самостоятельно изучать языки программирования. Уровень подготовки не всегда устраивает работодателей и они вынуждение сами в дальнейшем обучать своих работников.

В последние годы прослеживается рост участников данных мероприятий, что говорит о желании совершенствоваться среди участников олимпиад.

Мизгирев Александр Валерьевич, гр. ИЭ-412
Руководитель – Тимофеева Елена Геннадьевна,
ассистент кафедры ИТ ИнИ РГППУ

ЗАЩИТА ИНФОРМАЦИИ ОТ ВНУТРЕННИХ УГРОЗ

Проблема защиты информации от внутренних угроз сегодня стоит практически перед всеми российскими и зарубежными компаниями. Зачастую свои собственные сотрудники, случайно или намеренно, работают против организации

Очевидно, что обиженный или недовольный сотрудник компании, имеющий легальный доступ к сетевым и информационным ресурсам и обладающий определенными знаниями о структуре корпоративной сети, может нанести своей компании гораздо больший ущерб, чем хакер, взламывающий корпоративную сеть через Интернет.

Так, по различным оценкам, от 50 до 80% атак, направленных на получение информации ограниченного доступа, начинается из локальной сети предприятия (интрасети).

Особенную актуальность проблема внутренних угроз получила в связи с появлением и повсеместным распространением мобильных накопителей информации, подключаемых через USB порты - таких как flash-диски, винчестеры с USB-интерфейсом и т.д.

Если службой безопасности не предпринимаются специальные меры, нелояльно настроенный сотрудник компании может практически незаметно пронести на территорию предприятия компактный носитель большого объема и скопировать на него всю интересующую его информацию.

На сегодняшний день на рынке программного обеспечения существуют системы позволяющие снизить риск кражи информации. Они предназначены для блокирования портов персонального компьютера, к которым могут подключаться внешние устройства, предоставляют возможность гибкой настройки прав доступа на основе списков контроля доступа для каждого типа устройств. Для каждого физического или логического устройства и для каждого пользователя или группы пользователей можно разрешить либо полный доступ, либо только на чтение, либо запретить доступ.

Подключаемые устройства могут идентифицироваться по любым признакам, таким как класс устройства, код производителя, код устройства, серийный номер и т.д.

Таким образом, системы могут запретить использование внешних накопителей информации, и разрешить подключение каких-либо других внешних устройств, например, USB-ключей для аутентификации пользователей.

Также, для защиты информации, необходимо разработать политику безопасности в организации, донести ее до пользователей и обучить их правилам безопасной работы с информацией.