

■ Евгений БЕЛОВ,

заместитель председателя Совета учебно-методического объединения по образованию в области информационной безопасности

ПОПРИЩЕ СТРАЖА

В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – НОВОЕ, ТРЕТЬЕ ПОКОЛЕНИЕ ОТЕЧЕСТВЕННЫХ ОБРАЗОВАТЕЛЬНЫХ СТАНДАРТОВ

Современный этап развития общества характеризуется возрастающей ролью информационной сферы – совокупности самой информации и её инфраструктуры, различных субъектов, которые собирают, формируют, распространяют и используют информацию, а также системы регулирования сопутствующих общественных отношений. Неудивительно, что на рубеже тысячелетий появились новая профессия – специалист по защите информации и новые специальности по обеспечению информационной безопасности, которые весьма популярны у молодёжи.

ДОКТРИНА ТРЕБУЕТ

В Доктрине информационной безопасности, утвержденной Президентом Российской Федерации, говорится, что «национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать». Положения этой Доктрины были развиты в Стратегии развития информационного общества в Российской Федерации, утвержденной Президентом Российской Федерации от 7 февраля 2008 года № Пр-212.

В информационной безопасности, как во многих других областях, кадры решают всё. Как обстоит дело с их подготовкой, насколько она отвечает поставленным задачам? Система образования в области информационной безопасности, сформированная в последние 10–15 лет, включает в себя взаимодействующие компоненты:

- профильные министерства и ведомства;
- органы управления образованием и подведомственные им учреждения;
- учебно-методические объединения, советы и комиссии в области информационной безопасности;
- преемственные государственные образовательные стандарты;
- образовательные программы разного уровня и направленности;
- сеть образовательных учреждений, на основании лицензий обучающихся по этим программам;

- отраслевые научные, проектные, производственные организации и учреждения, ведущие научные исследования в соответствующей области образования.

Для совершенствования данной системы образования были разработаны научные подходы и принципы формирования нового перечня направлений и специальностей по информационной безопасности, а также соответствующих образовательных стандартов третьего поколения.

СТАНДАРТЫ ОБНОВЛЯЮТСЯ

Государство и общество предъявляют строгие требования к подготовке специалистов в области информационной безопасности. Высокая планка закладывается в федеральных государственных образовательных стандартах высшего и среднего профессионального образования (ФГОС ВПО и СПО).

За качеством подготовки, помимо Федеральной службы по надзору в сфере образования и науки, внимательно следят и другие профильные федеральные органы исполнительной власти, а также организации работодателей, непосредственно отвечающие за обеспечение информационной безопасности страны. Причина ясна: цена ошибки специалиста по защите информации государственного или коммерческого информационного ресурса слишком высока.

К настоящему времени завершена работа по созданию нового поколения ФГОС ВПО и СПО. Их главной особенностью является внедрение **компетентного и модульного подходов к обучению**. Предполагается не просто получение студентами некоторого набора теоретических знаний и практических навыков, а формирование определенных профессиональных компетенций, соответствующих

Появившаяся на рубеже тысячелетий новая профессия специалиста по обеспечению информационной безопасности завоевала колоссальную популярность у молодёжи

Перечень направлений подготовки (специальностей) ВПО и СПО

№	Наименование укрупненных направлений подготовки, направлений подготовки и специальностей	Код	Наименование квалификаций
090000	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ		
	<i>Высшее профессиональное образование</i>		
090900	Информационная безопасность – новое направление подготовки	62	Бакалавр
		68	Магистр
090101	Криптография	65	Специалист
090201	Противодействие техническим разведкам	65	Специалист
090301	Компьютерная безопасность	65	Специалист
090302	Информационная безопасность телекоммуникационных систем	65	Специалист
090303	Информационная безопасность автоматизированных систем	65	Специалист
090305	Информационно-аналитические системы безопасности – новая специальность	65	Специалист
	<i>Среднее профессиональное образование</i>		
090305	Информационная безопасность автоматизированных систем – новая специальность	51	Техник по защите информации (ЗИ)
		52	Старший техник по ЗИ
090303	Информационная безопасность телекоммуникационных систем – новая специальность	51	Техник по ЗИ
		52	Старший техник по ЗИ
090905	Организация и технология защиты информации – новая специальность	51	Техник по ЗИ
		52	Старший техник по ЗИ

ющих задачам и потребностям, которые ставят перед выпускниками потенциальные работодатели.

С внедрением новых стандартов система профессионального образования в области ИБ получает новый облик, отвечающий как политике реформирования образования в стране, так и вызовам развитию информационного общества в России.

