Вестник Томского государственного педагогического университета. 2022. Вып. 2 (220). С. 96–106.
Tomsk State Pedagogical University Bulletin. 2022, vol. 2 (220), pp. 96–106.

УДК 378.095
https://doi.org/10.23951/1609-624X-2022-2-96-106

ПЕДАГОГИЧЕСКИЕ ПРОТИВОРЕЧИЯ В СИСТЕМЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Игорь Александрович Кислицин

Омский государственный педагогический университет, Омск, Россия, ikisla@gmail.ru

Аннотация

Введение. Активный рост числа преступных деяний, совершаемых с использованием информационно-коммуникационных технологий (ИКТ), наблюдаемый в последнее время как на территории России, так и во всем мире, обуславливает потребность в сотрудниках органов внутренних дел (ОВД), способных оперативно решать задачи, связанные с профессиональной деятельностью, используя современные специализированные программы и средства вычислительной техники, в сжатые сроки осваивать необходимые навыки и умения, а также изыскивать нетрадиционные решения.

Цель – основываясь на данных статистических отчетов, результатах научных исследований, мнениях сотрудников ОВД, непосредственно осуществляющих практическую деятельность, а также курсантов образовательных организаций МВД России, провести анализ и выявить педагогические противоречия в рассматриваемой сфере, с тем чтобы в дальнейшем предложить возможные пути их устранения.

Материал и методы. Материалом исследования послужили сведения из статистических отчетов правоохранительных органов о преступлениях, совершенных с применением ИКТ, и результатах противодействия им, публикации иностранных и отечественных авторов о киберпреступности и подготовке соответствующих специалистов, а также выводы, сделанные на основе интервьюирования курсантов вузов системы МВД России и действующих сотрудников ОВД.

В основу методологии исследования положен качественный и количественный анализ статистических сведений, контент-анализ, сравнение и обобщение материалов и документов рассматриваемой тематики, ранжирование результатов анкетирования участников, а также метод экспертных оценок.

Результаты и обсуждение. Тезис о негативной ситуации, связанной с распространением киберпреступлений и недостаточной эффективностью противодействия им, подтверждается статистическими данными Главного информационно-аналитического центра МВД России. Такое положение дел обусловлено в том числе слабой цифровой компетентностью как выпускников образовательных организаций МВД России, так и действующих сотрудников ОВД.

Представители научного сообщества сходятся во мнении о имеющихся проблемах в системе подготовки специалистов в сфере информационной безопасности, а также необходимости создания образовательной платформы для успешного формирования специальных знаний в сфере ИКТ и их внедрения в практическую деятельность правоохранительных органов.

В настоящей работе выявлены и сформулированы педагогические противоречия в области подготовки сотрудников, способных эффективно противодействовать рассматриваемым преступным деяниям. В качестве примера преодоления вышеуказанных противоречий рассматривается опыт Омской академии МВД России, в которой предпринята попытка внедрения современных проблемно ориентированных технических средств и программного обеспечения в образовательный процесс.

Заключение. Выявленные педагогические противоречия указывают на имеющиеся проблемы в области подготовки будущих специалистов по противодействию преступлениям в сфере ИКТ.

Рассмотренные программные средства, предложенная методика их использования в образовательном процессе направлены на развитие у курсантов компетенций, позволяющих сделать практическую деятельность по раскрытию киберпреступлений максимально эффективной и преодолеть выявленные проблемы и противоречия.

Ключевые слова: *киберпреступления, информатизация образования, система информационно-аналитического обеспечения деятельности МВД России, специализированные проблемно ориентированные программные средства, профессиональные компетенции будущего сотрудника ОВД*

Для цитирования: Кислицин И. А. Педагогические противоречия в системе подготовки специалистов в области противодействия киберпреступности // Вестник Томского государственного педагогического университета. 2022. Вып. 2 (220). С. 96–106. https://doi.org/10.23951/1609-624X-2022-2-96-106

PEDAGOGICAL CONTRADICTIONS IN THE SYSTEM OF EDUCATING SPECIALISTS IN THE FIELD OF CYBERCRIMES COUNTERACTION

Igor A. Kislitsin

Omsk State Pedagogical University, Omsk, Russian Federation, ikisla@gmail.ru

Abstract

Introduction. Rapidly growing amount of crimes committed using information and telecommunication technologies, which has been observed lately both in Russia and all over the world determines the need in internal affairs employees capable of solving professional tasks with the help of modern software and hardware within minimal period of time, mastering new skills and abilities promptly and finding nonstandard solutions.

Aim and objectives. Basing on statistical data analysis, opinions of scientific community, current internal affairs employees and cadets of educational organizations of the Ministry of Internal Affairs of Russia (the MIA of Russia) the purpose is to analyze and reveal pedagogical contradictions in field in question in order to suggest possible ways of removing them in future.

Material and methods. Material of research was statistical data on the results of internal affairs bodies of Russian Federation counteraction to crimes committed with the use of information and telecommunication technologies (ITT), domestic and foreign publications on cybercrime and educating specialists in the field of countering it, and also the results of interview with current internal affairs employees and cadets of educational organizations of the MIA of Russia.

The research methodology is based on qualitative and quantitative analysis of statistical data, content-analysis, comparison and generalization of data and documents of theme in question, ranging of interviewing results, and also method of expert evaluations.

Results and discussion. As a result of analysis for statistical data from the Main Information and Analytical Center of the MIA of Russia the thesis about negative dynamic of amount of crimes committed using ITT was confirmed, unsatisfactory results of counteraction cybercrimes were marked. The reasons of indicated situation are revealed, including insufficient competence in the field of information technology, both for current internal affairs employees and graduates of educational institutions of the MIA of Russia.

The representatives of scientific community agree that problems exist in the system of educating specialists in the field of information security, and that a "platform" must be created for the successful development of special knowledge in the field of ITT and their implementation in the practical activities of law enforcement agencies.

Pedagogical contradictions in the field of educating specialists in cybercrime counteraction are revealed and formulated in this work. As one of possible ways to overcome these contradictions, Omsk Academy of the MIA of Russia experience in integrating modern problem-oriented software tools into the educational process, and in developing a methodology for their application is examined.

