Количество утечек информации растет с каждым днем. Это может коснуться и вас, чтобы предотвратить несанкционированный доступ к вашему компьютеру используйте программные и аппаратные средства защиты. Вместе они воздвигают перед злоумышленниками две линии обороны преодолеть которые сложно программные средства защиты информации от несанкционированного доступа.

Программные продукты которые устанавливаются на ваши компьютеры ноутбуки планшеты и серверы например dallas lock такие средства защиты разделяют доступ к информации и подключаемым устройствам и опираются на список пользователей в котором указаны их права доступа для входа в систему. После включения компьютера вам нужно ввести логин, и пароль программные средства защиты проверяют действия пользователей и регистрируют каждое событие в журнале они контролируют целостность файловой системой и позволяют объединять защищенные компьютеры для централизованного управления безопасности если на вашем компьютере хранятся персональные данные или осуществляется доступ к государственным информационным системам вам потребуется двух факторная аутентификация в этих случаях дополнительных программным используют аппаратные средства управления доступом.

Электронные замки соболь аккорд или secret net информационные таблетки сенсор отпечатков пальцев usb ключи или usb токены, а также смарт-карты с универсальным считывателем например Джакарты и тест-драйв 3 последних способ удобен потому, что в одной смарт-карте может поместиться все электронный пропуск сотрудника электронная подпись зарплатная медицинская карты и так далее считыватель тест-драйв, 3 имеет нет соединяем и usb кабель с защиты от перегиба не я и перетирания и может быть представлен в без корпусного встраиваемом малогабаритном и вертикальном исполнении как начать работу со смарт-карты Джакарта ознакомьтесь с руководством пользователя и проверьте требования к системе подключите считыватели порту на современных операционных системах считыватель определиться самостоятельно после чего загорится зеленый индикатор вставьте смарт-карту контактами вверх и вперед в момент передачи данных зеленый индикатор будет мигать обеспечьте надежное хранение смарт-карты в случае ее потери сообщите в службу идти безопасности вашей компании

Также можно отметить, что одна из наиболее распространенных, разновидностей программных закладок — клавиатурные шпионы. Такие программные закладки нацелены на перехват паролей пользователей операционной системы, а также на определение их легальных полномочий и прав доступа к компьютерным ресурсам.

Фильтры позволяют увеличить надёжность за счёт всеми данными, которые пользователь операционной системы вводит с клавиатуры компьютера. Самые элементарные фильтры просто сбрасывают перехваченный клавиатурный ввод на жесткий диск или в какое-то другое место, к которому имеет доступ злоумышленник. Более изощренные программные закладки этого типа подвергают перехваченные данные анализу и отфильтровывают информацию, имеющую отношение к пользовательским паролям.

Фильтры являются резидентными программами, перехватывающими одно или несколько прерываний, которые связаны с обработкой сигналов от клавиатуры. Эти прерывания возвращают информацию о нажатой клавише и введенном символе, которая анализируется фильтрами на предмет выявления данных, имеющих отношение к паролю пользователя.

Из этого можно понять, что безопасность можно усиль или улучшить, но главной уязвимостью будет человек.