# Информационная безопасность как необходимый элемент развития информатизации вуза

## А. И. Горелова, С. Н. Ефимова

ЗАО «Лаборатория Касперского»

Москва

Anastasiya.Gorelova@kaspersky.com

Информационная грамотность и навыки безопасной работы с современными компьютерными средствами сегодня являются одними из самых востребованных и необходимых современному выпускнику университета знаний. Информатизация вуза включает в себя несколько направлений, таких как административно-управленческое, улучшение характеристик учебного процесса, развитие научно-исследовательских проектов и создание новых форм обучения (например, дистанционное обучение); все они требуют не только достаточного финансирования, но и понимания проблем безопасности, порядка организации защищенной сети, обучения пользователей грамотной работе в новой информационной среде.

Ввиду новых условий на передовую информатизации после технического оснащения вуза должно выйти обучение всех участников: администрации вуза, преподавателей, студентов, родителей, непосредственно пользующихся всей новой инфраструктурой вуза.

Безопасность каждого из уровней инфраструктуры требует своего подхода, знаний и умений. Рассмотрим уровни подробно:

* Административно-управленческий уровень. Включает в себя использование ИТ-средств для оптимизации управленческих задач, построения единой корпоративной сети, создания баз данных. На этом уровне необходимо обеспечить безопасность всех узлов на уровне сети, как-то безопасность серверов, интернет-шлюзов, организовать и обеспечить резервное копирование, безопасность и сохранность персональных данных и т.п. Необходимыми знаниями должны обладать системные администраторы вуза. Однако их важно постоянно актуализировать: знакомиться с новыми технологиями, программными продуктами, инструментами, владеть знаниями о современных компьютерных угрозах и методах защиты от них.
* Персональный уровень. Важным разделом этого уровня является работа с пользователями инфраструктуры: преподавателями и студентами, а также родителями – внешними пользователями инфраструктуры. Помимо программной защиты персональных компьютеров на рабочих местах, необходимо образовывать пользователей на предмет ознакомления с новыми уловками киберпреступников, направленных на кражу, взлом и хищение важной информации. Для повышения уровня компьютерной грамотности требуется постоянное владение современной ситуацией в сфере угроз: какие атаки существуют, на что направлены, как их узнать, что делать при столкновении с киберугрозой.
* Пользовательский уровень. Значимыми являются знания сетевого этикета и понимание последствий необдуманных действий в сети. Не секрет, что большая часть студентов являются активными пользователями социальных сетей, форумов, блогов. Размещаемая на этих страницах информация, кажущаяся безобидной в настоящее время, может сыграть отрицательную роль в будущем. К сожалению, об этом практически не говорят на лекциях по информационным технологиям, безликость интернет-сообществ привлекает молодежь вседозволенностью. Однако последствия могут быть необратимы. Важно понимать, что любая информация, когда-либо размещенная в сети, останется там навсегда.

К сожалению, учебная программа вуза, загрузка преподавателей и недостаток необходимых актуальных сведений не всегда позволяют решить проблему обучения безопасной работе в условиях информатизации вуза в кратчайшие сроки. Необходимыми знаниями должны делиться представители ИТ-вендоров, заинтересованные в подготовке высококлассных специалистов. Именно на этом этапе возникает неразрывная связь вуз – предприятие, нацеленная на совершенствование образовательной среды. Добиться эффективной работы схемы вуз – предпритяие можно, решая комплекс задач:

1. Обучение преподавателей (стажировки). При участии ИТ-компании и ее экспертов;

2. Привлечение студентов к участию в дистанционных образовательных семинарах, организованных ИТ-компанией;

3. Вовлечение молодых ученых, талантливых преподавателей в развитие научно-исследовательского направления, востребованного ИТ-компанией и реализуемого совместно с вузом;

4. Создание методических материалов для преподавателя, курсов, пособий, готовых к использованию на лекциях, разработанных совместно экспертами ИТ-компании и преподавателями вуза.

Поддержку в решении подобных задач может оказать образовательная программа «Академия Касперского», предлагающая учебным учреждениям учебные курсы, обучение, НИР и т.п. Исходя из этого, для включения в учебный процесс «Лабораторией Касперского» рекомендуются учебные курсы, содержащие базовые разделы:

* Информационная безопасность и уровни ее обеспечения;
* Вредоносные программы и защита от них;
* Информационная безопасность в компьютерных сетях;
* Механизмы обеспечения информационной безопасности.

Для технических специальностей необходим дополнительный упор на развитие навыков защиты от атак, прикладных исследовательских проектов, практическое применение полученных знаний таких как:

* навыки детектирования вредоносной программы;
* исследование уязвимостей интернет-браузеров;
* изучение основ статического анализа программ с помощью дизассемблеров с целью обнаружения присутствия вредоносной составляющей, методы анализа программ;
* освоение особенностей упаковщиков исполняемых файлов и многое другое.

Курсы, включающие рекомендуемые разделы уже сегодня доступны для академических партнеров образовательной программы и размещены в партнерском разделе на сайте «Академии Касперского». Помимо учебного текста и практических работ, доступны видеоролики, презентации к лекциям, рекомендации авторов курсов, консультации экспертов и многое другое.

Применить полученные знания студенты могут, либо пройдя практику в «Лаборатории Касперского», либо став участниками программ стажировок. Также компания уделяет большое внимание развитию и поддержке научной работы молодых ученых и преподавателей. Для этих целей проводится Международная студенческая конференция по проблемам информационной безопасности «IT Security for the Next Generation», а также реализуется программа поддержки инновационных проектов (грантов). Любой желающий может подать заявку на участие в указанных мероприятиях и в случае высокой оценки научного исследования стать участником различных мастер-классов, встреч с экспертами и получить ценный приз.

В качестве дополнительного обучения компания предлагает вузам принимать участие в циклах дистанционных семинаров на тематику ИБ, викторинах, конкурсах, Днях информационной безопасности и др.

Подробнее о программах сотрудничества с образовательными учреждениями можно узнать на сайте: http://www.kasperskyacademy.com/ru/.