Conclusion. The revealed pedagogical contradictions indicate existing problems in the sphere of educating future specialists in crimes counteraction in the field of ITT.

Software tools reviewed in the article and the proposed method of their use in the educational process are aimed at developing competencies in cadets, thus letting the cybercrime counteraction activity to be the most effective and to overcome revealed issues and contradictions.

Keywords: *cybercrimes, informatization of education, information and analytical support system for the activities of the MIA of Russia, specialized problem-oriented software, professional competencies of future internal affairs employees*

For citation: Kislitsin I. A. Pedagogicheskiye protivorechiya kak novaya kriminal'naya ugroza [Pedagogical Contradictions in the System of Educating Specialists in the Field of Cybercrimes Counteraction]. *Vestnik Tomskogo gosudarstvennogo pedagogicheskogo universiteta – TSPU Bulletin*, 2022, vol. 2 (220), pp. 96–106 (In Russ.). https://doi.org/10.23951/1609-624X-2022-2-96-106

Введение

Бурная цифровизация жизнедеятельности общества повлияла и на сферу противоправной деятельности. Сегодня значительная часть преступлений совершается с применением современных технологий: бесконтактный сбыт наркотических средств через интернет-магазины, мошенничества и кражи, совершенные дистанционным способом, экстремистские и террористические проявления в социальных сетях. Даже для организации убийства или причинения тяжких телесных повреждений зачастую используются средства ИКТ.

Однако, несмотря на то что уголовное законодательство РФ претерпевает постоянные изменения, в нем по-прежнему нет внятного определения для понятия «киберпреступление». Многие ученые и исследователи предлагали свои формулировки, в той или иной степени отражающие различные аспекты данного понятия. Так, В. А. Номоконов и Т. Л. Тропина считают, что «понятие „киберпреступление" связано как с использованием компьютеров, так и с

использованием информационных технологий и глобальных сетей» [1]. Д. Н. Карпова раскрывает это понятие как «…акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет» [2].

Представляется, что «киберпреступление» выступает как часть целого по отношению к более широкому понятию – «киберпреступность», или «компьютерная преступность».

По нашему мнению, наиболее полно это понятие удалось раскрыть К. Н. Евдокимову, который рассматривает данный термин с двух точек зрения. С одной стороны, определение компьютерной преступности совпадает с установленной законодателем дефиницией «преступления в сфере компьютерной информации, т. е. совокупность противоправных деяний, в которых предметом посягательства являются информация, размещенная на компьютерной технике, средства ее защиты, хранения, обработки и передачи». С другой стороны, компьютерная преступность, или «киберпреступность», трактуется как «совокупность преступлений, в которых компьютерная информация, информационно-телекоммуникационные сети; средства создания, хранения, обработки, передачи компьютерной информации (компьютеры, смартфоны, платежные терминалы и иные компьютерные устройства) являются не только предметами преступного деяния, но и используются в качестве средства и орудия совершения преступления» [3, с. 324]. Аналогичным образом понятие «киберпреступление» трактует американский ученый Anthony Reyes в своей монографии [4, с. 26].

Корректность данного определения отчасти подтверждается изменившимся подходом правоохранительных органов РФ к статистической оценке распространенности преступлений, совершаемых с использованием ИКТ. В июне 2020 г. приказом МВД России введен в действие новый статистический отчет «О результатах деятельности органов внутренних дел Российской Федерации по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, а также результатах деятельности структурных подразделений органов внутренних дел Российской Федерации, специализирующихся на противодействии преступлениям данного вида». Указанная форма отчетности содержит информацию о 49 составах преступлений, при совершении которых могут использоваться ИКТ [5].

Резюмируя вышесказанное, под IT-преступлениями (или киберпреступлениями) мы предлагаем понимать любые преступные проявления, для совершения которых используются ИКТ, а не только деяния, предусмотренные главой 28 Уголовного кодекса РФ – «Преступления в сфере компьютерной информации».

Безусловно, для эффективной организации работы по противодействию IT-преступлениям сотрудникам ОВД недостаточно знаний уголовного и уголовно-процессуального законодательства, а также навыков применения тактических приемов раскрытия классических преступных деяний. В настоящее время полицейский должен в совершенстве владеть современными программными и техническими средствами, уверенно ориентироваться в информационном пространстве, находить неординарные решения.

В ходе настоящей работы предполагается проанализировать ситуацию, складывающуюся в системе подготовки будущих сотрудников ОВД в условиях увеличения распространенности преступных деяний, совершаемых с использованием новых цифровых технологий, выявить и сформулировать педагогические противоречия в рассматриваемой сфере, а также предложить возможные пути их устранения.

Материал и методы

В качестве базы эмпирического исследования выступило федеральное государственное казенное образовательное учреждение высшего образования «Омская академия МВД России» (ОмА МВД России) .

В основу исследования легли отечественные и зарубежные публикации о киберпреступности и подготовке специалистов в области противодействия ей, статистические сведения о результатах противодействия органов внутренних дел Российской Федерации IT-преступлениям, а также результаты собеседований с сотрудниками полиции и анкетирования курсантов и слушателей ОмА МВД России.

Статданные, полученные из ГИАЦ МВД России, изучались с использованием методов количественного и качественного анализа. Изучение публикаций по теме исследования проводилось методами сравнения и обобщения, а также контент-анализа.

В исследовании приняли участие 60 курсантов 5-го курса факультета подготовки сотрудников полиции ОмА МВД России, 12 действующих оперативных сотрудников ОВД Челябинской, Свердловской, Омской и Тюменской областей. Для сбора и изучения мнений участников использовали анкетный опрос, ранжирование и метод экспертных оценок.

Результаты и обсуждение

Потребность в модернизации подходов к противодействию киберпреступности неоднократно отмечалась на национальном и международном

уровне. В доктрине информационной безопасности, утвержденной президентом РФ в 2016 г., указывается на «…возрастание масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий» [6].

Равным образом Организация Объединенных Наций предлагает государствам «…опробовать конкретные меры, направленные на создание защищенной и устойчивой киберсреды, предупреждать и пресекать преступную деятельность, осуществляемую с помощью Интернета» [7].

