УДК 004.056

**Особенности практико-ориентированной**

**(квазипрофессиональной) подготовки специалистов по информационной безопасности: деловая игра – имитационный метод организации образовательного процесса**

**Features of practice-oriented (quasi-professional) training on information security in the form of business game - organization of educational process by simulation method**

**Соляной В.Н., Сухотерин А.И., Антоненко В.И.**

Финансово-технологическая академия, г. Королев, Россия

**Solyanoy V.N., Sukhoterin A.I.. Antonenko V.I.**

Financial and Technological Academy, Korolev city, Russia

В статье поднимается проблема внедрения в учебный процесс подготовки, обучаемых по кафедре информационной безопасности ФТА по направлению подготовки 090900 «Информационная безопасность» квалификация (степень) бакалавр, магистр путем реализации компетентностного подхода [1,5,7]. Новая система требований к освоению образовательных программ (результатам освоения) обуславливают усовершенствование содержания, разработку новых методик и технологий образовательной деятельности и объективных форм контроля, за ее осуществлением [1,2,7,8].

The article raises the problem of implementation of the learning process of preparation, students in the department of information security training towards FTA 090900 "Information Security" qualification (degree) Bachelor, Master through the implementation of competence-based approach [1,5,7]. The new system requirements for the development of educational programs (development results) influence the improvement of content, the development of new methods and technologies of educational activities and objective forms of control over its implementation [1,2,7,8].

**Ключевые слова:**информационная безопасность, компетентностный подход для внедрения инновационных образовательных технологий.

**Keywords:** information security, competence-based approach for the introduction of innovative educational technologies.

Гораздо шире, чем в традиционных, в формировании компетенций (или компонентов компетенций), играют роль технологии и методы квазипрофессиональной деятельности. В ее формах будет осуществляться отработка и освоение отдельных компонентов формируемых компетенций с их последующей интеграцией в учебный процесс, имитирующий профессиональную деятельность. Это будет проходить за счет применения инновационных методов обучения, как проблемное обучение, проектная деятельность, групповые осуждения, обучение с использованием компьютерных обучающих программ, деловые и ролевые игры, тренинги, мозговой штурм, видеоанализ и т.д.

В статье речь пойдет о деловой игре, как одного из основных методов практико-ориентированной подготовки студентов кафедры Информационной безопасности.

Деловая игра (Рис.1.) - это метод, предполагающий создание нескольких команд, которые соревнуются друг с другом в решении той или иной задачи. Деловая игра требует не только знаний и навыков, но и умения работать в команде, находить выход из неординарных ситуаций и т.д [1,2,5,7,8,9].

Цель деловой игры - проявить имеющиеся знания, показать умение самостоятельно (автономно) или в кооперации (в команде) пользоваться ими, получить навыки уяснения комплексных проблем выработки подходов к их решению. Деловая игра должна содержать игровую и учебные задачи. Игровая задача - выполнение играющим определенной профессиональной деятельности. Учебная задача - овладение знаниями и умениями [1,2,5,7,8,9].



**Рис.1. Квазипрофессиональная деятельность**

Деловая игра предполагает наличие определенного сценария, правил работы и вводной информации, определяющей содержание игры. Продолжительность деловой игры зависит от трудоемкости и размера задачи. Есть немало задач, которые "помещаются" в два-четыре аудиторных часа. Кроме этого, почти все деловые задачи сравнительно легко поддаются расчленению.

Подготовка деловой игры требует от преподавателя внимания и собранности. Если он сам составляет игровую задачу, он должен продумать её учебные цели. Если он берет для игры готовую задачу, он обязан в нее вникнуть со стороны игрока, и со стороны ведущего. Основными проблемами, с которыми приходится сталкиваться при проведении деловой игры, являются создание творческой, состязательной атмосферы, вовлечение участников в игру и поддержание высокого уровня эмоциональной напряженности в течение всей игры [1,2,5,7,8,9].

Игра должна быть описана - это обязательное условие. Нельзя задавать условие и цели игры "с голоса". Количество экземпляров описания игры должно быть достаточно для всех.

