

# ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ МОДЕЛИ ФОРМИРОВАНИЯ ГОТОВНОСТИ КУРСАНТОВ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

## *Practical Implementation of the Model of Formation of Cadets' Readiness to Ensure Information Security in Professional Activities*

**Dmitrij Dvoreckij**

Academy of Law Management of the Federal Penal Service of Russia (Pskov branch),  
Russian Federation

**Natalia Kolesnikova**

Academy of Law Management of the Federal Penal Service of Russia (Pskov branch),  
Russian Federation

**Oksana Makarkina**

Academy of Law Management of the Federal Penal Service of Russia (Pskov branch),  
Russian Federation

**Kira Lagvilava**

Pskov State University, Russian Federation

**Abstract.** *The mass introduction of information technologies in the activities of state structures has made it possible to transfer the efficiency of their functioning to a qualitatively new level. Unfortunately, as a means of action, they have characteristic vulnerabilities and can be used not only for good, but also for harm. For the state, as a guarantor of the stability of a civilized society, the issue of ensuring the security of information processing is particularly important. Despite the automation of many information processes, the most vulnerable link in the work of information systems remains a person. A person acts as an operator of information systems and a consumer of information. The entire service process depends on the competence of the operator and the quality of his perception. There are areas of government activity where the cost of error is particularly high. These include ensuring the life and health of citizens, protecting public order and the state system, and ensuring territorial integrity. The specifics of the spheres must be taken into account when ensuring the security of information. This study concerns official activities that are provided by paramilitary groups. Currently, there is a discrepancy in the level of competence of new personnel in the first months of service. The author traces the shortcomings of general and special professional qualities in the field of information security. The purpose of the study is*

*to substantiate certain pedagogical means of forming cadets ' readiness to ensure information security. As forms of theoretical knowledge, we will use the traditional hypothesis and model, as well as functionally distinguishable judgments – problem, assumption, idea and principle. Empirical forms of knowledge will be observation (experimental method) and fixation of facts. To evaluate the effectiveness of the developed pedagogical tools, we use statistical methods: observation (documented and interrogated) and calculation of generalizing indicators. To formulate conclusions, we will use logical methods: building conclusions and argumentation. The approbation of certain pedagogical tools described in this article showed a significant positive trend in terms of competence in information security issues.*

**Keywords:** *components of readiness, ensuring information security, formation of readiness, organizational and pedagogical conditions, professional competence, professional readiness, professionally important qualities.*

## **Введение** **Introduction**

Массовое внедрение информационных технологий в деятельность государственных структур позволило перевести эффективность их функционирования на качественно новый уровень. К сожалению, в роли средств деятельности они имеют характерные уязвимости, а также могут использоваться не только во благо, но и во вред. Для государства, как гаранта стабильности цивилизованного общества, вопрос обеспечения безопасности обработки информации особенно важен. Несмотря на автоматизацию многих информационных процессов, наиболее уязвимым звеном в работе информационных систем остается человек. Человек выступает в роли оператора информационных систем и потребителем информации. От компетентности оператора в первом случае и качества восприятия им сведений во втором зависит весь процесс обслуживания. Существуют сферы деятельности государства, где цена ошибки особенно велика. К ним относится обеспечение жизни и здоровья граждан, охрана общественного порядка и государственного строя, обеспечение территориальной целостности. Особенности сфер необходимо учитывать при обеспечении безопасности информации. Данное исследование касается служебной деятельности, которая обеспечивается военизированными формированиями. В настоящее время наблюдается несоответствие уровня компетентности новых кадров в первые месяцы службы. Прослеживаются недостатки общих и специальных профессиональных качеств в вопросах обеспечения информационной безопасности. Это затягивает интеграцию работника в полноценную служебную деятельность и подрывает общий уровень обеспечения безопасности информации в подразделении.

Цель исследования – обоснование отдельных педагогических средств формирования готовности курсантов к обеспечению информационной

безопасности. Объект исследования – формирование готовности курсантов ведомственных образовательных организаций к обеспечению информационной безопасности в профессиональной деятельности. Предмет исследования – практическая реализация ранее разработанной педагогической модели формирования готовности курсантов к обеспечению информационной безопасности. Гипотеза исследования данной статьи заключается в том, что если создать ряд педагогических средств, компенсирующих основные недостатки реализации образовательной программы по профилю информационной безопасности, то формирование готовности к ее обеспечению будет иметь более высокую степень эффективности. Для проверки предположения решим задачи: – представления теоретических оснований для разработки педагогических средств; – описания педагогических средств как практической реализации, теоретически обоснованных подходов к решению проблемы; – представление первичных результатов эмпирических исследований по внедрению педагогических средств.