По данным правоохранительных органов, на протяжении последних лет распространенность преступлений различных видов, совершаемых с использованием современных информационных технологий, неуклонно увеличивается. Так, результаты анализа, проведенного организационно-аналитическим департаментом МВД России, указывают на увеличение числа зарегистрированных преступлений данной категории в период с 2014 по 2019 г. более чем в 25 раз (рис. 1).

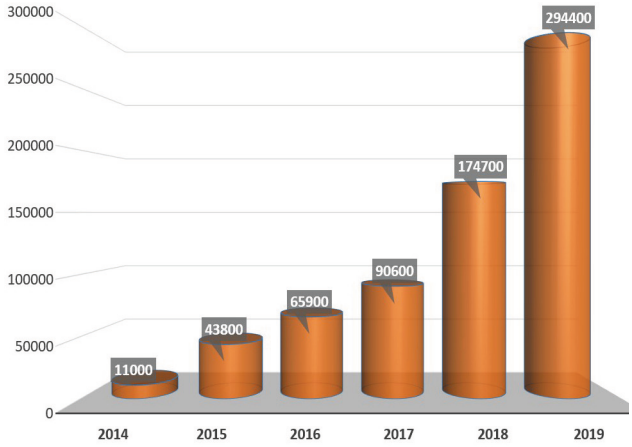

Рис. 1. Изменение количества преступлений, совершенных с применением ИКТ, в 2014–2019 гг.

Тенденция роста данного вида преступности отмечается и в 2020 г. (503,5 тыс.; +71 %).

Большинство преступлений рассматриваемой категории совершены против собственности: 81 % – кражи (172,6 тыс.; рост на 81,6 %) и дистанционные мошенничества (236,3 тыс.; рост на 76,1 %). Значительную долю (12 %) составили деяния в сфере незаконного оборота наркотических средств, психотропных и сильнодействующих веществ (60,8 тыс.; рост на 77,9 %) (рис. 2).

Структура иных 6,7 % IT-преступлений выглядит следующим образом:

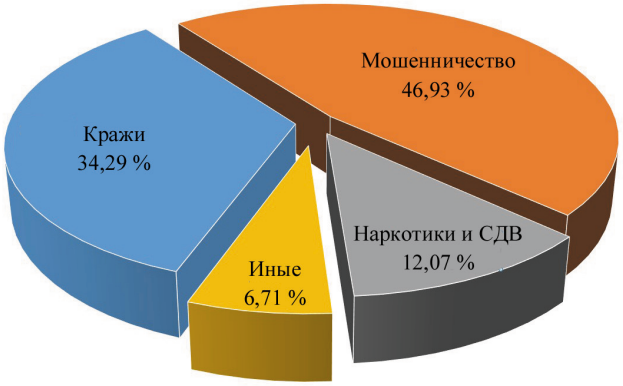

Рис. 2. Структура преступлений, совершенных в 2020 г. с использованием ИКТ

– свыше 8 тыс. совершены в сфере экономической деятельности (незаконное получение или разглашение банковской или коммерческой тайны, сбыт фальшивых денег или ценных бумаг, азартные игры и т. п.),

– около 4 тыс. – в сфере компьютерной информации,

– чуть менее чем по 2 тыс. – распространение порнографических материалов, а также посягательства на свободу, честь и достоинство личности (рис. 3).

Результаты интервьюирования действующих сотрудников уголовного розыска различных субъектов РФ показали, что в последнее время возрастает число киберпресуплений, предусмотренных статьей 163 Уголовного кодекса РФ «Вымогательство», совершенное с использованием коммуникационных возможностей сети Интернет.

Главный критерий эффективности противодействия преступности, в том числе киберпреступности, – это отношение числа раскрытых преступлений к общему числу преступных деяний, по которым приняты процессуальные решения, так называемая раскрываемость преступлений (рис. 4).

Необходимо обратить внимание на то, что раскрываемость преступлений рассматриваемой категории традиционно низкая и в рассматриваемом периоде также демонстрирует негативную тенденцию к снижению, составив 20,1 % (для сравнения: в 2019 г. – 24 %). Иными словами, из 455 тыс. IT-преступлений, по которым органами внутренних дел приняты решения, раскрыто и направлено в суд лишь каждое пятое (рис. 5).

Данная ситуация обусловлена рядом причин. Первая причина – это специфичность противоправной деятельности в данной сфере, а именно активное применение новейших информационно-телекоммуникационных технологий, постоянное появление новых способов и методов совершения преступлений, широкие возможности сокрытия личности преступников (обеспечение анонимности),

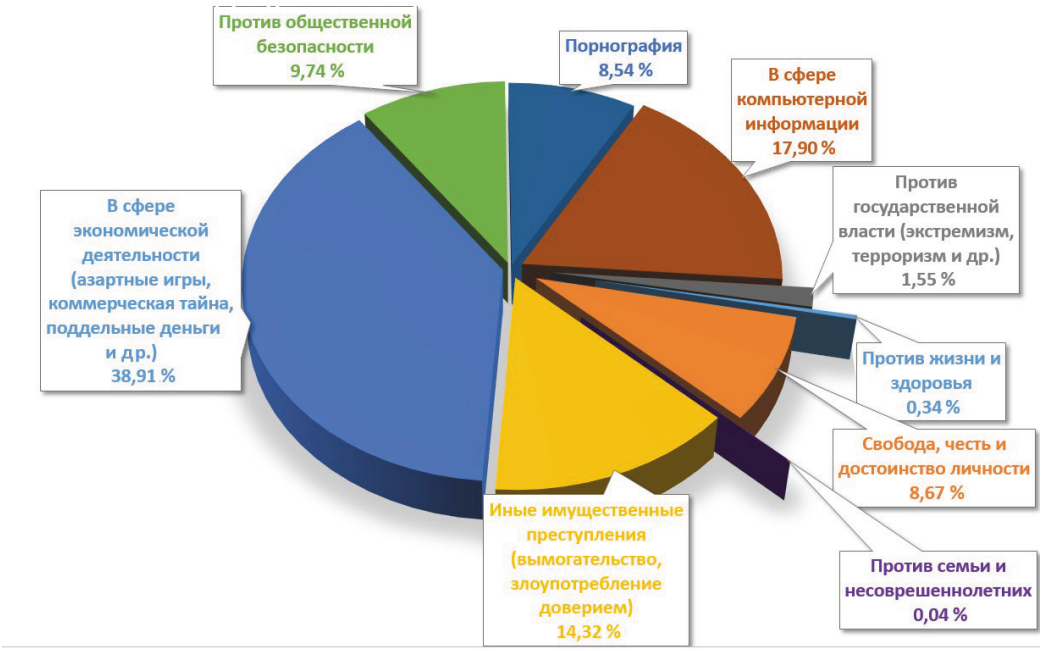

Рис. 3. Структура иных IT-преступлений, совершенных в 2020 г.

