

УДК 378:147.88

## ОПЫТ АКАДЕМИЧЕСКОГО ПАРТНЁРСТВА ВУЗА И ПРОИЗВОДИТЕЛЕЙ ПО В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ КОНКУРЕНТОСПОСОБНОСТИ СТУДЕНТОВ

**Чернова Е.В.**

*ФГБОУ ВПО «Магнитогорский государственный университет»,  
Магнитогорск, e-mail: EChernova@masu-inform.ru*

В статье описан опыт академического партнерства факультета информатики ФГБОУ ВПО «Магнитогорский государственный университет» и компаний разработчиков программного обеспечения в области информационной безопасности и защиты информации: ЗАО «Лаборатория Касперского», ООО «Digital Security», компания SearchInform. Перечислены основные элементы академических программ сотрудничества, возможности, которые предоставляют компании для студентов и внедрение их в образовательный процесс ИТ-специальностей. Приведены особенности программных средств, предоставленных компаниями-партнерами, а также их значимость в обучении будущих ИТ-специалистов для повышения их конкурентоспособности на рынке труда, особенно в условиях монопромышленного города. Описаны особенности включения академических программ в реальный образовательный процесс на примере изучения дисциплин, связанных с обеспечением информационной безопасности и защиты информации.

**Ключевые слова:** информационная безопасность, защита информации, академическое партнерство, государственный стандарт, ИТ-специалист, монопромышленный город, конкурентоспособность, компетенции в области информационной безопасности и защиты информации

## EXPERIENCE ACADEMIC PARTNERSHIP OF THE UNIVERSITY AND DEVELOPING SOFTWARE IN THE FIELD OF INFORMATION SECURITY AS TOOL TO INCREASE COMPETITIVE STUDENTS

**Chernova E.V.**

*Magnitogorsk State University, Magnitogorsk, e-mail: EChernova@masu-inform.ru*

The paper describes the experience of the faculty of computer science academic partnership Magnitogorsk State University and companies, software developers in the field of information security and data protection: «Kaspersky Lab, «Digital Security», company SearchInform. Are the key elements of the academic program of cooperation opportunities offered by the company for the students and put them in the educational process of IT-specialties. And the features of the software provided by partner companies, as well as their importance in the training of future IT professionals to enhance their competitiveness in the labor market, especially in monoindustrial city. The features include academic programs in the education process to a real example of the study subjects related to information security and data protection.

**Keywords:** information security, information security, academic partnerships, state standard, IT professional, monoindustrial city competitiveness, competence in the field of information security and data protection

Вопрос конкурентоспособности выпускника вуза является краеугольным камнем всей системы высшего образования. Не секрет, что на сегодняшний день в системе образования есть ряд проблем, которые нельзя не учитывать при построении образовательной траектории: уменьшение количества абитуриентов, рост и вариативность требований работодателей к содержанию подготовки будущего работника, изменения на рынке труда. В подобных условиях особое место в системе подготовки ИТ-специалиста занимает академическое партнерство с ведущими компаниями – как российскими, так и международными. Академическое партнерство – это способ сотрудничества на образовательном уровне между разработчиком программного обеспечения и вузом. Компания-партнер предоставляет вузу программные средства и образовательные материалы, для того

чтобы студенты могли освоить тот или иной программный продукт в процессе изучения определенной взаимосвязанной дисциплины. Выгода от партнерских программ очевидна как для самих компаний, так и для вузов. Вузы получают возможность бесплатно и при техническом сопровождении изучать дорогостоящие программные средства, получать методические материалы для углубленной работы с ними и давать возможность студентам получать дополнительные ИТ-навыки. Как считает Г.Н. Смородин: «Поскольку корпорация является публичной компанией, то можно утверждать, что присутствие академического партнера на рынке образовательных услуг сказывается на курсовой стоимости акций корпорации. Активность академического партнерства непосредственно воздействует на имидж корпорации и на узнаваемость ее бренда. Помимо этого формируется организацион-

ная структура партнерства и накапливается его интеллектуальная собственность» [7]. Таким образом, при минимальных затратах компании получают на местах готовых специалистов, ориентированных на использование именно их программного средства, а не каких-либо еще.

Факультет информатики Магнитогорского государственного университета является академическим партнером нескольких компаний, признанных в области обеспечения защиты информации и информационной безопасности: ЗАО «Лаборатория Касперского», ООО «Digital Security», компания SearchInform и других.

ЗАО «Лаборатория Касперского» – одна из наиболее динамично развивающихся компаний в сфере информационной безопасности. Она входит в четверку ведущих мировых производителей программных решений для защиты конечных устройств [1].