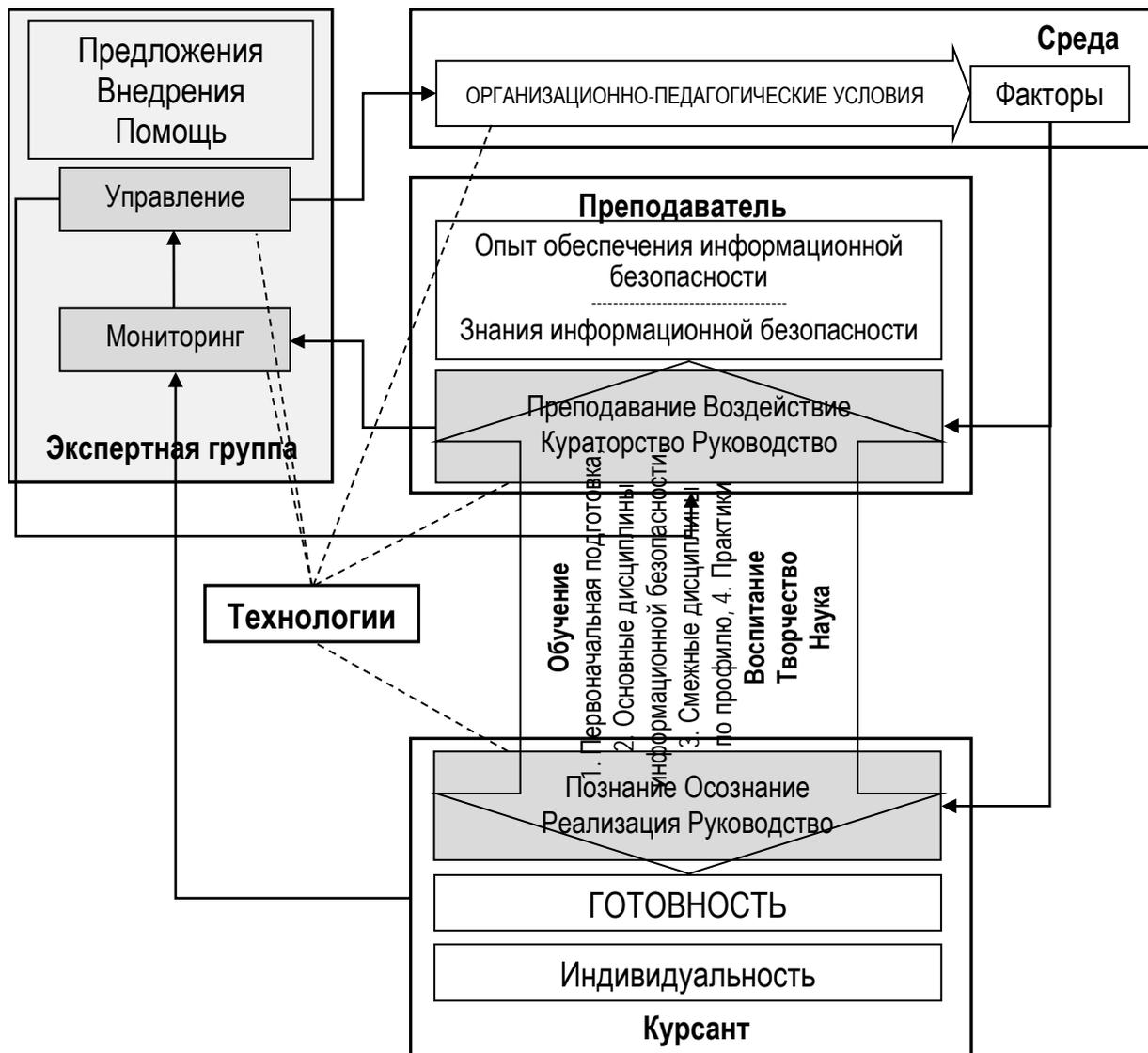
В качестве форм теоретического познания будем использовать традиционные гипотеза и модель, а так же функционально различаемые суждения – проблема, предположение, идея и принцип. Эмпирическими формами познания послужат наблюдение (экспериментальный способ) и фиксация фактов. Чтобы оценить эффективность разработанных педагогических средств используем методы статистики: наблюдение (документированным и опросным способом) и расчет обобщающих показателей. Для формулирования выводов воспользуемся логическими методами: построения умозаключений и аргументации.