Начиная с 2011 года она структурно будет включать в себя следующие образовательные программы (см. Таблицу).

В направлении подготовки «Информационная безопасность» следует предусмотреть выделение профилей, сопряженных с предлагаемыми образовательными программами специальностей СПО и ВПО.

Наиболее важными результатами совершенствования рассматриваемой системы образования являются:

- открытие подготовки бакалавров и магистров в рамках сформированного нового направления подготовки «Информационная безопасность» с выделением шести профилей, сопряженных с прежними и новыми образовательными программами специальностей СПО и ВПО;
- сохранение подготовки по моноспециальностям;
- обоснованное создание новой специальности «Информационно-аналитические системы безопасности»;
- вместо эксперимента с одной специальностью «Информационная безопасность» в СПО – введение трех новых специальностей (базовыми организациями являются Тульский колледж машиностроения и информационных технологий и Институт криптографии, связи и информатики).

КОЛЛЕКТИВНАЯ РАЗРАБОТКА

Давая общую характеристику образовательных стандартов, следует отметить, что в ходе их разработки сложнее всего было определить перечень профессиональных задач и сформулировать профессиональные компетенции. Рамки статьи не позволяют в полном объеме показать всю технологию разработки стандартов, но на некоторых моментах хотелось бы остановиться.

В качестве экспертов и разработчиков стандартов важно участие, наравне с вузовской общественностью, представителей заинтересованных федеральных органов исполнительной власти – ФСБ России, ФСТЭК России и Росфинмониторинга.

Следует привлекать и объединения работодателей, в первую очередь межрегиональное общественное объединение «Ассоциация защиты информации», в которую входят более 50 научных институтов, ведущих фирм, предприятий и организаций, работающих в сфере обеспечения информационной безопасности.

Далее, необходимо использования результатов НИР в области профессионального образования – научные работы, выполненные ИКСИ Академии ФСБ России, РГГУ,

Федеральные государственных стандартах высшего и среднего профессионального образования предъявляют в области информационной безопасности самые строгие требования к подготовке специалистов

Главной особенностью нового, третьего поколения образовательных стандартов является компетентностный и кредитно-модульный подходы к обучению

МИФИ, МГТУ им. Н.Э. Баумана по заказу Минобрнауки России, ФСТЭК России и Академии криптографии РФ.

Для понимания, кто такой бакалавр информационной безопасности, целесообразно ознакомиться с его общими профессиональными компетенциями, которые включают следующие способности:

- использовать знания основных естественнонаучных законов, применять математический аппарат и выявлять сущность проблем, возникающих в ходе профессиональной деятельности;
- понимать сущность информации и её значение в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации, проводить целенаправленный поиск в различных источниках информации по своему профилю, в том числе в глобальных компьютерных системах;
- по результатам анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия определять виды и формы информации, подверженной угрозам, типы, возможные методы и пути реализации угроз;
- формировать эффективный комплекс мер информационной безопасности с учетом правовой обоснованности, административно-управленческой и технической реализуемости, а также оценки экономической целесообразности;
- организовывать и поддерживать выполнение комплекса мер информационной безопасности, управлять процессом их реализации, учитывая решаемые задачи и организационную структуру предприятия, внешние воздействия, вероятные угрозы и уровень развития технологий защиты информации;
- организовывать и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов.

ПРОФИ МОНИТОРИНГА

Реализация направления (бакалавриат) «Информационная безопасность» предполагает получение студентом достаточной фундаментальной базы. Это даст возможность после первых лет обучения по выбранному направлению более осознанно определить профиль программы на старших курсах бакалавриата. Получив диплом о высшем профессиональном образовании, в случае изменений на рынке труда можно корректировать выбор дальнейшего пути — например, продолжить обучение, в магистратуре или в

системе дополнительного профессионального образования.

УМО по образованию в области информационной безопасности совместно с УМО по образованию в области историко-архивоведения разработало и согласовало с работодателями и заинтересованными федеральными органами исполнительной власти следующий перечень профилей:

1. Безопасность компьютерных систем;
2. Организация и технология защиты информации;
3. Комплексная защита объектов информатизации;
4. Безопасность автоматизированных систем;
5. Безопасность телекоммуникационных систем;
6. Информационно-аналитические системы финансового мониторинга.

