Модель мобильна и свободна, так как она предусматривает формирование компетенций на любой ступени образования, в соответствии с требуемым уровнем ее освоения.

Реализуемые в рамках компетентностного подхода идеи, на основе которых, создана модель специалиста в области информационной безопасности как основа конструирования и обоснования единого измерения в системе ВПО, а, следовательно, и построения содержания образования по направлению подготовки 090900 «Информационная безопасность», заключаются в следующем: представление о личности как о целостности; доминирование в структуре модели «личностного» начала как системообразующего, придающего направленность непрерывному развитию общепрофессиональной компетентности; трактовка модели как стратегического ориентира, образа, в направлении которого должен «твориться» специалист в области защиты информации как личность и профессионал.

Компетентностный подход соответствует условиям рыночного хозяйствования, ибо он предполагает ориентацию на формирование наряду с профессиональными знаниями, еще и развитие у обучающихся таких универсальных способностей и готовностей, которые востребованы современным рынком труда.

Таким образом, проектируемое на такой основе содержание вузовского образования в области информационной безопасности сможет обеспечить целостное компетентностное образование, которое призвано решать проблемы, связанные с подготовкой высококвалифицированного, конкурентноспособного на рынке труда специалиста.

Г.Н. Чусавитина

АПРОБАЦИЯ ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИХ УСЛОВИЙ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПОДГОТОВКИ НАУЧНО-ПЕДАГОГИЧЕСКИХ КАДРОВ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ЭЛЕКТРОННОГО ОБРАЗОВАНИЯ И НАУКИ

gala_m27@mail.ru

ФГБОУ ВПО «Магнитогорский государственный университет», Магнитогорск

The pilot study for the proof of efficiency of a complex of the allocated pedagogical conditions for increase of level of competence of scientific and pedagogical shots in the field of ensuring the information security, realized on the basis of the developed model was carried out.

В рамках научно-исследовательского проекта № 11-06-01006а «Разработка и апробация модели подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде», выполненного при финансовой поддержке РГНФ была разработана модель подготовки научно-педагогических кадров к обеспечению информационной безопасности (ИБ) в сфере электронного образования и науки, которая состоит из следующих основных компонентов: целевого, содержательно-технологического и результативного. Система может успешно функционировать при наличии комплекса условий способствующих повышения эффективности подготовки включающего в себя:

- междисциплинарную интеграцию при подготовке в области защиты информации;
- включение обучающихся в совместную продуктивную деятельность по разработке и внедрению программы (политики) безопасности образовательного учреждения;
- разработка специализированного образовательного портала посвященного проблематике обеспечения ИБ в сфере науки и образования.

Опытно-эксперименталная работа осуществлялась в рамках профессиональной подготовки студентов МаГУ обучающихся по направлениям 230700 «Прикладная информатика», 080500 «Бизнес-информатика», 050100 «Педагогическое образование (профили «Информатика и математика», «Начальное образование и информатика», «Технологии и информатика») и в системе повышения квалификации научно- педагогических кадров г. Магнитогорска и Челябинской обл. Были организованы курсы повышения квалификации для преподавателей вуза с выдачей удостоверений государственного образца о краткосрочном повышении квалификации в Институте дополнительного образования ФГБОУ ВПО «Магнитогорский государственный университет» по следующим программам: «Технологии электронного обучения. Администрирование систем электронного обучения», «Теория и практика свободного программного обеспечения». Была актуализирована тематика научно-исследовательской работы студентов, аспирантов и молодых исследователей, материалы исследования использовались в курсовом и дипломном проектировании со студентами вузов, в работе научных школ, при организации НИР и НИРС на базе учебной лаборатории «Информационная безопасность»: написание тезисов, эссе, рефератов и курсовых работ по направлениям тематики проекта. В 2012 году была продолжена работа по стратегическому партнерству с ИТ-компаниями при подготовке специалистов по вопросам обеспечения ИБ (Compas Plus, Cisco System, Inc., ЗАО «Лаборатория Касперского», Digital Security и др.). При этом партнеры участвовали в проведении учебных занятий со студентами, организации конференций, мастер-классов и круглых столов, руководстве научно-исследовательскими работами студентов и профессиональными студенческими практиками.

