**НОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ В ПОДГОТОВКЕ ПРОФЕССИОНАЛОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БАЗЕ ГБОУ ВПО МО «ФИНАНСОВО ТЕХНОЛОГИЧЕСКАЯ АКАДЕМИЯ»**

**NEW EDUCATIONAL TECHNOLOGIES IN TRAINING PROFESSIONALS OF INFORMATION SECURITY BASED ON NBEI HPE Moscow Region “Financial and Technological Academy”**

**Соляной В.Н., Сухотерин А.И., Успенский Ф. А.**

Финансово-технологическая академия, г. Королев, Россия

**Solyanoy V.N., Sukhoterin A.I., Uspensky F.A.**

Financial and Technological Academy, Korolev city, Russia

Проблема формирования подготовленного кадрового ресурса для новых сфер профессиональной деятельности в современной России становится чрезвычайно актуальной в связи с возникновением отраслей, не имеющих ранее аналогов. Если для традиционных сфер профессиональной деятельности (машиностроение, энергетика, металлургия и т.д.) становление новой отраслевой системы образования происходит в рамках уже существующей, то для новых сфер профессиональной деятельности (например, безопасности бизнеса) необходимо создавать систему подготовки кадров практически с нуля. В связи с интенсивным внедрением системы информационной безопасности в практику работы предприятия (организации) возникает потребность (дефицит) специалистов «специалист (бакалавр) в области безопасности бизнеса», то возникает задача подготовки таких специалистов (бакалавров) для региона на базе ФТА.

The problem of formation of trained human resource for new areas of professional activity in modern Russia becomes extremely relevant in connection with the emergence of industries that do not have analogues previously. If the traditional specialty areas (engineering , power engineering, metallurgy , etc. ) becoming the new industrial system of education takes place in the framework of an existing one, then for new areas of professional activity (eg business security ) must establish a system of training from scratch. Due to the intensive implementation of information security system into the practice of enterprise (organization) there is a need (deficit) specialists “specialist (bachelor) in business security ", then there is a problem that professionals( bachelors) for the region based on the FTA.

**Ключевые слова:** информационная безопасность, информационно-аналитические системы безопасности, новые образовательные технологии.

**Keywords:** information security, information and analytical systems security, new educational technologies.

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 молодежи [1,2].

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 в соответствующих областях образования [7]:

* 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 обучающих по этим программам;
* отраслевые научные, проектные, производственные организации и учреждения, ведущие научные исследования.

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 [1,2,3,4,5,6,7].

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) [1,2,3,4,5,6,7,8].

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 [7],.

Главной особенностью ФГОС ВПО и СПО является внедрение компетентностного и модульного подходов к обучению. Предполагается не просто получение студентами некоторого набора теоретических знаний и практических навыков, а формирование определенных профессиональных компетенций, соответствующих задачам и потребностям, которые ставят перед выпускниками потенциальные работодатели [1,2,7,10].

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 [1,2,3,4,5,6].

Для понимания, кто такой бакалавр информационной безопасности, целесообразно ознакомиться с его общими профессиональными компетенциями, которые включают следующие способности [4,5,6,7,8]:

* использовать знания основных естественно - научных 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.

Проблема формирования подготовленного кадрового ресурса для новых сфер профессиональной деятельности в современной России становится чрезвычайно актуальной в связи с возникновением отраслей, не имеющих ранее аналогов. Если для традиционных сфер профессиональной деятельности (машиностроение, энергетика, металлургия и т.д.) становление новой отраслевой системы образования происходит в рамках уже существующей, то для новых сфер профессиональной деятельности (например, безопасности бизнеса) необходимо создавать систему подготовки кадров практически с нуля. В связи с интенсивным внедрением системы информационной безопасности в практику работы предприятия (организации) возникает потребность (дефицит) специалистов в этой области. Анализ «Квалификационного Справочника по труду» показывает, что в нем отсутствует направление подготовки в области «специалист (бакалавр) в области безопасности бизнеса», то возникает задача подготовки таких специалистов (бакалавров) для региона [1,2,3,4,5,6,7,8,12,13].

