Некоммерческая организация
«Союз директоров профессиональных образовательных организаций Кемеровской области»
Государственное профессиональное образовательное учреждения
«Анжеро-Судженский горный техникум»

ИСТОРИЯ, СОВРЕМЕННЫЕ ТЕХНОЛОГИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ РАЗЛИЧНЫХ ОТРАСЛЕЙ ПРОМЫШЛЕННОСТИ

Сборник тезисов областной заочной научно-практической конференции, приуроченной к 300-летию Кузбасса

15.04.2021 г.

МЕТОДЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ МАССОВОМ ПРИМЕНЕНИИ IT – ТЕХНОЛОГИЙ НА ПРИМЕРЕ ГПОУ «СИБИРСКИЙ ПОЛИТЕХНИЧЕСКИЙ ТЕХНИКУМ»

Захаров Максим Евгеньевич
Бек А.Е., Щербакова К.А., преподаватели
ГПОУ «Сибирский политехнический техникум» ,
г. Кемерово

В настоящее время нам часто встречаются такие выражения как: реализованные угрозы, кибершпионаж, исследования, проведенные экспертами в области информационной безопасности. Данная проблема занимает ведущие позиции во многих странах. Однако далеко не все пользователи знают и понимают сферу информационной безопасности.

Целью данной работы является исследование принципов и направлений обеспечения информационной безопасности и ознакомление людей, которые не связанны с ИТ- сферой, с методами защиты информации.

В рамках достижения цели были поставлены следующие задачи: изучить имеющиеся источники по информационной безопасности, познакомиться с методами защиты информации, провести анкетирование и создать всплывающую памятку в компьютерной системе.

Объект исследования - информационная безопасность.

Предметом исследования являются методы защиты информации, а продуктом - всплывающая памятка в компьютерной системе.

В данной работе нами были использованы следующие методы исследования: анализ, анкетирование, обобщение.

Вопросы, касающиеся компьютерной безопасности, должны занимать первоочередное место. В результате несоблюдения мер безопасности компьютерные системы могут выйти из строя, а это в свою очередь может привести к потере персональных данных.

Меры для противодействия утечкам информации делятся на две большие группы:

- технические – защита от несанкционированного доступа к системе, установка сигнализации, резервирование значимых компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и др.
- организационные – подбор персонала, наличие плана восстановления работы сервера после выхода его из строя, охрана серверов и т.д.

Несанкционированный доступ к информации можно получить при ремонте компьютера при помощи прочтения с него информации, даже если