Одним из конкурентных преимуществ современного ИТ-специалиста является его компетентность в сфере информационной безопасности и защиты информации. В целях популяризации и обобщения опыта работы на базе МаГУ в 2012 г. была проведена Всероссийская конференция «Разработка инновационных механизмов повышения конкурентоспособности выпускников ИТ-специальностей вуза в условиях монопромышленного города». В рамках конференции была организована секция посвященная проблемам подготовки специалистов в области ИБ. По итогам проведенной конференции был издан сборник статей по материалам лучших докладов обсуждаемых на мероприятии. Участники проекта Чусавитина Г.Н., Давлеткиреева Л.З. вошли в организационный комитет, а Назарова О. Б. в программный комитет Международной научно-практической конференции «Новые информационные технологии в образовании» (г. Екатеринбург-Магнитогорск). По инициативе исполнителей проекта на данной конференции была организована секция «Информационно образовательная среда вуза», на которой рассматривались проблемы обеспечения безопасности информационно-образовательной среды. Участники проекта Чусавитина Г.Н., Давлеткиреева Л.З. являлись членами организационного комитета VII Международной научно-практической конференции «Современные информационные технологии и ИТ- образование» (г. Москва, МГУ имени М.В. Ломоносова). Материалы проекта использовались при разработке электронного учебно- методического комплекса (ЭУМК) «Информационная безопасность в открытом образовании» для студентов, обучающихся попедагогическим специальностя (Педагогическое образование (профили «Информатика», «Информатика и математика», «Начальное образование и информатика», «Технологии и информатика» и др.); ЭУМК «Информационная безопасность» (для

направлений подготовки 230700 «Прикладная информатика», 080500 «Бизнес-информатика», системы профессиональной подготовки и повышения квалификации). Поданы документы на получение свидетельства ОФАП об отраслевой регистрации ЭУМК «Информационная безопасность в открытом образовании». Исполнителями проекта написана монография «Аудит информационной инфраструктуры компании и разработка ИТ-стратегии» (О.Б. Назарова, Л.З. Давлеткиреева и др.). По результатам проекта опубликовано 18 публикаций, из них 12 статей (в том числе 1 из реестра ВАК), 4 тезисов, 1 сборник научных трудов, 1 монография, 2 ЭУМК.

Библиографический список

1. *Чусавитина Г.Н. , Чусавитин М.О.* Подготовка студентов педагогических специальностей университета к профилактике и противодействию идеологии киберэкстремизма среди молодежи, II Всероссийская научно-практическая конференция «Информационные технологии в образовании XXI века». //Сборник научных трудов. Т. 1. – М.: НИЯУ МИФИ.2012 -376с., Москва, 2012, -С. 322 – 326.

2. *Чусавитина Г.Н. , Чусавитин М.О.* Модель подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде// Материалы Международной научно-практической конференции «Новые информационные технологии в образовании», ФГАОУ ВПО «Рос. гос. проф.-пед. ун-т»., Екатеринбург, 2012, -С.519 – 521.

Е.Д. Шамонин

УГРОЗЫ, ИСХОЯЩИЕ ОТ ЗОМБИ-СЕТЕЙ

shamonined@mail.ru

Институт математики и компьютерных наук УрФУ, г. Екатерибург

Оснащение учебных заведений огромным количеством средств вычислительной техники (СВТ), в том числе с возможностью выхода в глобальную сеть Интернет, кроме беспрецедентных возможностей по автоматизации процессов обучения влечет за собой и ряд весьма негативных факторов, наиболее грозным из которых является вовлечение части этих компьютеров в зомби-сети (ботнеты).

Хотя термин «ботнет» может обозначать любую группу ботов, например IRC (Internet Relay Chat) ботов, обычно его относят к группе компьютеров, зараженной специальной программой — сетевым червем или троянской программой, управляемой из одного источника. Владелец ботнета может удаленно управлять группой, обычно через IRC сервер или специальный канал в публичной IRC сети. Заражение систем осуществляется с использованием различных инструментов (эксплойты, переполнение буфера и др.). Новые боты — компьютеры, вовлеченные в зомби-сети — могут автоматически сканировать среду, обнаруживать уязвимости, осуществлять атаки на слабые пароли, производить рассылку спама и пр. Ботнеты обладают мощными вычислительными ресурсами, являются грозным кибероружием и хорошим способом зарабатывания денег для злоумышленников.

Управление компьютером, который заражен ботом, может быть прямым и опосредованным. В случае прямого управления злоумышленник может установить связь с инфицированным компьютером и управлять им, используя встроенные в тело программы-бота команды. В случае опосредованного управления бот сам соединяется с центром управления или другими машинами в сети, посылает запрос и выполняет полученную команду.