

Сабельников С. А., Астахова Л. В.

МЕТОДИКА РЕАЛИЗАЦИИ ПЕДАГОГИЧЕСКИХ УСЛОВИЙ РАЗВИТИЯ ПРОЕКТНО-УПРАВЛЕНЧЕСКОЙ КОМПЕТЕНЦИИ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

В статье обоснована методика последовательной реализации комплекса педагогических условий развития проектно-управленческой компетенции будущих специалистов по защите информации. Научная новизна методики заключается в отражении связи проектно-управленческой компетенции с реально существующими в профессиональной деятельности специалиста по защите информации этапами проектирования в этой сфере; использовании инновационных методов оценки специфического ресурсного обеспечения проектов по защите информации; применении автоматизированных средств управления проектами по защите информации на разных этапах его разработки. Методика реализована на трех этапах: мотивационно - адаптивном, профессионально - формирующем (исполнительном) этапе и профессионально-закрепляющем этапе, соответствующих структуре проектно-управленческой компетенции специалиста по защите информации. Реализация комплекса педагогических условий в образовательном процессе показала, что произошли статистически значимые изменения в уровне развития проектно-управленческой компетенции у будущих специалистов по защите информации в вузе.

Ключевые слова: проектно-управленческая компетенция, специалист по защите информации, информационная безопасность.

Sabelnikov S. A., Astahova L. V.

METHODS OF IMPLEMENTATION OF PEDAGOGICAL CONDITIONS OF PROJECT- MANAGEMENT COMPETENCE OF THE FUTURE OF INFORMATION PROTECTION SPECIALISTS

The article describes the methods of the consistent set of pedagogical conditions of formation the project-management competence of the future information protection specialists. Novelty of the methods is the connection between project-management competence and the real design stages in the field of project-management; the use of innovative assessment criteria of specific resources provision of information protection projects and the application of automated project management systems at the different stages of developing. The methodology is implemented in three stages: motivational - adaptive, professional - forming (executive) and professional - imprinting, which conform to the structure of project management competence

of the information protection specialists. The implementation of complex pedagogical conditions in the educational process resulted in statistically significant modification of developmental level in project-management competence of the future information protection specialists.

Keywords: *project-management competence, information security specialist, information security.*

Исследование проблемы формирования проектно-управленческой компетенции будущих специалистов по защите информации позволило разработать модель развития данной компетенции и определить педагогические условия ее реализации в системе высшего образования. На основе теоретического осмысления проблемы выдвинуто предположение, согласно которому развитие проектно-управленческой компетенции у будущих специалистов по защите информации будет происходить эффективно при реализации следующего комплекса педагогических условий: создание, адаптация и внедрение в содержание отдельных учебных дисциплин компонентов видовой структуры проектно-управленческой компетенции по защите информации; использование технологий проектной деятельности в организации учебного процесса при подготовке специалистов по защите информации; ориентация учебного процесса на использование автоматизированных систем управления проектами по защите информации¹. Однако методика реализации определенных нами педагогических условий на сегодняшний день не разработана. Актуальность данного исследования выражена в необходимости обосновать методику реализации педагогических условий развития проектно-управленческих компетенций у будущих специалистов по защите информации в вузе.

В исследовании принимали участие 510 студентов, обучающихся по специальностям 100503 «Информационная безопасность автоматизированных систем», 100505 «Безопасность информационных технологий в правоохранительной сфере» на кафедре «Безопасность информационных систем» факультета компьютерных технологий, управления и радиоэлектроники Южно-Уральского государственного университета в 2013 – 2016 гг. При выборе периода проведения опытно-экспериментальной работы мы руководствовались накопленным опытом подобного рода исследований в педагогической науке, который позволил установить, что формирование особого вида компетенции занимает в среднем 3 года. В опытно-экспериментальной ра-

боте были задействованы 7 групп студентов: контрольные группы (КГ1, КГ2), экспериментальные группы (ЭГ1, ЭГ2, ЭГ3, ЭГ4, ЭГ5). В рамках исследования были приняты критерии сформированности проектно-управленческих компетенций у будущих специалистов по защите информации:

1. Когнитивный компонент (владение терминологией в сфере защиты информации, нормативной правовой базой, знание видов информационных технологий защиты информации);

2. Интегративно-деятельностный (понимание поставленной цели проекта по защите информации, определение набора возможных решений, анализ конкретной ситуации, выбор средств защиты для ее решения);

3. Личностный (потребность в информации в сфере защиты информации и наличие целевой установки на ее получение).