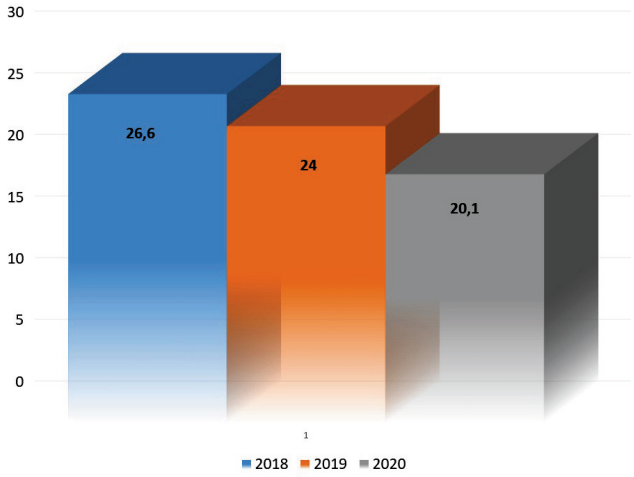

Рис. 4. Изменение раскрываемости преступлений, совершенных с использованием ИКТ в 2018–2020 гг.

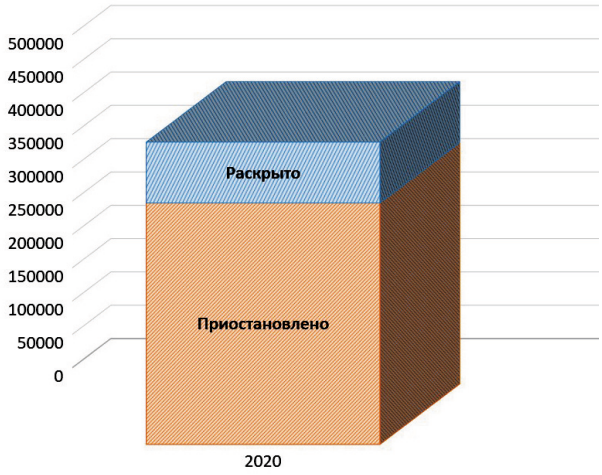

Рис. 5. Отношение раскрытых и приостановленных производством IT-преступлений в 2020 г.

виктимное поведение потерпевших. Вторая немаловажная причина – недостаточная компетентность действующих сотрудников ОВД в сфере информационных технологий.

В целях решения проблемы нехватки специалистов, способных эффективно противодействовать новым видам преступлений, предпринимаются определенные действия. Так, в учебных заведениях МВД России и в рамках межведомственного взаимодействия с гражданскими вузами проводится повышение квалификации действующих сотрудников, специализирующихся на противодействии IT-преступлениям. Актуализируются дополнительные профессиональные программы, разрабатываются и реализуются новые методики повышения квалификации соответствующих специалистов.

Однако необходимо уделять внимание не только переподготовке действующих полицейских кадров, но и обучению курсантов, которым после окончания учебного заведения необходимо в кратчайшее время включиться в рабочий процесс и адекватно противодействовать преступной активности новых видов.

На сегодняшний день в системе вузов МВД России наиболее прогрессивными в области подготовки специалистов компьютерных технологий, защиты компьютерной информации и раскрытия ки-

берпреступлений являются три образовательные организации: Московский университет МВД России им. В. Я. Кикотя, Санкт-Петербургский университет МВД России и Воронежский институт МВД России. При этом в других региональных ведомственных образовательных учреждениях отмечается серьезная нехватка аналогичных специальностей. С учетом темпов роста числа киберпреступлений и обширной территории нашей страны этого, разумеется, недостаточно.

На проблему недостатка квалифицированных кадров и необходимость создания образовательной платформы для успешного формирования специальных знаний в сфере IT-технологий и их внедрения в практическую деятельность правоохранительных органов в последнее время обращают внимание все большее число представителей научного сообщества. «Для того чтобы успешно противодействовать преступлениям, совершаемым с использованием информационных технологий, правоохранительным органам необходимо подготавливать (переподготавливать) кадры, способные работать в современных условиях и отвечать на новые угрозы, возникающие в мире в информационной сфере» [8, с. 161]. К аналогичному выводу приходит О. Р. Идрисов, отмечая, что «...на современном этапе развития общества возрастает актуальность профессиональной подготовки и качества современного высшего образования не только IT-специалистов, но и юристов, в том числе в целях выявления, пресечения и предупреждения киберпреступлений» [9]. А. В. Царегородцев очерчивает целый пласт проблем, имеющихся в системе образования при подготовке специалистов в сфере информационной безопасности, в том числе «...недостаточная оснащенность вузов современными стендами и оборудованием, стремительно устаревающие учебные материалы, в которых уделяется внимание только изучению теоретических вопросов, лишь расширяющих кругозор обучающихся» [10].

Применение новейших информационно-телекоммуникационных технологий и средств в образовательном процессе рассматривается в рукописях таких ученых, как С. В. Титова, Е. С. Полат, В. В. Красильников, В. С. Тоискин, И. Н. Семенова и др. Многие представители научного сообщества обращают внимание на то обстоятельство, что «темпы совершенствования самих информационно-коммуникационных технологий заметно опережают темпы развития методов обучения на их основе, в результате чего их дидактический потенциал оказывается востребованным не в полной мере» [11, с. 4].

С учетом вышеизложенного наблюдается *противоречие на социально-педагогическом уровне* между спросом в современном обществе на высокопрофессиональных специалистов по противодействию киберпреступности и недостаточным уровнем цифровой компетенции выпускников многих образовательных организаций системы МВД России, необходимым для эффективного осуществления этой деятельности.