С учетом проблематики журнала предлагаем потенциальным работодателям обратить внимание на профильно-специализированные компетенции выпускника-бакалавра по новому профилю «**Информационно – аналитические системы финансового мониторинга**», который способен:

- решать задачи первичного финансового мониторинга в рамках функционирования служб внутреннего контроля субъектов финансового мониторинга (ПСК6-1);
- учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах финансовых и экономических структур, для информационно-аналитического обеспечения финансового мониторинга (ПСК6 – 2);
- участвовать в разработке информационно-аналитических систем финансового мониторинга (ПСК6-3);
- реализовывать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур (ПСК6-4).

Основной вклад в разработку данного профиля внесли представители ИКСИ, МИФИ и Росфинмониторинга.

АНАЛИТИКА БЕЗОПАСНОСТИ

Академией ФСБ России совместно с Национальным исследовательским ядерным университетом «МИФИ», представителями Росфинмониторинга и членами УМО ИБ разработан ФГОС ВПО по новой специальности «**Информационно-аналитические системы безопасности**». Актуальность открытия этой специальности обусловлена потребностью в квалифицированных кадрах для нового направления деятельности федеральных органов исполнительной власти. Конкретно — ведения аналитического и финансового мониторинга социально-экономических процессов

Получив диплом о высшем профессиональном образовании, в случае изменений на рынке труда можно продолжить обучение в магистратуре или в системе дополнительного профессионального образования

Разработанная МИФИ специализация «Информационная безопасность автоматизированных банковских систем» предполагает самый широкий перечень профильно-специализированных компетенций выпускников

в целях обеспечения экономической безопасности государства и противодействия легализации денежных средств, полученных незаконным путем.

Заказчиками-работодателями специалистов по ИАСБ являются федеральные органы исполнительной власти (Росфинмониторинг, Минфин России, Минэкономразвития России и др.), правоохранительные органы, Банк России, другие финансовые и экономические организации.

Профессиональный цикл специальности ИАСБ включает:

- уникальный по своему составу **модуль информационных технологий**, формирующий, помимо собственно информационных технологий, ещё и компетенции в информационно-аналитической и проектной деятельности (нет аналогов данного модуля в других специальностях по информационной безопасности, а также и в специальностях других УМО);
- **модуль информационной безопасности**, который по своей идеологии соответствует другим специальностям по информационной безопасности;
- **экономический модуль**, формирующий компетенции в социально-экономической сфере, которая является предметной областью информационно-аналитической работы, финансового мониторинга;
- **юридический модуль**, формирующий правовые компетенции государственного служащего гражданского, административного, уголовного и финансового права, касающиеся профильных процессов.

Модули информационных технологий, юридический и экономический выделяют специальность «Информационно-аналитические системы безопасности» среди других специальностей по направлению информационная безопасность.

ФГОС ВПО по специальности ИАСБ предусматривает три специализации:

1. «Автоматизация информационно-аналитической деятельности»;
2. «Информационная безопасность финансовых и экономических структур»;
3. «Технологии информационно-аналитического мониторинга»

IT-СТРАЖИ БАНКОВ

Особого внимания и заслуживает разработанная МИФИ специализация «Информационная безопасность автоматизированных банковских систем».

Выпускники в рамках своих профильно-специализированных компетенций должны в отношении автоматизированных банковских систем владеть следующими способностями:

- проводить анализ и исследовать модели автоматизированных банковских систем;
- применять на практике стандарты, относящиеся к обеспечению информационной безопасности;
- на практике применять криптографические протоколы и стандарты при обеспечении информационной безопасности
- проводить синтез и анализ проектных решений по обеспечению информационной безопасности;

Самые сильные мотивы выбора профессии IT-стража для абитуриентов средних специальных и высших учебных заведений – стремление принадлежать к интеллектуальной элите Родины и находиться на передовых рубежах научно-технического прогресса

- обеспечить эффективное применение информационно-технологических ресурсов с учетом нормативных требований по защите информации;
- разрабатывать и реализовывать политики информационной безопасности;
- участвовать в проектировании и эксплуатации системы управления информационной безопасностью;
- проводить инструментальный мониторинг защищенности;
- разрабатывать предложения по совершенствованию системы управления информационной безопасностью;
- формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы.

* * *

Что побуждает абитуриентов средних специальных и высших учебных заведений выбирать непростой жребий «информационных стражей»? Самые сильные мотивы – стремление принадлежать к интеллектуальной элите Родины и находиться на передовых рубежах научно-технического прогресса. Ну и, конечно, перспективы быстрого служебного роста и, вполне естественно, высокооплачиваемой работы. Образовательные новации раскрывают всё более широкое поприще служения делу защиты информационного пространства России.