Подготовка таких специалистов позволит решать задачи, ранее не включаемые в учебный процесс, а именно, информационное противоборство в бизнес–среде, информационно-аналитическая поддержка безопасности бизнеса, противодействие «черному PR» [6,7,8,12,13].

Для подготовки специалистов в области информационного противоборства в бизнес - среде, в ФТА на кафедре «Информационной безопасности» с 2012 г. ведется разработка ООП ВПО для подготовки, владеющих основами экономики, бизнеса, информационного права, прикладной информатики, информационной безопасности и деловой разведки. Под деловой разведкой понимается легальное добывание и анализ информации из информационного поля бизнес - среды для принятия оптимальных управленческих решений [1,2,3,6,7,8,9,12,13].

При подготовке к внедрению на кафедре ИБ ФТА уделяется внимание разработке и апробации новых учебных программ дисциплин и использованию новых обучающих технологий, максимально приближенных к практике реального бизнеса.

Как считает один из ведущих мировых экспертов в области деловой разведки Иан Херинг, «..процесс анализа представляет собой этап в создании знаний (intelligence), при котором разрозненная «сырая» информация перерабатывается в сведения, позволяющие принимать оптимальные управленческие решения». Американским обществом профессионалов конкурентной разведки (Society competitive intelligence professionals – SCIP) разработан перечень требований, предъявляемых к аналитику (SBA) [12,13]. Разработка перечня базировалась на требованиях разведывательного цикла.

**Аналитик ИБ должен уметь выполнять** [6,7]:

На первом этапе постановке задачи и планировании операции: совместно с Заказчиком уметь грамотно формулировать задачу; уметь проектировать решение задачи; уметь определять временные, информационные и финансовые ресурсы, необходимые для решения задач; хорошо ориентироваться во внешних и внутренних информационных ресурсах.

На втором этапе сборе информации: знать способы и методы доступа к первичным и вторичным информационным источникам; владеть активными и пассивными методами сбора информации; уметь оценивать качественные характеристики полученной информации (по достоверности, полноте, актуальности и т.д.); знать и соблюдать правовые и этические нормы; знать и уметь работать с новыми информационными технологиями.

На третьем этапе анализе информации: знать основные методы анализа информации; уметь применять методы анализа конкурентной среды (метод ПЭСТ, модели М. Портера, методы «сети связи» и др.), анализа конкурента (метод SWOT, Метод БКГ и др.), методы ситуационного анализа, различные экспертные методы; знать и уметь применять современные информационно-аналитические системы деловой разведки (Интегрум, «Семантический архив»и т.д.).

На четвертом этапе представлении результатов: уметь использовать средства презентации результатов; знать особенности восприятия Заказчиком выводной информации; уметь готовить аналитические документы.

Этот перечень умений и навыков должен быть взят за основу исходя из реалий сегодняшнего дня в рамках подготовки студентов по кафедре информационной безопасности (Приложение 1).

В качестве инструментария предлагается использовать: информационные ресурсы сети Интернет, российские базы данных системы Интегрум, крупнейшая в мире он-лайновая система БД Lexis-Nexis, другие информационные технологии.

 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 в целях обеспечения экономической безопасности государства и противодействия легализации денежных средств, полученных незаконным путем. Срок обучения по этой специальности составляет 5.5 лет [6].

*Основное содержание учебного плана подготовки специалиста по ЗИ (аналитик ИБ)*

* **модуль информационных технологий** уникальный по своему составу, 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.

В тоже время при реализации 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.