Особенности документирования киберпреступлений требуют от сотрудников специфических умений и навыков, позволяющих уверенно ориентироваться в едином информационном пространстве, в кратчайшие сроки осуществлять поиск необходимых сведений, в том числе в специализированных информационных системах МВД России. Приходится признать, что в настоящее время теоретические основы и методические приемы формирования вышеуказанных качеств у обучающихся в вузах МВД России разработаны и применяются в недостаточной степени, что подтверждается опросом, проведенным среди слушателей 5-го курса, вернувшихся после прохождения практики в подразделениях уголовного розыска органов внутренних дел. Анализ результатов опроса показал, что, «несмотря на получение фундаментальных базовых знаний по дисциплинам „Информатика и информационные технологии в профессиональной деятельности“ и „Оперативно-разыскная деятельность“, будущим сотрудникам достаточно сложно ориентироваться во всех современных информационных банках данных, в том числе используемых в системе МВД» [12, с. 60].

Таким образом, прослеживаются противоречия еще на двух уровнях: *на научно-педагогическом* – между необходимостью формирования высокой IT-компетентности обучающихся в ходе занятий и низкой разработанностью дидактических средств и теоретических основ ее достижения; *на научно-методическом уровне* – между потребностью во внедрении современных педагогических технологий, ориентированных прежде всего на решение задач, максимально приближенных к практической деятельности, и недостатком соответствующих, в том числе программных, средств, отвечающих современным требованиям.

Исходя из выявленных противоречий, сформулируем проблему, требующую исследования: *как обеспечить приобретение, развитие IT-компетенции курсантов вузов МВД России, которая в перспективе позволит выпускникам незамедлительно включиться в профессиональную деятельность и максимально эффективно осуществлять противодействие преступлениям, совершаемым с применением ИКТ*.

Нивелировать вышеуказанные противоречия и в конечном итоге повысить качество подготовленности будущих сотрудников полиции позволит интеграция в образовательный процесс современных

проблемно ориентированных программных продуктов.

Предлагаем рассмотреть опыт профессорско-преподавательского состава кафедры информационных технологий в деятельности ОВД ОмА МВД России, которым в 2019–2020 гг. в рамках научно-исследовательской работы создан специализированный программный комплекс «Эмулятор сервисов системы информационно-аналитического обеспечения деятельности МВД России».

Единая система информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России) – это грандиозный проект, предназначенный для обеспечения цифровизации всех направлений деятельности сотрудников полиции по всей стране. ИСОД МВД России введена в эксплуатацию в 2015 г. Одной из составляющих данной системы являются так называемые сервисы обеспечения оперативно-служебной деятельности, которые представляют собой базы с информацией, необходимой для эффективной работы большинства подразделений ОВД, в том числе в сфере пресечения и раскрытия киберпреступлений.

Разумеется, доступ к сервисам ИСОД строго ограничен. Получать информацию имеют право только уполномоченные пользователи, что обусловлено требованиями безопасности и спецификой сведений, накапливаемых в центрах обработки данных. Ограничения, связанные с обеспечением режима секретности, делают невозможным изучение функционала сервисов ИСОД непосредственно на практических занятиях.

Представляется, что изучение возможностей системы только через просмотр презентаций и технической документации вряд ли обеспечит формирование у обучающихся практических навыков, необходимых для уверенной работы с сервисами обеспечения оперативно-служебной деятельности. Между тем до последнего времени полноценные тренажеры, позволяющие изучить функционал ИСОД, не разрабатывались. Данное обстоятельство подтолкнуло руководство кафедры информационных технологий в деятельности органов внутренних дел ОмА МВД России к созданию полнофункционального эмулятора системы информационно-аналитического обеспечения деятельности МВД России.

Интерфейс разработанного программного комплекса абсолютно идентичен реальному порталу. Кроме того, эмулятор предоставляет возможность работать с данными, которые по составу и структуре аналогичны хранимым в настоящей системе [13]. В учебных банках данных, используемых в эмуляторе, содержится около 30 млн объектов хранения. Это сведения о физических и юридических лицах, адресах, транспортных средствах, гражданском оружии, банковских счетах, телефонах, документах, удостоверяющих личность, правонарушениях и т. п. Общий объем информации, используемой в эмуляторе, достигает 20 гигабайт. Отметим, что данные, накапливаемые в эмуляторе, никоим образом не раскрывают персональные данные реальных лиц или какие-либо иные идентифицирующие сведения об объектах, так как сгенерированы случайным образом. Такой внушительный объем информации дает возможность ставить перед обучаемыми задачи любой сложности.

К примеру, формулировка задачи может быть представлена в виде синтезированного сообщения суточной оперативной сводки, т. е. содержать информацию о преступлении, отчасти похожую на реально происходившие события. В целях установления обстоятельств, связанных с условием задачи, курсанту необходимо проанализировать первичную информацию, а затем выбрать поисковые и аналитические средства, необходимые для поэтапного получения дополнительных данных, имеющих отношение к происшествию. Работа в основном осуществляется в разработанном эмуляторе сервисов ИСОД МВД России, кроме того, применяются программы визуализации, в которых наглядно отображаются схемы установленных связей между объектами и событиями или строятся социальные графы, позволяющие провести анализ, выдвинуть гипотезу и решить, в каком направлении двигаться дальше в решении задачи. В результате обучающиеся приобретают и закрепляют навыки эксплуатации реальных систем без угрозы разглашения, порчи или уничтожения сведений, хранимых в центрах обработки данных ИСОД МВД России.

Внедрение в образовательный процесс новых специализированных проблемно ориентированных программных продуктов требует разработки соответствующих методик их применения.

Так, для проведения педагогического эксперимента, призванного оценить эффективность интеграции в образовательный процесс вышеописанного программного комплекса, руководство ОмА МВД России приняло решение о создании новой учебной дисциплины «Профессиональные информационные системы в деятельности ОВД». Рабочая программа этой дисциплины направлена в том числе на развитие у обучающихся общепрофессиональной компетенции ОПК-13 «Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности», определенной новым ФГОС ВО по специальности 40.05.02 «Правоохранительная деятельность» [14, 15].