Нами были определены уровни сформированности проектно-управленческой компетенции специалиста по защите информации: низкий, средний, высокий. Диагностическая программа включала в себя методы: тестирование, интервьюирование, опрос, и т.д. На основании результатов исследования нами вносились коррективы в методику развития проектно-управленческой компетенции специалиста по защите информации.

Опытно-экспериментальная работа состояла из следующих этапов:

Этап I:

Определялось состояние изученности проблемы развития проектно-управленческой компетенции будущих специалистов по защите информации в отечественной и зарубежной науке и практике образовательных и высших учебных заведений, определялись наиболее эффективные направления решения; Уточнялись и дополнялись структурно-содержательные характеристики модели развития проектно-управленческой компетенции будущих специалистов по защите информации;

Определялись критерии и показатели уровней развития проектно-управленческой компетенции будущих специали-

стов по защите информации, разрабатывалась диагностическая программа; Проводилось определение уровня развития проектно-управленческой компетенции студентов контрольной группы КГ1 и экспериментальных групп ЭГ1, ЭГ2.

Реализовывался комплекс педагогических условий в образовательном процессе в экспериментальных группах ЭГ1-2.

Этап II:

- Продолжение реализации комплекса педагогических условий в ЭГ1-2;
- Проведение первого и второго диагностических срезов в экспериментальных и контрольных группах;
- В опытно-экспериментальную работу включена ЭГ3. Проведение определения уровня развития проектно-управленческой компетенции будущих специалистов по защите информации в ЭГ3.
- Реализация комплекса педагогических условий развития проектно-управленческой компетенции будущих специалистов по защите информации в ЭГ3.

Этап III:

- Проведение третьего диагностического среза в экспериментальной и контрольной группе;
- Завершение реализации комплекса педагогических условий развития проектно-управленческой компетенции будущих специалистов по защите информации в экспериментальных группах;
- Проведение итогового диагностического среза в экспериментальных и контрольных группах;
- Теоретическое осмысление и интерпретация данных, полученных в ходе опытно-экспериментальной работы;
- Оформление результатов и формулировка выводов проведенного исследования.

Методика реализации первого педагогического условия (создание, адаптация и внедрение в содержание отдельных учебных дисциплин компонентов видовой структуры проектно-управленческой компетенции по защите информации) предусматривала выполнение двух задач:

1. Изменение содержания дисциплин с учетом развития проектно-управленческой компетенции будущих специалистов по защите информации;

2. Обновление учебно-методических комплексов дисциплин, в рамках которых происходит развитие проектно-управленческой компетенции будущих специалистов по защите информации.

В процессе работы мы руководствовались принципом системности и последовательности, в основе которого лежит утверждение о том, что использование на практике полученных в процессе обучения знаний возможно только в случае, если они приведены к определенной логической системе. В основу исследования было положено определение понятия «*проектно-управленческая компетенция специалиста по защите информации*» – это способность специалиста применять знания, умения и личные качества для успешной профессиональной деятельности, выражающейся в объединении взаимосвязанных по времени и ресурсам процессов, нацеленных на достижение целей защиты информации (конфиденциальность, целостность, доступность) на всех уровнях, стадиях реализации проекта с определенными мерами обеспечения требуемого уровня защиты информации². На основании структуры управленческой компетенции специалиста по защите информации, определенной в авторской монографии³, в структуру проектно-управленческой компетенции специалиста по защите информации мы включили:

1. Методологический компонент, отражающий сущность управления проектами по защите информации: информационная и информационно-аналитическая компетенции.