### **Теоретическая основа темы** *The Theoretical Background*

Проведенные ранее авторские исследования (Kirillova & Dvoreckij, 2018) показали, что готовность к обеспечению информационной безопасности в профессиональной деятельности (составляющая профессиональной компетентности) является интегративным образованием в структуре личности. Компонентами такой готовности курсантов представляются: теоретический, практический, теоретико-практический, воспитательный. Компоненты готовности вначале рассматривались через общую структуру деятельности (целеполагание, планирование, активность, анализ), затем через анализ противоречий формирования готовности при освоении образовательной программы в условиях ведомственной организации (проблемы планирования и реализации программы, персональные трудности обучаемых). Общий

показатель готовности складывается из оценок полноты формирования компонентов по параметрам. Для ранжирования параметров изучалась востребованность профессионально-важных качеств среди специалистов по информационным технологиям и безопасности. Значимость параметров компонент готовности в порядке убывания выглядит следующим образом: 1) знания и самоконтроль; 2) умения и установки; 3) навыки и оценки, 4) привычки; 5) знания способа деятельности; 6) отношения; 7) уровень развития. В итоге были выявлены направления, последовательность, и ожидаемые результаты педагогического воздействия для формирования готовности по всем составляющим.

Сообразно области научных интересов авторов изыскания были ограничены организационно-педагогическими условиями формирования готовности в образовательном процессе ведомственной организации (Dvoreckij, 2017). Для уточнения их состава был исследован сам процесс, система, в которой он протекает и среда. Структура процесса дала возможность выявить внешние (актуальное состояние обеспечения информационной безопасности в ведомстве, потребности общества в эффективности функционирования ведомства и возможностей для его обеспечения) и внутренние (качество управления образовательным процессом в ведомственной организации) факторы создания организационно-педагогических условий. Структура образовательной системы ведомственной организации позволила выявить системные связи организационно-педагогических условий с другими компонентами, а характер внешних связей дал возможность уточнить их актуальный состав и оценить возможности их улучшения. Было определено, что организационно-педагогические условия – это совокупность актуально доступных информационных, учебно-методических, кадровых, материально-технических ресурсов, системы документирования управления реализацией образовательной программы, методик контроля и оптимизации освоения образовательной программы, регламентирующая содержание, обеспечивающая функционирование и развитие педагогической системы для достижения компетентности курсантов. Те условия, что будут удовлетворять критериям необходимости и достаточности станут причинами целесообразной активности педагогов и обучаемых для формирования требуемой готовности (см. рис. 1).



*Рисунок 1. Модель формирования готовности курсантов к обеспечению информационной безопасности в профессиональной деятельности*  
 Figure 1 Model of Formation of Cadets' Readiness to Ensure Information Security in Their Professional Activities

Главные авторские идеи повышения результативности формирования готовности курсантов к обеспечению информационной безопасности в профессиональной деятельности: поэтапное формирование готовности на стадиях, отчетливо различаемые при осуществлении образовательной программы в ведомственных образовательных организациях (первоначальная подготовка, основные дисциплины информационной безопасности, смежные дисциплины по профилю, практики); осуществление качественного педагогического сопровождения (Solov'eva & Makarkina, 2015) по всем направлениям деятельности участников образовательного