«Академия Касперского» – это образовательная программа для средних профессиональных и высших учебных заведений, а также центров повышения квалификации и переподготовки преподавателей. Основные направления программы – это распространение передовых знаний и опыта в области защиты информации от современных компьютерных угроз, модернизация учебного процесса в соответствии с потребностями рынка и обеспечение доступным комплексом антивирусной защиты в системе высшего, послевузовского и дополнительного образования.

Цели академического партнерства между ЗАО «Лаборатория Касперского» и факультетом информатики в рамках программы «Академия Касперского»:

- сотрудничество в разработке учебных курсов для студентов по информационной безопасности, включение их в учебный процесс и в систему дистанционного обучения;
- сотрудничество в разработке методического материала для педагогов по различным аспектам информационной безопасности, включение их в электронную библиотеку;
- проведение курсов по антивирусной безопасности при подготовке студентов вуза и в системе дополнительного образования и повышения квалификации;
- проведение научно-исследовательских работ;
- проведение конкурсов, олимпиад, конференций, семинаров и т.п.;
- организация и проведение производственной практики студентов на базе «Лаборатории Касперского».

Студенты факультета информатики участвуют в образовательных инициативах

в рамках «Академии Касперского» конкурс «IT Security for the Next Generation»; вебинары; разработка методических материалов; разработка инновационных проектов, связанных с обеспечением информационной безопасности и антивирусной защиты. За время сотрудничества было одержано 6 побед в заочном туре Международной студенческой конференции по проблемам компьютерной безопасности «IT Security Conference for the Next Generation». Победители получили возможность провести несколько дней в Москве в Лаборатории Касперского, посетить мастер-классы, познакомиться с сотрудниками и даже попробовать свои силы на практических занятиях. Программа «Академия Касперского» ориентирована на поиск в вузах одаренных студентов, им предлагают пройти практику на базе «Лаборатории Касперского» с последующим трудоустройством. Для преподавателей разработаны несколько курсов, которые можно полностью включить в читаемые дисциплины, связанные с обеспечением защиты информации: «Основы компьютерной безопасности», «Компьютерные угрозы: методы обнаружения и анализа», «Основы антивирусной защиты». На ресурсе «Академии» есть онлайн лекции по различным тематикам, учебные проекты, научные статьи, которые любой участник партнерской программы может использовать в своей образовательной и педагогической деятельности. Также «Академия» предоставляет возможность педагогам обмениваться своими разработками; проводить различные мероприятия, где основным спонсором выступает «Лаборатория Касперского»; участвовать в программе поддержки инновационных проектов для студентов, аспирантов, ученых в области информационной безопасности и смежных отраслях. Студенты имеют возможность проходить учебно-производственную практику в отделах компании для изучения и освоения одного из приемов производственного процесса или освоения используемой методики, проходить стажировку и приобрести опыт сотрудничества с ведущей компанией сферы защиты информации. Специалисты «Лаборатории Касперского» могут выступать консультантами при написании дипломных выпускных квалификационных работ, которые будут иметь прикладное значение.

ООО «Digital Security» – одна из ведущих российских консалтинговых компаний в области информационной безопасности, а также в области оценки соответствия информационных систем требованиям ISO 27001/ISO 17799, лидер на рынке специали-

зированных систем анализа и управления информационными рисками и политикой безопасности в соответствии с ISO 27001/ISO 17799 [3]. В настоящее время возникло множество технологических, правовых и организационных проблем, связанных с обеспечением информационной безопасности. Развитие компьютерных сетей и хранение информации на электронных носителях привело компании к необходимости предпринимать меры по защите своих информационных ресурсов от несанкционированного доступа, искажения или уничтожения информации. Понятно, что решение подобных задач требует привлечения большого числа высококвалифицированных специалистов и создания полноценных научных направлений, связанных с уровнем обеспечения комплексной защиты. Студентам факультета информатики МаГУ, изучающим вопросы информационной безопасности, предоставлена возможность работать с лицензионным программным обеспечением компании Digital Security, позволяющим осуществить аудит информационной безопасности:

- система анализа и управления рисками ГРИФ

- система разработки управления политикой информационной безопасности КОНДОР.

Система ГРИФ позволяет построить приближенную модель информационной системы, содержащую наиболее критичные ресурсы и основные угрозы и уязвимости с учетом вероятности их реализации. Полученная модель показывает наиболее уязвимые места информационной системы, уровень ущерба, к которому может привести каждая уязвимость, а также позволяет принять решение о том, какие контрмеры будут наиболее эффективны. Это позволяет расставить приоритеты и заранее оценить результативность планируемых мероприятий при управлении информационными рисками компании. Работа с этой системой помогает студенту в целом увидеть проблемы в системе безопасности изучаемого «виртуального» предприятия, а так же лучше изучить его структуру, так как для работы системы нужны сведения о ресурсах обработки и хранения информации; видах информации в информационной системе предприятия; группах пользователей, имеющих доступ к информации в системе; физическую структуру системы; бизнес-процессы компании; программные средства защиты информации.

