ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ КАФЕДРЫ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ

Марков А.Н., Боровская О.О., Михалькевич А.В., Пятосин А.В.

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Рассмотрены аспекты и требования, предъявляемые к политике информационной безопасности кафедры высшего учебного заведения. На основе требований информационной политики безопасности осуществлена настройка компьютерных лабораторий для учебно-образовательного процесса.

Современные темпы развития и распространения информационных технологий требуют создания целостной системы информационной безопасности, увязывающей комплекс мер защиты не только самой информации, обрабатываемой и хранящейся в компьютерной сети учреждения образования, но и направленной прежде всего на обеспечение бесперебойной его работы. Построение данной системы должно основываться на научно-технических принципах построения систем обеспечения безопасности информационных ресурсов корпоративных сетей с учетом современных тенденций развития сетевых информационных технологий, а также с использованием исследований по защите от внутренних и внешних нарушителей.

Задачей построения политики информационной безопасности кафедры является выявление и недопущение нарушений в области защиты информации, а также системы оперативного мониторинга и реагирования на нарушения. Основными угрозами информационной безопасности в рамках кафедры учебного заведения являются:

1. Нарушение конфиденциальности (разглашение тайны, утечка информации);
2. Нарушение работоспособности (лаборатории, оборудования, компьютерного класса или же отдельного рабочего места с ПЭВМ);
3. Нарушение целостности (искажение информации, подмена информации, уничтожение).

Информационными ресурсами, на которые направлены воздействия, в рамках кафедры можно считать оборудование, будь то ПЭВМ, или сервер, принадлежащий кафедре и используемый в учебных целях. В этом случае

политика построения информационной безопасности должна включать в себя следующие составляющие:

1. Организация единой локальной компьютерной сети в пределах кафедры, входящей в состав общеуниверситетской компьютерной сети и управляемой как единая система.
2. Организация разграничения политики доступа студентов на рабочие места, в лаборатории, в компьютерные классы и ПЭВМ.
3. Организация контроля пользователей ПЭВМ посредством политики безопасности, наследуемой в пределах учебного заведения свыше, или же создание разграниченной политики безопасности в пределах кафедры.
4. Организация контролируемого доступа к программным продуктам, используемым в учебно-образовательном процесса.
5. Организация контролируемого доступа к общеобразовательным университетским ресурсам и ресурсам кафедры.
6. Недопущение неправомерного и неконтролируемого доступа со сторонних устройств, не ограниченных политикой безопасности локальной сети.
7. Недопущения ограничения антивирусной защиты в пределах кафедры.
8. Неправомерное использование стороннего программного обеспечения, не используемого для учебно-образовательного процесса.
9. Недопущение неконтролируемого заражения вирусами информации посредством переноса на портативных носителях информации.
10. Организация контролируемого разграниченного использования дискового пространства на рабочих местах и сервере.
11. Недопущение доступа посторонних лиц к ресурсам локальной сети, незарегистрированных в ресурсах сети, или же посредством предоставления доступа им сторонними зарегистрированными лицами.

В соответствии с вышеперечисленными составляющими политики информационной безопасности кафедры ответственность за надлежащее исполнение политики лежит на администраторе локальной сети кафедры, инженерах кафедры. Контроль за выполнением требований осуществляет непосредственно заведующий лабораториями кафедры и заведующий кафедрой в целом.

Список использованных источников

[1] В.В. Аксёнов. Аудит системы менеджмента информационной безопасности. Руководство. – Минск: Интернет-изд. http://itsec.by, 2012. – 87 с.