В ходе освоения программы рассматриваемой дисциплины у курсантов и слушателей также

должны сформироваться профессиональные компетенции, указанные в квалификационных требованиях к специальной профессиональной подготовке выпускников образовательных организаций системы МВД России, утвержденных министром внутренних дел Российской Федерации, такие как: «способен решать задачи по предупреждению, выявлению, пресечению и раскрытию преступных проявлений, совершаемых в том числе с использованием ИКТ»; «способен формировать оперативные и иные учеты, использовать информационные ресурсы и технологии для решения задач оперативно-разыскной деятельности (ОРД)»; «способен использовать в служебной деятельности средства вычислительной техники, справочно-правовые системы, а также иные учеты и автоматизированные поисковые системы, в том числе с учетом требований информационной безопасности».

В качестве основных индикаторов достижения вышеуказанных профессиональных компетенций могут быть выделены следующие знания, умения и навыки, формируемые у обучающихся в ходе изучения дисциплины:

Знания:

– способов профилактики, пресечения, выявления и раскрытия преступных посягательств и административных правонарушений, в том числе совершаемых с использованием информационно-телекоммуникационных технологий;

– методов и средств обнаружения доказательственной информации, в том числе на объектах цифровой техники и в киберпространстве;

– состав, функции и конкретные возможности аппаратного и программного обеспечения средств вычислительной техники, используемых в органах внутренних дел, а также технологию работы профессионально ориентированных справочно-информационных, правовых и информационно-поисковых систем.

Умения:

– планировать и проводить оперативно-разыскные мероприятия, в том числе в глобальных компьютерных сетях;

– использовать оперативные и иные учеты, информационные ресурсы и технологии для выявления сведений, а также связей между различными объектами в целях решения задач оперативно-разыскной деятельности;

– применять в оперативно-служебной деятельности справочно-правовые системы, а также иные учеты и автоматизированные информационно-поисковые системы, используемые в ОВД;

– использовать открытые интернет-ресурсы, а также свободное и проприетарное программное обеспечение в служебной деятельности для сбора и анализа информации.

Навыки:

– поиска и анализа значимой информации в глобальных компьютерных сетях в целях решения задач ОРД;

– работы со справочно-правовыми информационными системами, учетами и автоматизированными информационно-поисковыми системами, используемыми в профессиональной деятельности;

– использования средств автоматизации аналитической работы.

Учебная дисциплина «Профессиональные информационные системы в деятельности органов внутренних дел» впервые прошла апробацию среди слушателей, обучающихся на 5-м курсе по специальности 40.05.02 «Правоохранительная деятельность (специализация ОРД)» во 2-м семестре 2019 г., после прохождения курсантами полугодовой преддипломной практики. После освоения рабочей программы дисциплины проведено анонимное анкетирование курсантов, анализ результатов которого показал, что более 90 % респондентов отмечают несомненную связь изученной дисциплины с практической деятельностью; около 50 % участников анкетирования высказали мнение, что данную дисциплину полезнее было бы изучать до прохождения преддипломной практики.

Принимая во внимание результаты анкетирования, учитывая модификации, на постоянной основе вносимые в ПК «Эмулятор ИСОД МВД России», такие как реализация новых сервисов и расширение функционала, а также постоянное возникновение новых способов совершения киберпреступлений, рабочая программа рассматриваемой учебной дисциплины в настоящее время перерабатывается.

Внесены изменения в учебные планы основных профессиональных образовательных программ высшего образования, в соответствии с которыми учебная дисциплина «Профессиональные информационные системы в деятельности ОВД» изучается курсантами на четвертом курсе, до прохождения производственной преддипломной практики, скрупулезно перерабатываются планы практических и семинарских занятий.

Безусловно, выявление и раскрытие преступлений, совершенных с использованием ИКТ, вряд ли будет эффективным, если в ходе осуществления этой деятельности использовать только лишь профессиональные информационные системы, эксплуатируемые в ОВД. Поэтому кафедрой информационных технологий в деятельности органов внутренних дел ОмА МВД России с учетом опыта профессорско-преподавательского состава Московского университета МВД России им. В. Я. Кикотя разрабатывается рабочая программа еще одной

дисциплины, получившей название «Криминальная среда и современные информационные технологии», в рамках которой планируется изучать как инновационные способы совершения преступлений, так и средства (в том числе программные) и методы, которые позволяют сотрудникам полиции эффективно противодействовать подобным преступным проявлениям. Разумеется, каждое программное средство проходит тщательную проверку на пригодность к применению в образовательном процессе. Это обусловлено тем, что нередко для использования подобных программ и сервисов необходимо оформление соответствующих допусков и специальных разрешений, имеющихся у действующих оперативных сотрудников.

Заключение

Проведенный анализ статистических сведений правоохранительных органов Российской Федерации, изучение мнения действующих сотрудников позволяют сделать вывод, что распространенность киберпреступлений ежегодно увеличивается. При этом имеющиеся в настоящее время методики подготовки специалистов в области противодействия инновационным видам преступности нельзя признать достаточно эффективными, что подтверждается мнениями научного сообщества.

На основании изложенного выделены педагогические противоречия, имеющие непосредственное отношение к настоящему исследованию.

Проведенное исследование показало, что интеграция в процесс обучения программного комплекса «Эмулятор ИСОД МВД России», разработанного на кафедре информационных технологий в деятельности органов внутренних дел ОмА МВД России, а также других проблемно ориентированных программных продуктов, разработка и внедрение учебной дисциплины «Профессиональные информационные технологии в деятельности ОВД» позволяет в определенной степени сформировать у будущих полицейских необходимые общепрофессиональные и профессиональные компетенции.

Приобретенные знания, умения и навыки положительно влияют на эффективность решения задач, возникающих в ходе осуществления оперативно-служебной деятельности по противодействию IT-преступности.

Вместе с тем нельзя не отметить, что стремительное развитие информационных технологий в современном обществе, к сожалению, имеет некоторые негативные аспекты, выражающиеся в динамичном изменении форм преступной деятельности, средств и методов ее осуществления.

В связи с этим профессорско-преподавательскому составу образовательных организаций в тесном взаимодействии с действующими сотрудниками ОВД и специалистами коммерческих организаций, осуществляющих деятельность в сфере информационной безопасности, необходимо проанализировать и тщательно переработать рабочие программы учебных дисциплин, непосредственно связанных с информационно-телекоммуникационными технологиями и IT-безопасностью.