2. Объектно-содержательные компоненты, отражающие способность специалиста по защите информации оказывать влияние на различные объекты управления проектами по защите информации включают в себя:

1) Компетенции руководителя (администратора) проекта по защите информации (способность осуществлять следующие функции управления: планирование проекта по защите информации, организацию проекта по защите информации, контроль трудовых, финансовых и материально-технических ресурсов проекта по защите информации);

2) Многоуровневые компетенции (способность оказывать влияние как на внутреннюю, так и на внешнюю среду проекта по защите информации): стратегическое управление программой

проектов, портфелем проектов, проектом по защите информации; управление инновациями (в том числе автоматизацией) в области управления проектами по защите информации, управление изменениями человеческого капитала команды проекта);

- 3) Компетенции управления собственной эффективностью как участника команды проекта по защите информации (способность к самодиагностике, самоорганизации, саморазвитию, в том числе к развитию своего человеческого капитала: информационного мировоззрения и культуры информационной безопасности и пр.).

В своем исследовании мы пришли к выводу, что данные компетенции могут развиваться последовательно в рамках четырех дисциплин: «Основы информационной безопасности», «Управление информационной безопасностью», «Технологии защиты информации в различных отраслях деятельности», «Комплексные системы защиты информации». Обратим внимание, что разделение компетенций по дисциплинам является достаточно условным и зависит от этапа формирования компетенций.

На первом, мотивационно - адаптивном этапе (1 – 2 курс) происходит развитие информационной и информационно-аналитической компетенций и компетенций руководителя проекта по защите информации. Особое внимание уделяется развитию мотивации получения студентами информационно-когнитивных знаний, умений и навыков⁴, а также их использования в процессе реализации четырех ключевых функций управления проектами в сфере профессиональной защиты информации.

На втором, профессионально-формирующем (исполнительном) этапе (3 – 4 курс) развиваются многоуровневые профессиональные компетенции в области управления проектами по защите информации. При этом делается акцент на развитие способности студента управлять инновациями в проектной деятельности по защите информации, изменениями человеческого и культурного капитала команды проекта. Согласно современным тенденциям практики управления информационной безопасностью, качество защиты информации недостижимо без наличия этих способностей специалиста⁵. В нашей работе использовались инновационные мето-

дики оценки культурного капитала организации в контексте обеспечения информационной безопасности⁶.

На третьем, профессионально-закрепляющем этапе (5 курс) развиваются компетенции управления собственной эффективностью студента, в т.ч. его культурного капитала как участника команды проекта по защите информации. На данном этапе закрепляются личностные качества, необходимые для управления проектами в сфере защиты информации, появляется устойчивая потребность и способность к самодиагностике и саморазвитию в этой динамичной сфере.

Как видно, развитие проектно-управленческой компетенции будущих специалистов по защите информации происходит по пути постепенного увеличения сложности осваиваемого учебного материала.

Второй задачей при реализации первого педагогического условия было обновление учебно-методических комплексов названных дисциплин, в рамках которых происходит развитие проектно-управленческой компетенции будущих специалистов по защите информации. Программы дисциплин «Основы информационной безопасности», «Управление информационной безопасностью», «Технологии защиты информации в различных отраслях деятельности» и «Комплексные системы защиты информации» были обновлены с выделением отдельных теоретических аспектов управления проектами, опирающимися на цели защиты информации (конфиденциальность, целостность, доступность) в каждой дисциплине, и включением практического компонента по управлению ресурсами проекта по защите информации.

При реализации второго педагогического условия (использование технологий проектной деятельности в организации учебного процесса при подготовке специалистов по защите информации) использовался междисциплинарный практический компонент по работе с кейсами, последовательно реализуемых в процессе подготовки специалистов по защите информации. Метод кейсов является технологией развивающего обучения. С помощью процедур коллективного развития формируется набор личных качеств необходимых в управлении проектами по защите информации (ответственность, нацеленность на результат, лидерские качества, коммуникативность и др.).

