (2021) Big Data: How Big Data Technologies are Changing Our Lives. *Big Data and Advanced Analytics. Collection of Scientific Articles of the VII International Scientific and Practical Conference, Minsk, May 19–20*. Minsk, Bestprint Publ. 188–192 (in Russian).
3. Kosareva E. M., Likhachevsky D. V. (2024) 'Smart City' as a Public Safety Monitoring System. *Artificial Intelligence in Belarus: III Forum of IT-Akademgrad, Minsk, 10–11 Oct*. Minsk, United Institute of Informatics Problems of the National Academy of Sciences of Belarus. 162–166 (in Russian).

4. Kosareva E. M., Likhachevsky D. V. (2024) Characteristics of Potentially Dangerous Individuals as One of the Threats in 'Smart City' Systems. *Modern Problems of Radio Electronics and Telecommunications: Collection of Scientific Papers No 7*. Moscow-Sevastopol, RNTORES named after A. S. Popov, Sevastopol State University Publ. (in Russian).
5. Kosareva E. M., Likhachevsky D. V. (2024) Machine Learning Methods for Recognizing Potential Anthropogenic Threats in 'Smart City' Systems. *Digital Environment: Technologies and Perspectives. DETP 2024. Proceedings of the II International Scientific and Practical Conference, Brest, Oct. 31–Nov. 1*. Brest, Brest State Technical University. 86–90 (in Russian).
6. Vasilyev L. V. (2009) *Legal Psychology: A Textbook for Universities*. St. Petersburg, Piter Publ. (in Russian).

Received: 7 April 2025 Accepted: 5 May 2025 Available on the website: 10 July 2025

Вклад авторов

Косарева Е. М. разработала метод оценки потенциальных антропогенных угроз «умного города», провела исследование.

Лихачевский Д. В. сформулировал задачу исследования.

Казак Т. В. определила общую методологию исследования.

Тиунчик Д. Р. разработал программный код, выполнил обучение модели.

Authors' contribution

Kosareva E. M. developed the method for assessing potential anthropogenic threats to a "smart city", conducted the research.

Likhachevsky D. V. formulated the research task.

Kazak T. V. defined the general research methodology.

Tiunchik D. R. developed the program code, trained the model.

Сведения об авторах

Косарева Е. М., асс. каф. проектирования информационно-компьютерных систем, Белорусский государственный университет информатики и радиоэлектроники (БГУИР)

Лихачевский Д. В., канд. техн. наук, доц., декан факультета компьютерного проектирования, БГУИР

Казак Т. В, д-р псих. наук, проф., зав. каф. инженерной психологии и эргономики, БГУИР

Тиунчик Д. Р., студент БГУИР

Адрес для корреспонденции

220013, Республика Беларусь,
Минск, ул. П. Бровки, 6
Белорусский государственный университет
информатики и радиоэлектроники
Тел.: +375 17 293-20-88
E-mail: kksrvvv@gmail.com
Косарева Екатерина Максимовна

Information about the authors

Kosareva E. M., Assistant at the Department of Design of Information and Computer Systems, Belarusian State University of Informatics and Radioelectronics (BSUIR)

Likhachevsky D. V., Cand. Sci. (Tech.), Associate Professor, Dean of the Faculty of Computer Design, BSUIR

Kazak T. V., Dr. Sci. (Psych.), Professor, Head of the Department of Engineering Psychology and Ergonomics, BSUIR

Tiunchik D. R., Student, BSUIR

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki St., 6
Belarusian State University
of Informatics and Radioelectronics
Tel.: +375 17 293-20-88
E-mail: kksrvvv@gmail.com
Kosareva Ekaterina Maksimovna