# Бауманский учебный центр «Специалист»

## Программа курса Информационная безопасность для пользователей

Код курса: **ИБПОЛ**

| Тема | Ак. часов |
|---|---|
| **Модуль 1. Информационная безопасность и киберпреступность**<br><br>• От «сбоев» и «зависаний» до кражи информации, денег и других ценностей – основные угрозы информационной безопасности<br>• Знание и соблюдение требований безопасности – основа эффективного использования компьютера<br>• Киберпреступность<br>• Основные направления и технологии защиты информации для пользователя:<br>  ◦ Безопасность операционной системы<br>  ◦ Безопасность данных пользователя<br>  ◦ Восстановление после сбоев<br>  ◦ Сетевая безопасность | **1** |
| **Модуль 2. Безопасность использования Windows и прикладных программ**<br><br>• Ошибки в программном обеспечении – лазейки для проникновения вредоносных программ<br>• Установка обновлений программного обеспечения – латание «дыр» в системе безопасности<br>• Настройка центра обновления Windows<br>• Зачем ограничивать возможности пользователя компьютера при повседневной работе?<br>• Создание пользователя с ограниченными полномочиями<br>• Создание стойких паролей<br>• Принцип наименьших привилегий. Повышение уровня контроля учетных записей (UAC)<br>• Блокировка компьютера во время простоя<br>• Защита системы. Использование точек восстановления системы<br>• Возврат компьютера в исходное состояние<br>• Создание архивного образа системы и восстановление из образа | **2.5** |
| **Модуль 3. Безопасность данных пользователя**<br><br>• Установка паролей на доступ к документам<br>• Резервное копирование – гарантия сохранения данных пользователя. Резервное копирование файлов и папок<br>• Удаление данных – это не их уничтожение. Восстановление «случайно» удаленных данных - программа Recuva<br>• Безопасное удаление данных – гарантия что никто не получит доступ к вашей личной информации. Средства безопасного удаления данных пользователя<br>  ◦ Команда CIPHER<br>  ◦ Программа Ccleaner<br>• Шифрование – надежный способ уберечь ваши данные от посторонних лиц. Шифрующая файловая система в Windows (EFS) | **2.5** |

| | |
|---|---|
| **Модуль 4. Сетевая безопасность. Защита от вирусов и шпионских программ**<br>• Защита общих папок<br>• Социальная инженерия – использование некомпетентности и доверчивости пользователя<br>• Технологии внедрения вредоносных программ<br>• Виды вредоносного программного обеспечения<br>  ◦ Вирусы<br>  ◦ Черви<br>  ◦ Трояны<br>  ◦ Шпионы<br>• Безопасность при работе в Интернет. Простые советы<br>• Обзор и сравнение наиболее популярных антивирусных средств<br>• Инструменты безопасности Windows<br>• Windows Defender (Microsoft Security Essentials)<br>• Средство удаления вредоносных программ - MRT<br>• Обзор средств борьбы со шпионскими программами | **2** |
| Аудиторная нагрузка в классе с преподавателем | **8 ак.ч. + 8 ак.ч. самостоятельно** |

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

## Контакты центра


Для частных лиц
**+7 (495) 232-32-16**

Для организаций
**+7 (495) 780-48-44**

E-mail
**info@specialist.ru**