Крайне важно исходить из того, что все знают правила игры, но кое-что в них забыли или неточно помнят. Поэтому необходимо раздать участникам деловой игры материал с выдержками из документов, регламентирующих наиболее "скользкие" вопросы (узлы) решения деловой задачи. Например, фрагменты из источников, Конституции, законов, инструкций, постановлений, указов и т.п.

Деловая игра требует соблюдения некоторых последовательных шагов [1,2,5,7,8,9]:

*Первое - доведение задачи до участников*. Распечатанный текст задачи должен быть у каждого участника (что касается условий игры, то заранее следует договориться: принимаются ли они те же, что и в реальной жизни при решении сходных задач, или же вносятся какие-либо игровые изменения).

*Второе - создание команд.* Команды формируются любым образом, при этом они вправе присвоить себе какие-нибудь названия или номера.

*Третье - это непосредственная работа команд.*

Затем каждая команда готовит короткий (до 10 минут) устный доклад о своих подходах и методах решения задачи и о самом решении. Доклад составляется в произвольной форме. Выбор формы доклада - тоже игровой результат.

После заслушивания докладов необходимо оценить их, сравнить и подвести итоги. Это важная часть учебного процесса.

Если времени мало, то итоги подводит преподаватель. И здесь важно не сводить дело к "пьедесталу почета", определению победителя и призеров, а лучше отметить успехи каждой из команд. Если время позволяет, то подведение итогов и разбор результатов могут стать вторым туром обучения в рамках деловой игры. Тогда формируется жюри из представителей каждой команды во главе с ведущим - председателем жюри. Жюри начинает "принародно" обсуждать итоги игры. В ходе такого обсуждения приоритет подчеркивания успехов или недостатков определяется в зависимости от ценности потенциала участников. Но преподавателю стоит, ни чуть не ломая избранного жюри критерия "справедливой оценки", стремиться подчеркнуть успехи каждой из групп.

Неплохо было бы выдать и специальные призы за успехи (например, книги с дарственными надписями преподавателями кафедры).

В зависимости от содержания задачи при проведении деловой игры могут потребоваться калькуляторы, учебная доска или ватман для изображения схем и формул, справочники, тексты законов и нормативных актов, а также необходимо иметь не менее двух аудиторий для работы групп.

Деловую игру желательно вести силами двух преподавателей. Некоторые моменты игры могут заставить одновременно выполнять разные функции, например, придумывать следующий игровой поворот и удерживать группу "в игровом тонусе". Но и без таких ситуаций двух преподавателям хватает работы, особенно при наблюдении за работой групп.

Деловая игра идеально подходит для группового зачета по части учебной дисциплины, а также по учебной дисциплине в целом.

Указанные подходы получили свою реализацию после внедрения в образовательный процесс КОК (компьютерного обучающего комплекса) на кафедре информационной безопасности в ноябре 2014г [9,10,11,12,13,14].

КОК позволит осуществить реализацию инновационного подхода в учебном процессе с использованием современных интерактивных компьютерных образовательных технологий в области подготовки профессионалов (бакалавров и магистров) по ИБ в соответствии с требованиями новых государственных образовательных стандартов РФ (стандартов третьего поколения).

В качестве ключевых принципов построения такой инновационной научно-образовательной технологии реализованы следующие установки [9,10,11,12,13,14]:

1. Реализацию комплексного подхода. Данный подход позволяет в едином образовательном процессе поэтапно и последовательно приобрести все структурные компоненты требуемых компетенций у обучаемых: знания, умения и навыки;
2. Возможность, наряду с традиционными обучаемыми технологиями (усвоение теоретического материала – приобретение знаний и освоение практики – умений и навыков), реализовать освоение исследовательских процессов.

 Первое положение наиболее характерно для подготовки, прежде всего, бакалавров. Второе положение в полной мере относится к подготовке магистров. Данная установка особенно важна при подготовке профессионалов в области информационной безопасности (специалистов, бакалавров и магистров). Это положение объясняется тем, что все решаемые задачи в области обеспечения информационной безопасности не могут иметь заранее готовых решений и относятся к трудно формализуемым творческим задам на основе проведения серьёзных исследовательских процессов в различных условиях информационной обстановке.

