

ПАРОЛЬНАЯ ЗАЩИТА ИНФОРМАЦИИ НА ПЕРСОНАЛЬНОМ КОМПЬЮТЕРЕ

БНТУ, Минск

Научный руководитель Дробыш А.А.

Одним из важнейших методов защиты для соблюдения конфиденциальности является разграничение доступа. Практически с момента создания первых многопользовательских операционных систем для ограничения доступа используются пароли. Наверное, у каждого владельца компьютера есть важная информация, которую он хранит на компьютере. Это могут быть отчеты, документы, личное фото, пароли и т.д. Вся эта информация нуждается в защите.

Особенности защиты персонального компьютера от несанкционированного доступа обусловлены спецификой его использования. Как правило, ПК пользуется ограниченное число пользователей. Персональные компьютеры могут работать как в автономном режиме, так и в составе локальных сетей, могут быть подключены к удаленному ПК или локальной сети с помощью модема по телефонной линии.

Защита информации представляет собой применение различных средств и методов, использование мер и осуществление мероприятий для того, чтобы обеспечить систему надежности передаваемой, хранимой и обрабатываемой информации. Процессы по нарушению надежности информации подразделяют на случайные и злоумышленные (преднамеренные). Источниками случайных разрушительных процессов являются непреднамеренные, ошибочные действия людей, технические сбои. Злоумышленные нарушения появляются в результате умышленных действий людей.

Для защиты ПК используются различные программные методы, которые значительно расширяют возможности по обеспечению безопасности хранящейся информации. Среди стандартных защитных средств персонального компьютера наибольшее распространение получили: средства защиты вычислительных ресурсов, использующие парольную идентификацию и

ограничивающие доступ несанкционированного пользователя; применение различных методов шифрования, не зависящих от контекста информации; средства защиты от копирования коммерческих программных продуктов; защита от компьютерных вирусов и создание архивов. Запаролить учётную запись достаточно легко. Однако это считается не внушающим доверие методом в защите компьютера. Такой пароль обойти совсем не сложно.

Также присутствует вероятность загрузки системы с Live CD, вследствие чего, откроется доступ ко всем данным. Для полноценной и надёжной защиты, нужно запаролить полное включение вашего компьютера. После чего ни одна операционная система не сможет загрузиться до того времени, пока не будет указан пароль. Как все-таки создать такую мощную защиту? Чтобы достичь желаемого результата потребуется ввести пароль в структуру BIOS. Такой пароль бывает двух видов: доступ в BIOS, а также пароль на загрузку компьютера. Надо заметить, что все варианты версий BIOS, имеют возможность закрытия доступа. А что касается функции по установке пароля на полную загрузку компьютера, то, она может не предоставляться в его некоторых версиях. Следует помнить и то, что в период работы с BIOS, нужно соблюдать максимальную осторожность. Любая неправильная настройка имеет возможность нанести компьютеру неисправимый урон.

Установленный в BIOS пароль нужно непременно записывать. Устроить это надо таким образом, чтобы всегда была возможность его найти, так как пароль, задаваемый в BIOS, не так легко снять. Существует опция по его сбрасыванию, а чтобы достичь желаемого результата вам также будет нужен заданный ранее пароль. В случае если пароль ввести не получится, то, операционная система попросту не сможет загрузиться, и с данным фактом ничего не поделаешь.

Впрочем, если более глубоко рассмотреть описываемую тему, то и этот метод защиты компьютера с лёгкостью решаем, в случае если человек отлично разбирается в устройстве компьютера.

Пользователь, не обладающий достаточными знаниями, столкнётся с огромной и сложной проблемой, если надумает добраться до информационных данных, которые защищены таким, далеко не простым, паролем на вашем компьютере.