На первом, мотивационно - адаптивном этапе (1 – 2 курс) в рамках дисциплины «Основы информационной безопасности» осуществлялось общее знакомство с этапами разработки проекта по защите информации, обучение разработке концепции проекта и определению требований к проекту по защите информации.

На втором, профессионально - формирующем (исполнительном) этапе (3 – 4 курс) в рамках дисциплин «Технологии защиты информации в различных отраслях деятельности» и «Управление информационной безопасностью» осуществлялось обучение технологиям разработки эскизного и технического проектов системы защиты информации и сопроводительной документации.

На третьем, профессионально-закрепляющем этапе (5 курс) в рамках дисциплины «Комплексные системы защиты информации» осуществлялось обучение технологиям ввода проекта по защите информации в эксплуатацию и сопровождения проекта.

В ходе реализации второго педагогического условия для развития профессиональных компетенций в области поэтапного управления проектами по защите информа-

ции будущих специалистов проектный метод был внедрен с использованием кейсов по каждому этапу управления проектами по защите информации (ГОСТ 34.601-90 Автоматизированные системы. Стадии создания).

Набор кейсов «Управление проектами по защите информации» включал в себя 7 разделов, которые реализовывались в рамках четырех дисциплин в процессе непрерывной подготовки будущих специалистов по защите информации с 1 по 5 курс. Кейсы были составлены нами таким образом, что каждый этап соответствует четко определенной цели, имеет определенный уровень трудности и иллюстрирует несколько аспектов профессиональной деятельности будущих специалистов по защите информации. В процессе подготовки будущих специалистов по мере разбора кейсов (т.е. прохождения ими этапов) решалась задача по формированию определенной компетенции в области управления проектами по защите информации. В рамках выполнения некоторых кейсов студентам необходимо было освоить и применить на практике программные продукты, необходимые для профессиональной деятельности.

Таблица 1

Этапы развития проектно-управленческой компетенции будущих специалистов по защите информации

Этап	Раздел	Результат	Дисциплина
Мотивационно-адаптивный	1. Инициация проекта по защите информации	Концепция проекта по защите информации	Основы информационной безопасности
	2. Формирование требования и разработка технического задания	Техническое задание на создание системы защиты информации	Основы информационной безопасности
Профессионально-формирующий	3. Разработка эскизного проекта СЗИ	Эскизный проект системы защиты информации	Технологии защиты информации в различных отраслях деятельности
	4. Разработка технического проекта СЗИ	Технический проект системы защиты информации	Управление информационной безопасностью
	5. Подготовка рабочей документации по проекту СЗИ	Рабочая документация на проект системы защиты информации	Управление информационной безопасностью
Профессионально-закрепляющий	6. Ввод в эксплуатацию СЗИ	Рабочая документация на ввод системы защиты информации в эксплуатацию	Комплексные системы защиты информации
	7. Сопровождение СЗИ	Гарантийная документация на проект	Комплексные системы защиты информации

С целью более детального изучения использованной методики рассмотрим задачи, решаемые на каждом этапе управления проектом по защите информации в форме кейсов в определенной дисциплине:

1. *Этап «Инициация проекта по защите информации» (дисциплина «Основы информационной безопасности»)*. Первый этап включает в себя группу кейсов, реализация которых в процессе подготовки будущих специалистов по защите информации позволяет изучить способы определения проблемы защиты информации или возможности, определить прогнозируемый результат проекта, определить его приоритет. В рамках данного этапа студенты решают практические задачи в группах, каждая из которых ведет собственный проект по защите информации на протяжении всех этапов реализации методики. На этапе инициации проекта студентам даются ситуации проблемного характера, максимально приближенные к реальным потребностям рынка. Каждая из ситуаций связана с конкретной предметной областью в сфере защиты информации: защита персональных данных, информации, составляющей коммерческую тайну, и т.д. Результатом первого этапа является оформленная в виде документа концепция проекта по защите информации, включающая цель, задачи проекта по защите информации, тип, вид проекта, результаты проекта, требования к качеству, основных участников проекта, границы проекта, необходимые ресурсы, оборудование, сроки реализации, временные ограничения, вехи, движение денежных средств, риски и т.д.

