Цифровой Страж Key_P1 MultiClet для защиты данных

Key_P1 MultiClet - многофункциональное устройство для защиты информации на ПК и накопителях, разработанное на базе мультиклеточного процессора с универсальной не фон-неймановской архитектурой. Выполнено в виде миниатюрного блока с тремя разъёмами: USB – розетка и вилка, а также разъём для SD-карт. Количество инициируемых обычных флеш-накопителей не ограничено.

Функционал устройства

Иерархический доступ к информации	В Key_P1 MultiClet предусмотрено разграничение прав доступа к зашифрованным файлам. Служба безопасности предприятия будет иметь возможность создавать различные разграничения прав по отделам. При этом руководитель будет иметь доступ ко всем файлам. Сотрудники компании могут кодировать файлы для своих коллег с помощью программы Corporate Key_P1 Manager при наличии соответствующего уровня доступа.
Контроль персонала	Служба информационной безопасности предприятия может заблокировать возможность записи информации с корпоративных компьютеров на съемные накопители. Для этого устанавливается режим «только чтение» для того, чтобы Key_P1 заблокировал любую несанкционированную запись конфиденциальных данных, вирусов или других программ на накопитель на аппаратном уровне. Т.е. записать информацию на накопитель в этом режиме не получится, пользователю понадобиться получить разрешение службы информационной безопасности для возможности записи на накопители.
Защита от шпионских флешек (проблема badUSB)	Key_P1 разрешает подключение только обычных накопителей информации, работа «устройств-шпионов» (представляются одновременно клавиатурой и накопителем) будет заблокирована.
Запрет на отключение	Устройство Key_P1 сохраняет в «лог журнал» основные события, совершаемые пользователем. Просмотр «лог журнала» может быть закрыт для пользователя. Для разблокировки просмотра необходимо ввести ПИН-код администратора. Таким образом, работник не может незаметно изъять устройство Key_P1 для записи на флэш-накопитель корпоративных данных, так как все попытки отключения будут зафиксированы службой безопасности.
Сотрудник в командировке	Пользователи могут создать одинаковые ключи для обмена зашифрованными сообщениями друг с другом или головным офисом компании в случае обмена данными во время деловых поездок с помощью открытой электронной почты и других интернет-ресурсов.

Надежное шифрование	Шифрование информации возможно на накопителях и компьютере. Шифрование осуществляется по алгоритму ГОСТ 28147-89 с шириной ключа 256 бит для поставки на территории РФ, с шириной ключа 56 бит для поставки за пределы РФ. Шифрование алгоритмом ГОСТ28147-89 на накопителях осуществляется защищенным методом – по секторам (вскрытие потребует тысячи лет машинного времени).
Неуязвимость данных	Пользователь имеет возможность создания резервных копий зашифрованной информации, таким образом, при потере или повреждении устройства Key_P1 и/или накопителя пользователь сможет восстановить свою информацию. В случае потери устройство бесполезно для злоумышленника. Потерянное устройство Key P1 нельзя использовать ни в каких целях, связанных с шифрованием и дешифрованием. Из потерянного устройства нельзя извлечь информацию о принципах работы аналогичных устройств.
Поддержка разных накопителей	Устройство поддерживает работу с накопителями типа SD, micro SD и USB. Также существует возможность использования USB удлинителей, если размер посадочного USB порта на компьютере недостаточен.
Использование разных ОС	Поддерживается работа устройства в операционных системах WindowsXP, Windows 7, Windows 8, Linux 2.6.x, Linux 3.x и (в разработке) MacOS
Сейф для паролей	Устройство позволяет сохранять пользовательские пароли и логины на внутреннюю защищенную память устройства Key_P1. В дальнейшем пользователь может, кликнув мышкой, скопировать логин в буфер обмена операционной системы и вставить в нужное поле для ввода логина. Аналогичную операцию можно проделать для пароля. Этим мы обеспечиваем удобное использование и хранение своих паролей, а также защищаемся от кейлогеров на ПК.
Быстрое криптопреобразование	Устройство Key_P1 MultiClet позволяет провести быстрое шифрование или расшифрование информации. Таким образом пользователи могут легко и быстро обмениваться зашифрованными текстовыми сообщениями, которые пересылаются с помощью электронной почты, различных систем обмена сообщениями (например skype), социальных сетей и т.д.

Порядок работы с устройством

Для работы с устройством необходимо загрузить приложение **Key_P1 Manager**. Программное обеспечение поддерживает весь функционал устройства, обеспечивает инициализацию устройства, инициализацию накопителей, формирует корпоративные ключи и др.

Отличительные особенности программы

- не требует установки на операционную систему
- поддерживает ОС семейства Windows и Linux (и в разработке ОС Mac)
- для поддержки кроссплатформенной работы рекомендуется сохранить на открытый раздел накопителя версию программы для ОС Windows и Linux
- программа и устройство, не привязывается к конкретному ПК или накопителю, что позволяет обеспечить работу устройства на различных ПК и обеспечить поддержку неограниченного количества накопителей
- простой и удобный интерфейс, разграничение прав доступа к функционалу устройства (по ПИН коду для пользователя и администратора, который может быть от 4-х до 16-ти

символов)

Подключение и Инициализация	Для большей надежности работа с устройством осуществляется посредством виртуальной клавиатуры. Подключив Key_P1 MultiClet к USB порту своего ПК, Вы запустите установленное с нашего сайта ПО. Далее Вы сгенерируете набор ключей и введете пин-код для Key_P1 MultiClet. Вы сможете инициализировать для Key_P1 MultiClet неограниченное количество накопителей. В накопителе необходимо будет задать размер приватной области, где будут размещаться зашифрованные файлы, и она будет доступна в системе после ввода пин-кода на виртуальной клавиатуре. В результате инициализации накопителя будут сформированы открытый (для обычных файлов) и приватный (для закодированных файлов) разделы для работы с файлами.
Обмен информацией	Внутри отдела сотрудники могут обмениваться зашифрованной информацией, кодируя файлы через программу Key_P1 Manager при подключенном устройстве Key_P1 Multiclet на жёсткий диск персонального компьютера, ноутбука или на съёмный накопитель, или пересылая их через различные почтовые программы. Также предусмотрена возможность кодирования коротких текстовых сообщений для пересылки через различные мессенджеры, в т.ч. с мобильных устройств.
Разграничение доступа	В Key_P1 MultiClet предусмотрено разграничение прав доступа к зашифрованным файлам. Служба безопасности предприятия будет иметь возможность создавать различные разграничения прав по отделам. Например, отдел "Программисты" сможет шифровать файлы для отдела "Бухгалтерия", а отдел "Бухгалтерия" не сможет читать файлы отдела "Электронщики". При этом руководитель будет иметь доступ ко всем файлам. Сотрудники компании могут кодировать файлы для своих коллег с помощью программы Corporate Key_P1 Manager при наличии соответствующего уровня доступа.