процесса (учеба, воспитание, творчество, наука); создание экспертной группы по вопросам информационной безопасности (коллегиального органа) в составе управляющего органа. При этом комплекс педагогического воздействия ориентируется на актуально востребованные в профессиональной среде специалистов по информационной безопасности качества, а учебно-воспитательный процесс учитывает индивидуальные достижения курсантов. Это позволит поддерживать уровень готовности на приемлемом значении после достижения основных показателей в течение всего освоения образовательной программы. Образовательный процесс по профилю инфобезопасности с традиционно проработанным обучением предметно и акцентированно дополнится всеми видами педагогического взаимодействия. А именно, воспитательным воздействием со стороны преподавателя с ожидаемым осознанием у курсанта, отношениями куратора творческой реализации курсанта, взаимодействием научного руководителя по исследовательской работе курсанта. Казарменные условия проживания курсантов на территории ведомственного учреждения дадут реализовать практико-ориентированный подход в профессиональной подготовке (Kolesnikova & Ushkov, 2017), так как режим деятельности, объекты информатизации образовательной организации и практического учреждения схожи. Технологичность обязательно должна присутствовать в образовательной системе как гарант получения рационального уровня образования. Образовательным технологиям отводится роль средства разработки условий и формы их существования. Результаты изысканий и предложений были представлены в виде графической модели.

На рисунке можно наблюдать основные элементы, влияющие на формирование требуемой готовности курсанта. Видно, что индивидуальность курсанта является неотъемлемой частью его личности и образовательный процесс строится с учетом этого обстоятельства. Преподаватель находится с курсантом в педагогическом взаимодействии под влиянием среды, стимулируя возможности к самообразованию (Luzgin, 2017). Среда настраивается коллегиальными силами организаторов процесса на основе непрерывного наблюдения за результатами готовности курсанта сообразно частной образовательной цели. Усилия по направлениям педагогического взаимодействия также подвергаются корректировке, однако это не должно усложнять процесс и оставаться в рамках используемых педагогических технологий. Разработанная модель обоснована, уточнена на основе авторских идей, и полученные знания обогащают теоретико-методологические представления об организационно-педагогических условиях формирования профессиональной готовности.

## **Результаты эмпирического исследования** ***The Results of Empirical Research***

Для практической реализации модели на текущем этапе были учтены лишь наиболее востребованные на практике профессионально-важные качества по обеспечению информационной безопасности и недостатки в профессиональной подготовке по профилю, исправление которых требует наименьшие затраты ресурсов. Осуществлены следующие мероприятия по разработке педагогических средств: переработана общепринятая структура (тематика) учебной дисциплины «Информационная безопасность» с пересмотром требований к результатам обучения, описаны критерии и показатели оценивания компетенций, внедрен соответствующий курс лекций; разработаны практические рекомендации по управлению информационными рисками для сотрудников, осуществляющих деятельность в условиях непосредственного контакта с потенциальным злоумышленником; подготовлены вспомогательные материалы для организации работы с курсантами ведомственных образовательных организаций по формированию готовности к обеспечению информационной безопасности в профессиональной деятельности учебного, воспитательного, творческого, научного характера.

Предварительные исследования показали, что учебная дисциплина «Информационная безопасность» стандартна для любого уровня профессионального образования и не учитывает профиль подготовки. Тематика дисциплины имеет явно выраженный технический уклон. Фактически представляет собой набор стандартов по безопасности без всякой систематизации. Очевидно, что это следствие относительно новой отрасли знаний. То есть изначально отсутствует универсальная часть знаний. Вводная тема должна содержать подробнейшее рассмотрение всех базовых понятий дисциплины во взаимосвязи между собой и с более общими понятиями. В новой области знаний не допускается простое изложение терминов перечнем. А уже из отношений понятий можно выделить специфические термины. Такой подход поднимает познавательную мотивацию. Должна присутствовать тема обеспечения информационной безопасности. С дидактической точки зрения правильно изучить общую схему процесса, чтобы представлять последовательность операций, возможные способы взаимодействия со специалистами по безопасности и другими организациями. И объективно необходима тема, ориентированная на профиль образования, образовательный и профессиональный стандарт. В этом разделе необходимо уточнить общие сведения применительно к специфике предстоящей практической деятельности, рассмотреть вопросы прикладного характера. Например, для технического профиля подойдет