2. *Этап «Формирование требования и разработка технического задания» (дисциплина «Основы информационной безопасности»)*. Второй этап состоит из группы кейсов, реализация которых в педагогической практике направлена на формирования у будущих специалистов компетенции по определению требований и разработке технического задания на внедрение системы защиты информации. В рамках данного этапа студенты решают практические задачи в группах, каждая из которых ведет собственный проект по защите информации, начатый на первом этапе реализации методики. На этапе определения требований и разработки технического задания студентам даются ситуации, связанные с конкретной задачей, в рамках определенной ранее предметной

области, кроме этого определяются ресурсы и внешний факторы, влияющие на проект. Результатом второго этапа является оформленное в виде документа техническое задание на создание системы защиты информации, включающее назначение системы защиты, цель, характеристику объектов системы защиты информации, требования к системе защиты информации, состав и содержание работ по созданию СЗИ, порядок контроля и приемки СЗИ, требования по вводу СЗИ в эксплуатацию, требования к документированию и т.д.

3. *Этап «Разработка эскизного проекта СЗИ» (дисциплина «Технологии защиты информации в различных отраслях деятельности»)*. Третий этап включает в себя группу кейсов, реализация которых в процессе подготовки будущих специалистов по защите информации позволяют изучить способы разработки и совокупность документов, дающих общее представление о назначении, устройстве, принципе работы будущей системы защиты информации. В рамках данного этапа студенты продолжают решать практические задачи в группах, каждая из которых ведет собственный проект по защите информации. На этапе разработки эскизного проекта СЗИ может быть выделено несколько вариантов реализации системы, для каждого из которых составлены схемные решения (эскизы) будущей СЗИ. Эскизный проект служит основанием для разработки технического проекта СЗИ. Результатом третьего этапа является оформленный в виде документа эскизный проект системы защиты информации, включающий структуры входных и выходных данных, уточнение методов достижения цели проекта, общее описание алгоритма достижения цели проекта, технико-экономическое обоснование проекта по защите информации и т.д.

4. *Этап «Разработка технического проекта СЗИ» (дисциплина «Управление информационной безопасностью»)*. Четвертый этап состоит из группы кейсов, реализация которых в педагогической практике направлена на формирования у будущих специалистов компетенции по разработке технического проекта системы защиты информации. На основании разработанного ранее эскизного проекта СЗИ будущие специалисты продолжают решать практические задачи в группах. На этапе разработки технического проекта студентами проводится уточнение

структуры входных и выходных данных, подготовка итогового алгоритма реализации проекта по защите информации, определение структуры входных и выходных данных, определение конфигурации технических средств защиты информации, определение настроек программного обеспечения и т.д. Результатом четвертого этапа является оформленный в виде документа технический проект системы защиты информации, включающий: определение формы представления входных и выходных данных, план мероприятий по внедрению системы защиты информации и т.д.

5. *Этап «Подготовка рабочей документации по проекту СЗИ» (дисциплина «Управление информационной безопасностью»)*. Пятый этап включает в себя группу кейсов, реализация которых, в процессе подготовки будущих специалистов по защите информации позволяют изучить методику разработки рабочей документации на систему защиты информации и ее компоненты. На основе проектной документации, разработанной студентами, ранее реализуется этап разработки рабочей документации. На данном этапе будущими специалистами по защите информации проводится разработка документов, которые описывают проведение пуско-наладочных работ СЗИ, календарный план проведения работ, сметную документацию и т.д. Результатом пятого этапа является оформленная в виде документов рабочая документация на проект системы защиты информации.