При этом ООП должен учитывать и профильно-специализированные компетенции выпускника-бакалавра по новому профилю **«Информационно-аналитические системы финансового мониторинга**», который способен реализовывать следующие компетенции [6,12,13]:

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

Одним из основных мотивов соискателей (абитуриентов) побуждающих выбирать жребий «информационных стражей» – стремление принадлежать к интеллектуальной элите Родины и находиться на передовых рубежах научно-технического прогресса. Немаловажный фактор это перспективы быстрого служебного роста и, вполне естественно, высокооплачиваемой работы. Образовательные новации раскрывают всё более широкое поприще служения делу защиты информационного пространства России.

Кроме того просматривается необходимость подготовки наших выпускников для службы в Российской армии в связи с созданием отдельного рода войск «Киберкомандования» в 2014 году. Главным заданием которого станет ведение операций в виртуальном пространстве, как в мирное так и в военное время, а это и есть обеспечение информационной безопасности страны, связанной с мониторингом и обработкой информации, поступающей извне, а также борьба с киберугрозами [14].

Таким образом, указанные положения по подготовке профессионалов информационной безопасности должны базироваться на вышеизложенных образовательных технологиях.

**Список использованных источников:**

1. Федеральные законы Российской Федерации: «Об образовании» (от 29 декабря 2012 г. №273) и «О высшем и послевузовском профессиональном образовании» (от 22 августа 1996 г. №125-ФЗ);
2. Распоряжение Правительства РФ от 03.11.2011 № 1944-р
«О перечне направлений подготовки (специальностей) в образовательных учреждениях высшего профессионального образования, специальностей научных работников, соответствующих приоритетным направлениям модернизации и технологического развития российской экономики» Официальная публикация в СМИ: "Российская газета", № 254, 11.11.2011 "Собрание законодательства РФ", 14.11.2011, № 46, ст. 6584
3. Типовое положение об образовательном учреждении высшего профессионального образования (высшем учебном заведении), утвержденное постановлением Правительства Российской Федерации от 14 февраля 2008 г. №71;
4. ФГОС ВПО по направлению подготовки 090900 Информационная безопасность (квалификация (степень) "бакалавр") Приказ Минобрнауки РФ от 28 октября 2009 г. N 496.
5. ФГОС ВПО по направлению подготовки 090900 Информационная безопасность (квалификация (степень) "магистр") Приказ Минобрнауки РФ от 28 октября 2009 г. N 497.
6. ФГОС ВПО 090305 по направлению подготовки (специальности) 090305 Информационно-аналитические системы безопасности (квалификация (степень) "специалист")" Приказ Минобрнауки РФ от 17.01.2011 N 56.
7. Материалы пленума учебно-методического объединения вузов Российской Федерации по образованию в области историко -архивоведения. РГГУ «Институт информационных наук и технологий безопасности». Сборник аннотаций программ учебных дисциплин ОООВПО по направлению подготовки 090900 «Информационная безопасность» квалификация: бакалавр. Профили: «организация и технология защиты информации», «Комплексная защита объектов информации». – М. 2012г.
8. ООП ВПО 090900.62 Информационная безопасность, квалификация (степень) выпускника «Бакалавр», форма обучения – очная, нормативный срок освоения программы - 4 года. Утверждена УМС ФТА: Протокол №01 от «24» сентября 2013 г.
9. Методические материалы по обучающему комплексу по направлению подготовки 090900 информационная безопасность квалификация (степень) бакалавр и магистр: Санкт- Петербург 2013 г.
10. Соляной В.Н., Сухотерин А.И.. Обоснование открытия на ОАО ТРВ базовой кафедры по обеспечению комплексной безопасности предприятий. г. Королев. Сборник научных трудов, Информационно-технологического факультета. ФТА. 2012г.
11. Соляной В.Н., Сухотерин А.И.. Взаимодействие человека, техники и природы: проблема информационной безопасности. Научный журнал (КИУЭС) Вопросы региональной экономики. УДК 007.51 №5 (05) г. Королев. ФТА. 2010г.
12. Сайт Американского общества профессионалов конкурентной разведки. – http:/www.scip.org.
13. Баяндин Н.И. Технологии безопасности бизнеса. – М.: Юристъ, 2002.
14. Информационно – методический журнал: «Защита информации» INSIDE №5 сентябрь-октябрь 2013г. 95 с.
15. Агафонов А.В. Семинар «Создание моделей образования и формирование образовательных стандартов для Национальной системы противодействия легализации доходов, полученных преступным путём, и финансированию терроризма». Москва, МИФИ, 2 июня 2009 года.