Система КОНДОР включает в себя базы стандартов управления информационной безопасностью (ISO 17799:2000, ISO 17799:2005, ISO 27001, СТО БР ИББС-1.0-

2006), представленных в виде перечня требований. Анализируя выполнение каждого требования, система позволяет получить полную картину – какие положения стандартов выполняются, а какие нет. Модуль управления контрмерами отражает все невыполненные положения стандартов безопасности. Помимо этого в системе предусмотрена возможность создавать свои базы требований, чтобы провести оценку соответствия, например, корпоративному стандарту безопасности. Студенты могут с помощью КОНДОР разработать с нуля, проанализировать существующую политику безопасности, разработать и внедрить изменения и дополнения в соответствии с лучшими международными стандартами [3].

Компания «SearchInform» – ведущий российский разработчик средств информационной безопасности. Компания образовалась в 1995 году и сначала специализировалась на технологиях поиска, хранения и обработки информации. Сегодня эта компания – признанный лидер и эксперт на рынках информационной безопасности России и других стран СНГ. Продукция компании сертифицирована и отмечена рядом специализированных наград. Основным продуктом компании на сегодняшний день является «Контур информационной безопасности SearchInform» – комплексное решение для защиты от утечек конфиденциальной информации и контроля информационных потоков в организациях [2]. «Контур информационной безопасности SearchInform» позволяет выявлять утечки конфиденциальной информации через e-mail, ICQ, голосовые и текстовые сообщения Skype, посты на форумах или комментарии в блогах, внешние устройства (USB/CD/DVD), документы, отправляемые на печать, а также появление конфиденциальной информации на компьютерах пользователей. На базе компьютерных классов факультета информатики открыт учебный стенд для проведения лабораторных работ по обеспечению защиты конфиденциальной информации в организации. Контур имеет модульную структуру и осуществляет контроль за информационными потоками предприятия на всех уровнях – от компьютера каждого отдельного пользователя до серверов локальной сети; контролируются также все данные, уходящие в интернет [4].

Работа с подобным мощным инструментом позволяет студентам четко представлять потоки информации, циркулирующие на предприятии, уметь классифицировать информацию по степеням конфиденциальности, определять допуск лиц к работе с конфиденциальной информацией, отсле-

живать действия, производимые с каждым документом. Работа с контуром подразумевает под собой четкое понимание законодательной базы обеспечения информационной безопасности и защиты информации на предприятии, что, несомненно, является дополнительным плюсом к получаемым компетенциям. Академическое партнерство позволяет вузу не только получить бесплатно «Контур информационной безопасности», но и быть равным партнером, создавая методические разработки и участвуя в совершенствовании данного программного средства.

На факультете информатики программы и учебные материалы, предоставляемые академическими партнерами, широко используются для преподавания дисциплин, связанных с информационной безопасностью и защитой информации. Студенты на протяжении всего обучения работают с «виртуальной компанией» и по окончании курса они должны иметь представление о построении политики информационной безопасности предприятия с использованием предлагаемых программных средств. В начале студенты разбивают весь массив информации, циркулирующей в системе, по степеням конфиденциальности, затем определяют группы пользователей, имеющих доступ к каждой степени конфиденциальности. После этого составляется схема физических и логических взаимосвязей ресурсов и доступа к ним пользователей, определяются программные средства и доступ в Интернет и т.п. Затем производится настройка антивирусного и антишпионского программного обеспечения по учебным материалам, предоставленным «Академией Касперского». Параллельно с этим студенты изучают основы компьютерной вирусологии, их действий, последствий и принципов работы антивирусных программ (вебинары или дистанционные курсы от «Лаборатории Касперского» – с получением сертификатов об обучении). После этого студенты приступают к работе с системами ГРИФ и КОНДОР, знакомясь со стандартами информационной безопасности: ISO/IEC 27000 «Словарь и определения», ISO/IEC 17799:2000 «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности», ISO/IEC 27001:2005 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования», СТО БР ИББС-1.0–2006. Обеспечение информационной безопасности организаций банковской системы Российской Федерации», BS 7799-3:2006 «Руководство по менеджменту рисков ИБ»,

ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения» и др. Проведя анализ угроз и уязвимостей системы в программе ГРИФ, студент должен получить инвентаризацию ресурсов и видов информации компании; значения рисков для каждого ресурса и вида информации; перечень уязвимостей, влияющих на значения рисков. И в соответствии с полученными результатами провести работу над данными в системе. В системе КОНДОР студент проверяет разработанную политику информационной безопасности на соответствие требованиями международных стандартов по информационной безопасности, затем снова модифицирует разработанную политику согласно полученным результатам. Программный продукт «Контур информационной безопасности» ориентирован на выявление внутренних утечек компании, на инсайдеров. Студенты изучают основы работы с персоналом, принципы распределения ролей в системе, организации доступа к информации, а затем отслеживании возможных утечек с помощью специального инструментария.