6. *Этап «Ввод в эксплуатацию СЗИ» (дисциплина «Комплексные системы защиты информации»)*. Шестой этап включает в себя группу кейсов, реализация которых в процессе подготовки будущих специалистов по защите информации позволяют изучить методику подготовки системы защиты информации для ввода в действие. На этапе ввода в эксплуатацию студентами проводится изучение методик подготовки персонала, описание строительно-монтажных работ, описание пусконаладочных работ, проведение предварительных и эксплуатационных испытаний и т.д. Результатом шестого этапа является оформленная в виде документов рабочая документация на ввод системы защиты информации в эксплуатацию.

7. *Этап «Сопровождение СЗИ» (дисциплина «Комплексные системы защиты информации»)*. Седьмой этап включает в себя

группу кейсов, реализация которых в процессе подготовки будущих специалистов по защите информации позволяют изучить методы сопровождения СЗИ после ввода в эксплуатацию. На этапе сопровождения СЗИ студентами проводится изучение методик гарантийного и послегарантийного обслуживания системы защиты информации. Результатом седьмого этапа является оформленная гарантийная документация на проект по защите информации.

Третье педагогическое условие (ориентация учебного процесса на использование автоматизированных систем управления проектами по защите информации) также реализовывалось на всех этапах. На мотивационно-адаптивном этапе в рамках изучения курса «Основы информационной безопасности» в процессе аудиторной работы студенты были ознакомлены с существующими программными комплексами по управлению проектами (Jira, 1С:PM, «Битрикс24», Microsoft Project, д.р.). На профессионально-формирующем этапе в рамках дисциплины «Технологии защиты информации в различных отраслях деятельности» осуществлялось практико-ориентированное изучение программного комплекса «1С:PM Управление проектами», обеспечивающего автоматизированную поддержку жизненного цикла проектов по защите информации, планирование и управление работами, соответствие российским стандартам и требованиям в области управления проектами (ГОСТ Р 54869 2011. Проектный менеджмент. Требования к управлению проектом). Этап освоения программного продукта соответствует этапу жизненного цикла проекта по защите информации. На профессионально-закрепляющем этапе в рамках дипломного проектирования будущими специалистами осуществляется выполнение реальных проектов по защите информации по заявкам работодателей с использованием данного комплекса.

После реализации обоснованной методики результаты итогового среза показали, что уровень компетенций в области управления проектами по защите информации у будущих специалистов повысился. Из 510 студентов 134 человек показали высокий уровень развития компетенций в области управления проектами по защите информации, 280 студентов – средний уровень развития компетенций, 96 – низкий уровень.

