Тема 4.4. Технологии безопасной работы в Сети.

Залогом безопасной работы в сети Интернет является соблюдение основных правил и рекомендаций, таких как грамотное посещение сайтов и проверка почты. Особенно это становится актуальным при работе на общедоступном компьютере. Безопасность при навигации по сайтам и по приему почты будет достигнута при соблюдении следующих рекомендаций:

1. Не ходите на незнакомые сайты.
2. Если ходите, то выключайте (на всякий случай) поддержку языка Java и использование cookies.
3. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы.
4. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину в вашей программе чтения почты. Бывали случаи рассылки вирусов, а также вскрытия крупнейших узлов бесплатной почты. Так что не исключено, что с адреса Вашего знакомого может прийти вирус.
5. Никогда не посылайте никому свой пароль.
6. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв. А еще лучше сгенерируйте его специальной программой или попросите сделать это своего провайдера.

Пять советов по безопасности при работе на общедоступном компьютере

1. *Не сохраняйте свои учетные данные для входа в систему*. После завершения работы на Web-узле обязательно пользуйтесь функцией завершения сеанса работы с Web-узлом. Просто закрыть окно обозревателя или ввести другой адрес недостаточно. Многие программы (особенно программы для обмена мгновенными сообщениями) имеют функцию автоматического входа в систему, сохраняющую имя пользователя и пароль. Отключите эту функцию, чтобы никто, кроме вас, не смог войти в систему.
2. *Не оставляйте без присмотра компьютер с важными сведениями на экране.* Закончив работу на общедоступном компьютере, воспользуйтесь функцией выхода из системы во всех программах и закройте все окна, в которых могут отображаться конфиденциальные данные.
3. *Заметайте свои следы.* В Internet Explorer и других web-обозревателях сохраняются сведения о паролях пользователя и всех посещенных им web-страницах, даже если он закрыл их и вышел из системы.
4. *Опасайтесь подглядывания через плечо.* Работая на общедоступном компьютере, следите за мошенниками, которые подглядывают через плечо, как вы вводите секретные пароли, чтобы потом получить доступ к вашим данным.
5. *Не вводите важные сведения на общедоступном компьютере.*

Эти меры обеспечат некоторую защиту от хакеров-любителей, которые могут воспользоваться компьютером после вас. Однако профессиональный мошенник может установить на общедоступном компьютере специализированное программное обеспечение, которое будет записывать каждое нажатие клавиши, а затем отправлять ему эту информацию по электронной почте.