изложение специальных стандартов безопасности и защиты информации, гуманитарного – рассмотрение информационных противоречий, юридического – анализ правонарушений в информационной сфере. Проработка структуры учебного курса позволяет более отчетливо отслеживать междисциплинарные связи. Таким образом, для служебной деятельности военизированных подразделений тематика учебной дисциплины и разработанный курс лекций содержат разделы: «Введение в теорию информационной безопасности», «Система управления информационной безопасностью», «Конфликты и правонарушения в информационной сфере». В первой теме представлены теоретические основы информационной безопасности, раскрыты правовые источники, сущность и содержание деятельности по обеспечению информационной безопасности. Во второй теме представлены сведения о порядке разработки единой политики информационной безопасности, организации управления информационными рисками, проектировании системы управления информационной безопасностью, построении системы защиты информации, аттестации объектов информатизации по требованиям безопасности информации, эксплуатации объектов информатизации с использованием системы защиты информации, управлении инцидентами нарушения информационной безопасности. В третьей теме представлены сведения о понятии, структуре конфликта в информационной сфере, особенностях информационного противоборства и профилактике данных явлений. Так же рассматриваются правонарушения в информационной сфере как не уголовного, так и преступного характера. Характеризуется киберпространство с точки зрения безопасности. Даются рекомендации по профилактике информационных правонарушений. Отдельный вопрос посвящен информационным конфликтам, противоборству в экстремальной среде и информационным правонарушениям в учреждениях, где обращение информации строго регламентировано. Разработанные документы (паспорта компетенций, рабочие программы, оценочные средства) содержат требования к результатам обучения по компонентам и этапам, начиная с первоначальной подготовки и заканчивая практикой.

Практические рекомендации по управлению информационными рисками для сотрудников отражают один из подходов к обеспечению информационной безопасности. Данный подход наиболее соответствует практической деятельности, напрямую не имеющей отношение к обслуживанию вычислительной и коммуникационной техники. Акцент для служебной деятельности, связанной с использованием оружия и специальных средств, сделан на условия антагонистического характера. Рекомендуются методики оценки информационных рисков, типовые приемы и средства защиты информации, особенности безопасного

обращения с распространёнными информационными технологиями. Особое внимание уделяется безопасному поведению и общению с целью недопущения раскрытия конфиденциальной информации. Приводятся примеры стандартных угроз, типовых информационных атак и провокационных действий. Предлагаются предпочтительные варианты выхода из опасной ситуации.

Для организации работы по всем направлениям педагогического взаимодействия с курсантами в целях формирования требуемой готовности подготавливается самый разнообразный материал. Решаемые задачи: активизация познавательной активности обучаемых; поэтапное формирование компетентности с последующим поддержанием ее на требуем уровне; документальное обеспечение образовательного процесса; использование условий проживания курсантов как практического полигона. Учебное пособие дополняет курс лекций и другое учебно-методическое обеспечение по профильным и смежным дисциплинам, учитывая предыдущий уровень образования. Дополнительные материалы по объему соответствуют трудоемкости затрагиваемых дисциплин, запланированных в рабочем учебном плане, и их содержанию. Пособие согласовывается с типовыми ежегодными планами воспитательных, научных, творческих, спортивных, культурно-досуговых мероприятий, графиком служебной подготовки. Наименование разделов: «Общие положения по обеспечению образовательного процесса»; «Учебные материалы и самостоятельная работа»; «Материалы для воспитательной работы»; «Исследовательские и творческие задания»; «Материалы для занятий по служебной подготовке».

В рамках этой статьи подготовлены наиболее существенные результаты мероприятий по практической реализации модели, описанной в разделе о теоретических исследованиях. С целью проверки эффективности разработанной модели процесса формирования готовности курсантов к обеспечению информационной безопасности в профессиональной деятельности были проведена опытная проверка с контрольной и экспериментальной группой методами математической статистики для обнаружения отличий до и после внедрения педагогических средств. Контрольная и экспериментальная группы в количестве по 24 курсанта из числа обучаемых Псковского филиала Академии ФСИН России. Такое разбиение удалось достичь за счет того, что занятия проводятся изначально в подгруппах. Объем выборки дает достаточно объективный результат в виду высокой степени однородности исследуемых единиц (обучаемых). Такое допущение оправдывается реализацией обучения по типовой программе. Первое измерение уровня компетентности контрольной и экспериментальной групп по вопросам информационной

безопасности состоялось на первоначальной подготовке в августе 2019 года. Второе измерение – после окончания второго семестра обучения (завершение курса основных дисциплин по информационной безопасности). Измерения уровня компетентности осуществлялось путем комплексной экспертной оценки каждого курсанта путем опросов, собеседований, тестирований на знания, проверки умений, навыков, изучения опыта, исследований воспитательного компонента (тесты на склонность к риску, на внимание, мотивацию). Оценка складывалась по методике, разработанной авторами эталонной компетентностной модели достаточного специалиста по вопросам информационной безопасности среди сотрудников. Ситуационный сдвиг у контрольной группы без экспериментального воздействия и у экспериментальной группы со специально созданными экспериментальными условиями по осредненному показателю готовности составил +13%.