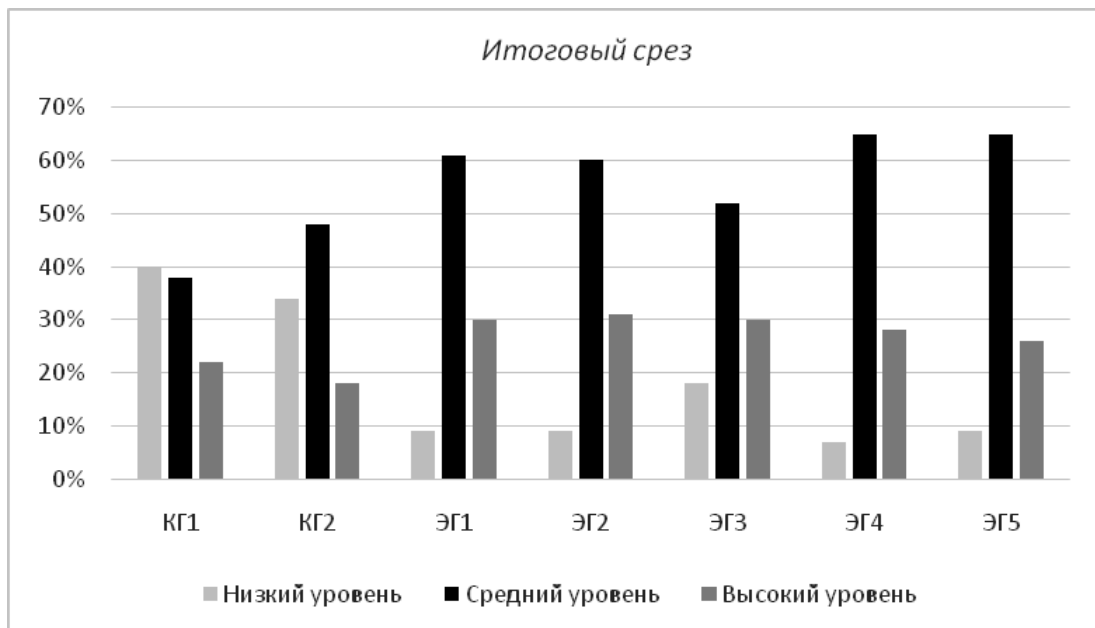


Рис.1. Распределение студентов по уровням развития проектно-управленческих компетенций. Итоговый срез

Более высокие результаты показали студенты экспериментальных групп. Результаты итогового среза приведены на рис. 1.

Таким образом, руководствуясь результатами опытно-экспериментальной работы можно утверждать, что достижение уровня развития компетенции в области управления проектами по защите информации у будущих специалистов обусловлено влиянием реализованного в процессе непрерывной подготовки комплекса педагогических условий: создание, адаптация и внедрение в содержание отдельных учебных дисциплин компонентов видовой структуры компетен-

ций в области управления проектами по защите информации, использование технологий проектной деятельности в организации учебного процесса при подготовке специалистов по защите информации, ориентация учебного процесса на использование автоматизированных систем управления проектами по защите информации. Методика реализации названных педагогических условий обеспечивает целенаправленный поэтапный переход на более качественный уровень развития проектно-управленческой компетенции будущих специалистов по защите информации.

Примечания

1. Сабельников С.А., Астахова Л.В. Модель развития компетенций в области управления проектами по защите информации в вузе // Вестник Челябинского государственного педагогического университета. 2016. №4. С.76-84.
2. Сабельников С.А. Проблема определения понятия компетенции в области управления проектами специалиста по защите информации // Современные проблемы науки и образования. 2015. №6-0. С.392.
3. Астахова, Л.В. Управленческая компетенция специалиста по защите информации: монография / Л.В. Астахова. - Челябинск: Издательский центр ЮУрГУ, 2014. – С. 78-80.
4. Астахова, Л.В. Понятие информационной компетенции специалиста: когнитивный подход // Вестник Южно-Уральского государственного университета. Серия: Образование. Педагогические науки. 2013. Т. 5. № 4. С. 10-16.
5. Astakhova L.V. Evaluation Assurance Levels for Human Resource Security of an Information System // Procedia Engineering. 2015. N29. С.635-639.
6. Astakhova L.V. Information security: risks related to the cultural capital of personnel (review). Scientific and Technical Information Processing. 2015. Т. 42. № 2. С. 41-52.

САБЕЛЬНИКОВ Сергей Александрович, преподаватель кафедры «Защита информации», Южно-Уральский государственный университет», г. Челябинск, проспект Ленина, 76. E-mail: sabelnikovsa@gmail.com

АСТАХОВА Людмила Викторовна, доктор педагогических наук, профессор кафедры «Защита информации», Южно-Уральский государственный университет», г. Челябинск, проспект Ленина, 76. E-mail: lvastachova@mail.ru

SABELNIKOV Sergey Aleksandrovich, instructor, department of informations security, South Ural State University, Chelyabinsk, Russia. E-mail: sabelnikovsa@gmail.com

АСТАХОВА Ludmila Viktorovna, Doctor of Sciences (Pedagogy), Professor, South Ural State University, Chelyabinsk, Russia. E-mail: lvastachova@mail.ru