Стариченко Е.Б.

НЕКОТОРЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СРЕДЫ ВУЗА

old@uspu.ru
ГОУ ВПО Уральский государственный педагогический университет
г. Екатеринбург

В настоящее время трудно переоценить значение сетевых и коммуникационных технологий и их роль в развитии общества. Умение пользоваться ими как для поиска необходимой информации, так и для организации взаимодействия с окружающими, становится элементом информационной культуры современного человека. Однако её формирование по-прежнему остаётся достаточно сложной задачей. Эта проблема касается как людей, получивших образование достаточно давно, так и современных студентов, выросших рядом с компьютером.

Следствием пренебрежения элементарными правилами информационной безопасности чаще всего являются локальные эпидемии компьютерных вирусов, что приводит к снижению работоспособности сети учебного заведения, к отказам и простоям в работе оборудования, к потере важных данных. Опыт администрирования кампусной сети Уральского государственного педагогического университета показывает, что пользователи всецело полагаются на установленную антивирусную программу, считая, что одного факта наличия её на компьютере вполне достаточно для полноценной защиты. При этом совершенно не принимается во внимание необходимость выполнения стандартных и простых действий по проверке носителей и жёсткого диска, а также элементарные правила работы с электронной почтой. В значительной степени это касается работников, достаточно давно закончивших образование, для которых компьютер до сих пор не стал полноценным рабочим инструментом.

Для разрешения сложившейся ситуации, управлением информатизации УрГПУ принимаются меры в различных направлениях. С одной стороны в течение учебного года постоянно действуют и регулярно проводятся курсы повышения квалификации профессорско-преподавательского состава и административных работников, на которых сотрудникам объясняют основы информационной культуры, обучают их работе с базовыми программными средствами, акцентируя внимание на правильном и систематическом использовании антивирусных пакетов.

Защита сети техническими средствами является другим направлением деятельности сотрудников нашего управления. В 2008 году в значительной степени реорганизована кабельная система, созданы активные узловые точки, в которых расположены управляемые коммутаторы. Все узлы соединены магистральными линиями с центральным коммутатором. Такая схема, невозможная на начальном этапе создания сети (как по финансовым, так и по временным причинам), позволила предоставить каждому пользователю персональный порт, логически разделить всё сетевое пространство на виртуальные подсети, контролировать и легко определять источник паразитного трафика, порождаемого вредоносными программами. Разделение пользователей по виртуальным сетям осуществляется по подразделениям или кабинетам. Это позволяет сохранить привычную и комфортную обстановку для работы, когда коллеги, работая над решением одной производственной задачи, обмениваются документами, предоставляя к ним общий доступ. С точки зрения безопасности такой подход позволяет ограничить ареал распространения вирусов одной виртуальной сетью, а также блокировать распространение широковещательного трафика за её пределы.

Со времени начала работ по реорганизации сети УрГПУ значительно устойчивее стала работать сеть, прекратились отказы на обслуживание абонентов со стороны оборудования, стабилизировалась скорость доступа к внешним и внутренним ресурсам.

Таким образом, решение проблемы недостаточной информационной культуры работников вуза должно вестись по нескольким направления, что повышает результативность принимаемых мер как технического, так и организационного характера.

Шамонин Е.Д.

ЗАЩИТА ПРИВАТНОЙ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

shamonined@mail.ru
Уральский государственный университет (УрГУ)
г. Екатеринбург

Практически любой вид деятельности, в том числе научная и преподавательская, в настоящее время немыслима без использования в том или ином виде средств вычислительной техники (СВТ) и информационных технологий (ИТ). Использование для такой деятельности многопользовательских автономных рабочих мест (АРМ), либо рабочих мест в составе сети, неизмеримо повышает ее эффективность, но неизменно влечет за собой вопросы, связанные с необходимостью обезопасить приватную информацию от доступа со стороны посторонних лиц. Однако далеко не каждый преподаватель на рабочем месте имеет в своем полном распоряжении персональный компьютер, на котором вопрос защиты конфиденциальной информации решается достаточно просто. И речь здесь не идет о системах защиты от несанкционированного доступа (НСД), реализованных путем активации защитных функций BIOS (Basic Input/Output System, базовая система ввода/вывода) или установкой сложного пароля на вход в операционную систему.