1. Обоснование и принятие решений в области обеспечения информационной безопасности профессионалы должны осуществлять на основе коллегиальных (групповых) подходах. При этом должны учитываться как интересы внутренних компонентов информационной безопасности (компьютерной, инженерно-технической, физической, организационной, правовой, информационно-психологической и т.д.), так и особенности внешних факторов обеспечения безопасности в целом (экономической, финансовой и т.д.).
2. Особенность протекающих реальных процессов в области обеспечения информационной безопасности требует обязательного включения обучения профессионалов (бакалавров, специалистов и магистров) инновационных образовательных подходов. Это прежде всего интерактивных «деловых» двухсторонних игр, с наличием как нападающей, так и обороняющей сторон. Именно данный подход позволит обучаемым наиболее полно понять все специфические процессы связанные с обеспечением информационной безопасности в реальном масштабе времени. Реализация этого положения особенно важна для подготовки профессионалов – организаторов и технологов по обеспечению информационной безопасности различных организационно-структурных объектов, т.е. менеджеров по информационной безопасности.

 На КОК ИБ возлагаютя следующие целевые (ключевые) интерактивные образовательные задачи [9,10,11,12,13,14]:

- проведение исследований возможных сценариев обеспечения информационной безопасности для информационных объектов различного масштаба (оценка информационной обстановки, выявление информационных угроз, нарушителей\злоумышленников и уязвимостей, определение ожидаемых ущербов и т.д.);

- обоснование возможных вариантов построения целесообразных систем обеспечения информационной безопасности, применительно к исследуемым сценариям и др.

Реализация указанных современных научно-образовательных технологий должна базироваться на следующей логической последовательности проведения основных этапов обучения.

Следует указать о наличии специфических особенностях реализации этих этапов применительно к разным категориям обучаемым (бакалавр и магистр). Это касается как содержания, так и объема изучаемому материалу, включая и количество реализуемых этапов.

Едиными этапами обучения бакалавров и магистров с использованием рассматриваемого научно-образовательного комплекса следует рассматривать последовательность от этапа 1 до этапа 4 [9,10,11,12,13,14].

Этап 1. Изучение теоретического материала по предметной области в виде мультимедийных курсов-лекций, структурированных по отдельным разделам учебной дисциплины.

Этап 2. Тестирование степени освоенности теоретического учебного материала обучаемыми. Цель проверки определение потребного уровня знаний, путем анализа ответов на контрольные вопросы и, как итоговый результат, получения допуска к следующему этапу обучения.

Этап 3. Моделирование отельных процессов (событий и явлений). Этап предусматривает выполнение интерактивных лабораторных работ. Данные работы организованны по принципу постепенного усложнения простых заданий в моделирующие сложные ситуации.

Этап 4. Анализ достигнутого уровня теоретических знаний у обучаемых (по результатам тестирования по второму этапу) и первичных навыков, получаемых в процессе выполнения лабораторных работ. При этом осуществляется формирование итоговых отчетов по каждому студенту. Итоговые отчеты представляются преподавателю. Преподаватель определяет уровень освоения требуемого учебного материала (знаний и первичных навыков).

Применительно к процессу подготовки магистров полученный положительный итоговый отчет является основанием для допуска обучаемых к следующему образовательному этапу.

Специфическим этапом подготовки магистра (этап 5), который обязательно должен реализовывать научно-образовательного комплекса, следует рассматривать следующий учебный процесс.

Этап 5. Проведение исследований на учебном виртуальном полигоне в форме двухсторонней «деловой игры».

На данном этапе из состава обучаемых формируются группы нападающей и обороняющейся сторон. Нападающая сторона (одна часть обучаемых) выступает в роли «злоумышленников». Они ищут уязвимости в существующей системе информационной безопасности. «Злоумышленники», найдя уязвимые места в защищаемой информационной системе, реализуют информационные угрозы [9].