В результате работы с тремя академическими программами студент получает компетенции, позволяющие ему обеспечивать защиту информации и информационную безопасность на разных уровнях – на прикладном (программы), на уровне персонала (распределение степени допуска, работа с утечками, изучение «человеческого фактора»), на уровне предприятия (политика информационной безопасности организации в целом).

Таким образом, академические партнерские программы вузов и производителей программного обеспечения позволят вузам монопромышленных городов готовить ИТ-специалистов, обладающих конкурентоспособностью в области обеспечения информационной безопасности предприятия, так как они будут иметь опыт работы со специализированными программными средствами высокого уровня, и работодателю не придется самостоятельно обучать сотрудника необходимым средствам обеспечения защиты информации и информационной безопасности.

*Публикация выполнена при поддержке РГНФ № 11-06-01006а «Разработка и апробация модели подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде» и № 10-06-01184а «Разработка инновационных механизмов повышения конкурентоспособности выпускников ИТ-специальностей вуза в условиях монопромышленного города».*



**Список литературы**

1. ЗАО «Лаборатория Касперского». [Электронный ресурс]. – URL: <http://www.kaspersky.ru> (дата обращения: 18.10.2012).
2. Компания «SearchInform». [Электронный ресурс]. – URL: <http://searchinform.ru> (дата обращения: 18.10.2012).
3. ООО «Digital Security». [Электронный ресурс]. – URL: <http://www.dsec.ru> (дата обращения: 18.10.2012).
4. Попова И.В. Проблемы взаимодействия системы профессионального образования и рынка труда в монопромышленном городе // Проблемы и перспективы социально-экономического реформирования современного государства и общества: материалы IV международной научно-практической конференции 3–4 октября 2011 г. – М., 2011. – С. 264–270.
5. Повышение конкурентоспособности выпускников ИТ-специальностей вуза в условиях монопромышленного города / под ред. Г.Н. Чусавитиной. – Магнитогорск: МаГУ, 2010. – 158 с.
6. Смородин Г.Н. Академическое партнерство как инвестиционный проект корпорации. [Электронный ресурс]. – URL: <http://2011.ит-образование.рф/section/77/3897/> (дата обращения: 18.10.2012).
7. Султанова Г.Г., Лапшина В.Б. Будущее ИТ-специалистов. – Социально-экономические и гуманитарные приоритеты развития России: материалы XXVIII междунар. науч.-практ. конф.: в 2 ч. / Урал. соц.-экон. ин-т (ф) АТиСО. – Челябинск, 2011 – Ч. II. – 260 с – С. 199–203., Челябинск, 2011, 28, 2, 199–203.

**References**

1. Kaspersky Lab Available at: <http://www.kaspersky.ru> (accessed 18.10.2012).

2. SearchInform Available at: <http://searchinform.ru> (accessed 18.10.2012).

3. Digital Security Available at: <http://www.dsec.ru> (accessed 18.10.2012).

4. Popova I.V. Problems of interaction between vocational education and the labor market in monoindustrial city. – Problems and prospects of socio-economic reforms of the modern state and society: Proceedings of the IV International Scientific Conference on October 3–4, 2011: Moscow, 2011. 264–270.

5. Improving the competitiveness of graduates of IT professions university in the city monoindustrial / ed. G.N. Chusavtina. Magnitogorsk: MaSU, 2010. 158 p.

6. Smorodin G.N. Academic partnerships as an investment corporation Available at: <http://2011.ит-образование.рф/section/77/3897/> (accessed 18.10.2012).

7. Sultanova G.G., Lapshina V.B. The future of IT professionals. – Socio-economic and human development priorities of Russia: Materials XXVIII Intern. Scientific-practical conference. Conf.: 2 hrs / Urals. Social-economical. Institute (f) ALSR. – Chelyabinsk, 2011 Ч. II. 260 p. – pp. 199–203., Chelyabinsk, 2011, 28, 2, 199–203.

**Рецензенты:**

Назарова О.Л., д.п.н., профессор кафедры информатики и экономики ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», г. Магнитогорск;

Девятов Д.Х., д.т.н., профессор, зав. каф. вычислительной техники и прикладной информатики ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», г. Магнитогорск.

Работа поступила в редакцию 26.11.2012.