Практическая значимость полученных результатов исследования выражается в возможности использования образовательными организациями военизированных формирований методики создания организационно-педагогических условий при проектировании ресурсов, подготовке системы документации, оптимизации средств контроля образовательного процесса для повышения эффективности формирования общекультурных компетенций информационного профиля и профессиональной компетентности в вопросах обеспечения информационной безопасности. Практические органы могут использовать методические и практические рекомендации для проведения занятий по служебной подготовке, инструктажей, организации информирования об инцидентах информационной безопасности и актуальных угрозах личному составу и безопасности службы со стороны киберпреступности.

## **Выводы** *Conclusions*

Противоречие между желаемым качеством подготовки курсантов к обеспечению информационной безопасности в профессиональной деятельности и действительным подтверждается экспертными оценками, а также результатами текущей успеваемости. Одним из путей разрешения противоречия является переработка имеющихся и создание вспомогательных педагогических средств организации образовательного процесса с целью устранения объективных недостатков в нем. Педагогические средства создадут условия для повышения эффективности взаимодействия участников процесса и самостоятельной деятельности. Реализация замысла не требует привлечения значительных дополнительных ресурсов и

решается силами образовательной организации. Апробация отдельных педагогических средств, описанных в данной статье, показала значительную положительную динамику по показателю компетентности в вопросах информационной безопасности.

### Summary

The article is devoted to the substantiation of certain pedagogical means of forming the readiness of cadets of educational departmental organizations to ensure information security in their professional activities. To study the process of readiness formation, a model of it was constructed and studied. The research conducted earlier by the team of authors showed that the readiness to ensure information security in professional activities (professional competence) is an integrative education in the structure of the individual. A system of professionally important qualities of an information security specialist was developed. The organizational and pedagogical conditions in the educational process of a departmental organization were chosen as the direction of research to improve the effectiveness of the formation of readiness components. The elimination of the objective shortcomings of this process and the use of all available areas of pedagogical interaction does not overload it, but only optimizes it. The practical implementation of the model of the process flow focused on the conditions took place in the development, implementation and evaluation of the effectiveness of the pedagogical tools presented in the article.

### Литература References

- Dvoreckij, D. (2017). Teoretiko-metodologicheskie osnovy issledovanija pedagogicheskikh uslovij formirovanija gotovnosti kursantov FSIN k obespecheniju informacionnoj bezopasnosti. *Mezhdunarodnyj nauchno-issledovatel'skij zhurnal*, 11 (2-65), 103-105. DOI: 10.18454/IRJ.2227-6017
- Kirillova, T., & Dvoreckij, D. (2018). Osnovnye tendencii i zakonomernosti formirovanija gotovnosti k obespecheniju informacionnoj bezopasnosti. *Pravo i obrazovanie*, 12, 13-21.
- Kolesnikova, N., & Ushkov F. (2017). Praktiko-orientirovannaja professional'naja podgotovka v Pskovskom filiale Akademii FSIN Rossii. *Issledovanija pskovskih uchenyh v sfere duhovno-nravstvennogo vospitaniya i psihologo-pedagogicheskogo obrazovanija : materialy Mezhvuzovskogo nauchno-metodicheskogo seminara, posvjashhennogo Dnju rossijskoj nauki (Pskov, 08 fevralja 2017 goda)*, 51-54.
- Luzgin, S. (2017). Lichnostno-professional'noe samosovershenstvovanie sotrudnikov ugovovno-ispolnitel'noj sistemy. *Vedomosti ugovovno-ispolnitel'noj sistemy*, 10 (185), 24-28.
- Solov'eva, T., & Makarkina, O. (2015). Innovacionnaja dejatel'nost' v sisteme povyshenija kvalifikacii kak faktor rosta professional'noj kompetentnosti prepodavatelej vedomstvennyh obrazovatel'nyh organizacij. *Pravo i obrazovanie*, 6, 69-75.