

Таким образом, использование подобного шлюза может решить проблему взаимодействия информационных систем разного класса.

Данное решение проблемы взаимодействия информационных систем разного класса было применено в ГУП «Московский социальный регистр». Информационная система данной организации относится к классу К1, так как содержит больше ста тысяч записей персональных данных второй категории [1]. Организация всех информационных потоков с ИС других учреждений, таких как МГФОМС, МЖД и прочие, имеющих класс ниже К1, через шлюз, который в результате проведенных работ был отнесен к классу К3, позволила обеспечить защищенный обмен и полностью выполнить все требования руководящих документов.

## СПИСОК ЛИТЕРАТУРЫ:

1. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. № 55/86/20 г. Москва «Об утверждении Порядка проведения классификации информационных систем персональных данных».

*В. С. Горбатов, А. П. Дураковский, Ю. Н. Лаврухин, В. А. Петров*

## УЧЕБНО-МЕТОДИЧЕСКИЕ ТРЕБОВАНИЯ К ЛАБОРАТОРНОМУ ПРАКТИКУМУ В ОБРАЗОВАТЕЛЬНЫХ СТАНДАРТАХ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НОВОГО (ТРЕТЬЕГО) ПОКОЛЕНИЯ

В настоящее время высшая школа находится в состоянии ожидания перехода на многоуровневую подготовку выпускников в системе профессионального образования: среднее специальное образование — бакалавриат — специалитет — магистратура. Для нашего направления «Информационная безопасность» такой переход будет, несомненно, положительным фактором, так как на данный момент для него пока предусматривается сохранение всех указанных выше уровней. Таким образом, расширяется возможность более творческого подхода к организации подготовки широкого спектра выпускников с учетом современных требований науки, техники и промышленности. Однако эффективное решение указанной задачи во многом будет зависеть от качества интенсивно разрабатываемых в настоящее время образовательных стандартов нового (третьего) поколения.

В связи с этим были проанализированы проекты разрабатываемых федеральных государственных образовательных стандартов (ФГОС) высшего профессионального образования нового (третьего) поколения с одной, но, с нашей точки зрения, очень важной позиции: определения требований к уровню знаний, умений и практических компетенций специалистов (бакалавров, магистров) по защите информации в области аттестации объектов информатизации по требованиям безопасности информации. Именно эти требования должны лечь в основу учебно-методического обеспечения такого важного компонента организации учебного процесса, как лабораторные практикумы, а также послужить основой технико-экономического обоснования их дорогостоящей материальной базы.



Подобная работа была проделана ранее с ныне действующими ГОС по пяти специальностям: ГОС 09.01.02 – ГОС 09.01.06. Из сводной таблицы полученных аналитических данных следует, что ряд аналогичных дисциплин, входящих в различные специальности, могут быть поддержаны одними и теми же лабораторными практикумами, в которых требования к знаниям, умениям и практическим компетенциям выпускников, связанные с аттестацией ОИ по требованиям безопасности информации, затронуты лишь косвенно. Это дало возможность разработки типового перечня, структур и описаний (аннотаций) типовых лабораторных практикумов, предназначенных для профессиональной подготовки работников подразделений служб безопасности и технической защиты информации.

Последняя совокупность ФГОС третьего поколения по направлению «Информационная безопасность» представлена проектами по специальностям: 09.03.01 – КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ; 09.03.03 – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ; 09.03.05 – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ; 09.03.07 – ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ. Анализируя состав и объем общепрофессиональных дисциплин и дисциплин специализаций, сведенных в одну таблицу, по предъявляемым требованиям к знаниям и практическим умениям выпускников, можно сделать вывод о потенциальной готовности к проведению аттестации объектов информатизации по требованиям безопасности информации лишь выпускников по так называемой пятой специальности – «Информационная безопасность автоматизированных систем». При этом только в проекте ФГОС этой специальности предполагается включение в курсы профессионального цикла (в базовую и вариативную части) лабораторных практикумов, связанных с аттестацией объектов информатизации по требованиям безопасности информации.

Еще печальнее картина с данным вопросом в проекте ФГОС ВПО выпускников с квалификацией «бакалавр». Так как в подготовленных проектах стандартов отсутствует какая-либо ориентация на первичные должности выпускников, то основное внимание уделяется дисциплинам общеобразовательного характера, в том числе гуманитарного цикла, обеспечивающим фундаментальную подготовку. Задача получения практических навыков, особенно работы с применением сложных инструментальных средств, решается очень слабо, в недопустимо малом объеме учебной нагрузки.

Все это означает, что представленные на суд научно-педагогической общественности проекты ФГОС ВПО третьего поколения пока не закрепляют достоинств действующих стандартов, по крайней мере в части повышения уровня навыков практической работы.

*Ю. Г. Горшков*

## РЕШЕНИЕ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

За последние годы традиционный набор биометрической персональной информации отпечатков пальцев и ладоней, радужной оболочки глаз и голоса человека дополняется акустическими данными, получаемыми в процессе аускультации сердца.