В частности, для выявления концептуальных подходов к формированию знаний, умений и навыков, необходимых для эффективного противодействия IT-преступности, необходимо проанализировать научно-методические, психолого-педагогические и технические материалы; теоретически доказать и реализовать на практике организационно-педагогические условия формирования соответствующих компетенций в процессе обучения курсантов; предложить и обосновать применение выбранных современных проблемно ориентированных программных продуктов как активных и интерактивных средств обучения тактике и методике выявления и раскрытия IT-преступлений, кроме того, разработать комплекс практических учебных заданий с их использованием; предложить методы оценки сформированности компетенций в области противодействия киберпреступности у выпускников образовательных организаций МВД России; осуществить опытно-поисковую работу по проверке эффективности применения разработанной педагогической технологии.

Список источников

1. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология. Вчера. Сегодня. Завтра. 2012. № 1 (24). С. 45–55.
2. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46–50.
3. Евдокимов К. Н., Скляров С. В. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2016. Т. 10, № 2. С. 322–330.
4. Reyes A. Cyber Crime Investigations: Bridging the Gaps Between, Security Professionals, Law Enforcement, and Prosecutors // Syngress Publishing, Inc. 2007.
5. Приказ МВД России от 16 июня 2020 г. № 434 «Об утверждении формы статистической отчетности о результатах деятельности органов внутренних дел Российской Федерации по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, а также результатах деятельности структурных подразделений органов внутренних дел Российской Федерации, специализирующихся на противодействии преступлениям данного вида».

6. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf (дата обращения: 02.07.2021).
7. Арзамасцев М. В. К вопросу об уголовно-правовой классификации киберпреступлений // Актуальные вопросы права и отраслевых наук. 2017. № 1(3). С. 11–16.
8. Архипцев И. Н., Сарычев А. В., Красников Р. В. Совершенствование подготовки сотрудников правоохранительных органов по противодействию преступлениям, совершаемым с использованием информационных технологий // Правовая парадигма. 2020. Т. 19, № 2. С. 154–163.
9. Идрисов О. Р. Актуализация подготовки юридических кадров в условиях роста киберпреступности и необходимости борьбы с ней // Современное образование: качество образования и актуальные проблемы современной высшей школы: материалы международной научно-методической конференции, Томск, 31 января 2019 года. Томск: Том. гос. ун-т систем управления и радиоэлектроники, 2019. С. 218–219.
10. Царегородцев А. В., Цацкина Е. П. Влияние информационного общества на подготовку обучающихся в сфере информационной безопасности // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2019. № 4 (833). С. 191–199.
11. Арбузов С. С. Формирование компетенций в области компьютерных сетей у бакалавров в процессе обучения информатике: автореф. … дис. канд. пед. наук. Екатеринбург, 2016. 23 с.
12. Гайдамакин А. А., Дивольд В.Е. Практико-ориентированное обучение информационным технологиям в Омской академии МВД России // Совершенствование образовательных программ, планирование и реализация учебного процесса: материалы всерос. учеб.-метод. конф., посвящ. 100-летию со дня образования Омской академии МВД России, Омск, 28 февраля 2020 г. / под ред. В. А. Гусева, М. С. Десятова. Омск: Омская академия Министерства внутренних дел Российской Федерации, 2020. С. 59–62.
13. Дивольд В. Е., Гайдамакин А. А., Батюшкин М. В. Профессиональные информационные системы: проблемы и опыт практико-ориентированного обучения // Вестник экономической безопасности. 2020. № 1. С. 329–332.
14. Приказ Министерства науки и высшего образования Российской Федерации от 28 августа 2020 г. № 1131 «Об утверждении федерального государственного образовательного стандарта высшего образования – специалитет по специальности 40.05.02 „Правоохранительная деятельность“» URL: http://publication.pravo.gov.ru/Document/View/0001202009150044 (дата обращения: 04.07.2021).
15. Приказ Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1456 «О внесении изменений в федеральные государственные образовательные стандарты» URL: http://publication.pravo.gov.ru/Document/View/0001202105270015 (дата обращения: 04.07.2021).

References

1. Nomokonov V. A., Tropina T. L. Kiberprestupnost' kak novaya kriminal'naya ugroza [Cybercrime as a new criminal threat]. *Kriminologiya. Vchera. Segodya. Zavtra – Criminology. Yesterday. Today. Tomorrow*, 2012, no. 1 (24), pp. 45–55 (in Russian).
2. Karpova D. N. *Kiberprestupnost': global'naya problema i yeye resheniye* [Cybercrime: a global problem and its solution]. Vlast', 2014, no. 8, pp. 46–50 (In Russian).
3. Evdokimov K. N., Sklyarov S. V. Sovremennyye podkhody k opredeleniyu ponyatiya, struktury i sushchnosti komp'yuternoy prestupnosti v Rossiyskoy Federatsii [Modern approaches to the definition of the concept, structure and essence of computer crime in the Russian Federation]. *Vserossiyskiy kriminologicheskiy zhurnal*, 2016, vol. 10, no. 2, pp. 322–330 (in Russian).
4. Reyes A. *Cyber Crime Investigations: Bridging the Gaps Between, Security Professionals, Law Enforcement, and Prosecutors.* Syngress Publishing, Inc. 2007.
5. *Prikaz MVD Rossii ot 16 iyunya 2020 g. № 434 "Ob utverzhdenii formy statisticheskoy otchetnosti o rezul'tatakh deyatel'nosti organov vnutrennikh del Rossiyskoy Federatsii po protivodeystviyu prestupleniyam, sovershayemym s ispol'zovaniyem informatsionno-telekommunikatsionnykh tekhnologiy, a takzhe rezul'tatakh deyatel'nosti strukturnykh podrazdeleniy organov vnutrennikh del Rossiyskoy Federatsii, spetsializiruyushchikhsya na protivodeystvii prestupleniyam dannogo vida"* [Order of the Ministry of Internal Affairs of Russia dated June 16, 2020 No. 434 "On approval of the form of statistical reporting on the results of the activities of the internal affairs bodies of the Russian Federation in countering crimes committed using information and telecommunication technologies, as well as the results of the activities of structural units of the internal affairs bodies of the Russian Federation specializing in combating crimes of this type"] (in Russian).
6. *Ukaz Prezidenta RF ot 5 dekabrya 2016 g. № 646 "Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii"* [Decree of the President of the Russian Federation dated December 5, 2016 No. 646 "On Approval of the Doctrine of Information Security of the Russian Federation"] (in Russian). URL: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf (accessed 2 July 2021).
7. Arzamastsev M. V. K voprosu ob ugolovno-pravovoy klassifikatsii kiberprestupleniy [On the issue of criminal-legal classification of cybercrimes]. *Aktual'nyye voprosy prava i otraslevykh nauk*, 2017, no. 1 (3), pp. 11–16 (in Russian).
8. Arkhiptsev I. N., Sarychev A. V., Krasnikov R. V. Sovershenstvovaniye podgotovki sotrudnikov pravookhranitel'nykh organov po protivodeystviyu prestupleniyam, sovershayemym s ispol'zovaniyem informatsionnykh tekhnologiy [Improving the training of law enforcement officers in countering crimes committed with the use of information technologies]. *Pravovaya paradigma – Legal Concept*, 2020, vol. 19, no. 2, pp. 154–163 (n Russian).