Приложение 1

**090305.65 Информационно-аналитические системы безопасности**

1. **Код и наименование направления подготовки, наименование программы:** специальность 090305 «Информационно-аналитические системы безопасности». Специализация «Информационная безопасность финансовых и экономических структур»
2. **Предлагаемая образовательная траектория:** специалитет.
3. **Краткая характеристика программы:** цель: подготовка специалистов в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, дневная форма подготовки, 5,5 лет, базовая кафедра – 75.
4. **Характеристика сферы и объектов профессиональной деятельности будущих выпускников**.

Область профессиональной деятельности:сферы науки, техники и технологии, охватывающие сследования и разработки, направленные на создание, эксплуатацию, развитие и защиту автоматизированных информационно-аналитических систем, обеспечивающих обработку и анализ специальной информации (в дальнейшем - специальных АИС), а также функционирующих в составе этих систем прикладных средств современных информационных технологий.

Профессиональная деятельность выпускников связана с решением задач по созданию и обеспечению работы узловых элементов национальной системы по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма на всех уровнях (международном, государственном, первичном).

Выпускники будут выполнять работу в рамках следующих видов профессиональной деятельности: информационно-аналитическая, научно-исследовательская, проектная, эксплуатационно-технологическая, организационно-управленческая, правоохранительная. Основные потребители выпускаемых специалистов: федеральные органы государственной власти и их территориальные подразделения – участники национальной системы по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;  органы государственного контроля и надзора в кредитно-финансовой сфере и в смежных областях; подразделения внутреннего контроля кредитных и не кредитных организаций – субъектов финансового мониторинга.

1. **Программы, для которых планируется подготовка кадров.** Подготовка кадров развернута в соответствии с требованиями Концепции национальной стратегии противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (утверждена Президентом Российской Федерации).
2. **Краткая характеристика учебного плана, особенности образовательного процесса по программе, основные базовые и специальные дисциплины.** Учебный план реализуется в соответствии с требованиями ФГОС ВПО по специальности 090305. Кроме обязательных дисциплин ФГОС он включает в себя следующие дисциплины специализации: Международная система по противодействию легализации преступных доходов и финансированию терроризма, противодействие финансированию терроризма и экстремизма; Формы и методы подготовки аналитической информации; Информационные ресурсы в первичном (государственном) финансовом мониторинге; Информационное взаимодействие и ресурсы в государственном финансовом мониторинге; Основы контрольно-надзорной деятельности; Международная гражданская служба; Государственная гражданская служба в РФ; Системы внутреннего контроля в субъектах финансового мониторинга; Финансовые расследования в международном (государственном) финансовом мониторинге; Типологический анализ в первичном (государственном, международном) финансовом мониторинге; Национальная система по противодействию легализации преступных доходов и финансированию терроризма.

Привлекательные стороны программы - в процессе обучения студенты освоят дисциплины, впервые поставленные в НИЯУ МИФИ или ориентированные на неудовлетворенный спрос работодателей.

1. **Практики**.

1)Практикум на ЭВМ: проводится в недели теоретического обучения.

2)Производственная практика: проводится в течение 13-ти недель (с 10 августа по 16 ноября для студентов 10-ого и 11-ого семестров.

3)Преддипломная практика: не предусмотрена ФГОС.

4)Перечень предприятий для прохождения практики: Федеральная служба по финансовому мониторингу и ее территориальные подразделения в регионах РФ, кредитные и некредитные (страховые, лизинговые, риэлторские, факторинговые, ювелирные, игорные и пр.) организации - субъекты национальной системы по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.