Другая группа обучаемых (обороняющаяся сторона) анализирует и формирует целесообразные меры по обеспечению информационной безопасности. Пятый этап следует рассматривать как ключевой цикл в подготовки магистров - исследователей и менеджеров-организаторов в области информационной безопасности.

Общий технический облик рассматриваемого научно-образовательного комплекса представляет собой аппаратно-программный комплекс в виде самостоятельного интерактивного компьютерного учебного комплекса по информационной безопасности в виде защищенной локальной вычислительной сети [9].

В состав такого специализированного компьютерного комплекса входят следующие функциональные объекты: автоматизированные рабочие места преподавателя и студентов, а также, специализированный многофункциональный сервер.

В целом облик научно-образовательного комплекса должен обеспечивает информационную и методическую поддержку как обучаемых, так и преподавателей при организации образовательного процесса подготовки профессионалов по информационной безопасности в различных условиях [9].

Выработка профессиональных компетенций реализуется на основе изучении как отдельных базовых учебных дисциплин в целом, так и на изучении ключевых тем (разделов) отдельных учебных курсов.

Учебно-методическое обеспечение КОК ИБ состоит из следующих документов [9]:

Методические рекомендации преподавателю по организации и проведению занятий со студентами (бакалавры) с использованием КОК ИБ;

Методические рекомендации преподавателю по организации и проведению занятий со студентами (магистры) с использованием КОК ИБ;

Методические рекомендации студентам (бакалавриата) по организации и проведению занятий со студентами с использованием КОК ИБ;

Методические рекомендации студентам (магистратуры) по организации и проведению занятий со студентами с использованием КОК ИБ;

Методическое пособие СОТСБИ ОС LINUX основные аспекты работы в консоли. Сетевые средства. Управление сетевыми соединениями;

Методическое пособие аппаратно-программный комплекс СОТСБИ:

* Общее описание;
* Инструкция по эксплуатации;
* Система документирования.

В комплексе имеются [9]:

* методические материалы и рекомендации (инструкции) для преподавателей для проведения теоретических, практических, лабораторных занятий, тестирования и проведения «деловых» игр, включая инструкции, наборы заданий и варианты правильных решений;
* методические материалы и рекомендации (инструкции) для обучаемых при проведении теоретических, практических, лабораторных занятий, тестировании и проведении «деловых» игр, включая инструкции, наборы заданий и формы отчетных документов;
* электронную библиотеку, содержащую потребную учебную литературу для проведения занятий и др. документы.

 Таким образом, внедрение и освоение преподавателями кафедры КОК ИБ позволит поднять уровень подготовки студентов кафедры новый уровень, прежде всего на выработку требуемых профессиональных компетенций, предъявляемых для профессионалов в области информационной безопасности.

**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 №11 от «30» июля 2014 г.
9. Методические материалы по обучающему комплексу по направлению подготовки 090900 информационная безопасность квалификация (степень) бакалавр и магистр: Санкт- Петербург 2014 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. Соляной В.Н., Сухотерин А.И., Федоров М.А. Выбор и внедрение новых образовательных технологий в (учебный процесс) подготовку бакалавров (специалистов) и магистров по информационной безопасности. «Современные образовательные технологии, используемые в очном, заочном и дополнительном образовании» [Текст] сборник – Королев МО: Изд-во «Канцлер», ФТА, 2014.
13. Соляной В.Н., Сухотерин А.И., Успенский Ф. А. Новые образовательные технологии в подготовке профессионалов информационной безопасности на базе ГБОУ ВПО МО «ФИНАНСОВО ТЕХНОЛОГИЧЕСКАЯ АКАДЕМИЯ» «Современные образовательные технологии, используемые в очном, заочном и дополнительном образовании» [Текст] сборник – Королев МО: Изд-во «Канцлер», ФТА, 2014.
14. Манько Н.П., Сухотерин А.И., Антоненко В.И. Взгляды на роль и технологию организации самостоятельной работы, как одного из направлений совершенствования образовательного процесса. «Современные образовательные технологии, используемые в очном, заочном и дополнительном образовании» [Текст] сборник – Королев МО: Изд-во «Канцлер», ФТА, 2014.