9. Idrisov O. R. Aktualizatsiya podgotovki yuridicheskikh kadrov v usloviyakh rosta kiberprestupnosti i neobhodimosti bor'by s ney [Updating the training of legal personnel in the context of the growth of cybercrime and the need to combat it]. *Sovremennoye obrazovaniye: kachestvo obrazovaniya i aktual'nyye problemy sovremennoy vysshey shkoly: materialy mezhdunarodnoy nauchno-metodicheskoy konferentsii, Tomsk, 31 yanvarya 2019 g*. [Modern education: the quality of education and topical problems of modern higher education: materials of the international scientific and methodological conference, Tomsk, 31 January, 2019]. Tomsk, Tomsk State University of Control Systems and Radioelectronics Publ., 2019. P. 218–219 (in Russian).
10. Tsaregorodtsev A. V., Tsatskina E. P. Vliyaniye informatsionnogo obshchestva na podgotovku obuchayushchikhsya v sfere informatsionnoy bezopasnosti [Influence of the information society on the training of students in the field of information security]. *Vestnik Moskovskogo gosudarstvennogo lingvisticheskogo universiteta. Obrazovaniye i pedagogicheskiye nauki – Vestnik of Moscow State Linguistic University. Education and teaching,* 2019, no. 4 (833), pp. 191–199 (in Russian).
11. Arbuzov S. S. *Formirovaniye kompetentsiy v oblasti komp'yuternykh setey u bakalavrov v protsesse obucheniya informatike.* Avtoref. dis. kand. ped. nauk [Formation of competencies in the field of computer networks among bachelors in the process of teaching computer science. Abstract of thesis cand. ped. sci.]. Yekaterinburg, 2016. 23 p. (in Russian).
12. Gaidamakin A. A., Divol'd V. E. Praktiko oriyentirovannoye obucheniye informatsionnym tekhnologiyam v Omskoy akademii MVD Rossii [Practice-oriented training in information technology at the Omsk Academy of the Ministry of Internal Affairs of Russia]. *Sovershenstvovaniye obrazovatel'nykh programm, planirovaniye i realizatsiya uchebnogo protsessa: materialy vserossiyskoy uchebno-metodicheskoy konferentsii, posvyashchennoy 100-letiyu so dnya obrazovaniya Omskoy akademii MVD Rossii, Omsk, 28 fevralya 2020* [Improvement of educational programs, planning and implementation of the educational process: Materials of the All-Russian educational and methodological conference anniversary of the foundation of the Omsk Academy of the Ministry of Internal Affairs of Russia, Omsk, February 28, 2020]. Edited by V. A. Gusev, M. S. Desyatov. Omsk, Omsk Academy of the Ministry of Internal Affairs of the Russian Federation Publ., 2020. P. 59–62 (in Russian).
13. Divol'd V. E., Gaydamakin, A. A., Batyushkin M. V. Professional'nye informatsionnye sistemy: problemy i opyt praktiko-orientirovannogo obucheniya [Professional information systems: problems and experience of practice-oriented learning]. *Vestnik ekonomicheskoy bezopasnosti,* 2020, no. 1, pp. 329–332 (in Russian).
14. *Prikaz Ministerstva nauki i vysshego obrazovaniya Rossiyskoy Federatsii ot 28 avgusta 2020 g. № 1131 "Ob utverzhdenii federal'nogo gosudarstvennogo obrazovatel'nogo standarta vysshego obrazovaniya – spetsialitet po spetsial'nosti 40.05.02 Pravookhranitel'naya deyatel'nost'"* [Order of the Ministry of Science and Higher Education of the Russian Federation dated August 28, 2020 No. 1131 "On the approval of the federal state educational standard of higher education – specialty in the specialty 40.05.02 Law enforcement"] (in Russian). URL: http://publication.pravo.gov.ru/Document/View/0001202009150044 (accessed 4 July 2021).
15. *Prikaz Ministerstva nauki i vysshego obrazovaniya Rossiyskoy Federatsii ot 26 noyabrya 2020 g. № 1456 "O vnesenii izmeneniy v federal'nyye gosudarstvennyye obrazovatel'nyye standarty"* [Order of the Ministry of Science and Higher Education of the Russian Federation of November 26, 2020 No. 1456 "On Amendments to Federal State Educational Standards"] (in Russian). URL: http://publication.pravo.gov.ru/Document/View/0001202105270015 (accessed 4 July 2021).

Информация об авторах

И. А. Кислицин, аспирант, Омский государственный педагогический университет (наб. Тухачевского, 14, Омск, Россия, 644099).

Information about the authors

I. A. Kislitsin, postgraduate student, Omsk State Pedagogical University (nab. Tukhachevskogo, 14, Omsk, Russian Federation, 644099).

Статья поступила в редакцию 07.09.2021; принята к публикации 05.02.2022
The article was submitted 07.09.2021; accepted for publication 05.02.2022