Программа криптографической защиты информации (ПКЗИ) "Барьер"

Разработана ООО «Новые современные технологии»

Актуальность защиты коммерческой информации трудно переоценить. Самый простой и распространённый пример - уволился сотрудник, скопировал клиентскую базу и ушёл к конкурентам. По нашему опыту, убытки от таких действий составляют сотни тысяч, миллионы, а иногда и сотни миллионов рублей!!! Иногда данные потери невосполнимы, они влияют на престиж и финансовое благополучие компании. Годы разработок и миллионы вложенных средст вылетают в трубу при промышленном шпионаже или простой программе-шпионе просочившейся через брэндмауэр и антивирусную защиту вашего сервера! Китайские бытовые приборы уже сегодня оснащаются чипами внедряющимися в беспроводные сети (http://hi-tech.mail.ru/bytovaya/misc/iron-bugs.html). Не пора ли нам задуматься о сохранении наших данных, в век, когда информация становиться самым дорогим товаром?!

Программа криптографической защиты информации (ПКЗИ) "Барьер" позволит вашей компании избавиться от всех выше перечисленных проблем, а также от множества других рисков, связанных с утратой данных.

Использование программы криптографической защиты информации (ПКЗИ) "Барьер" решает следующие задачи:

1. Шифрование коммерческой информации (списки клиентов в "1С-бухгалтерии" или любой другой программе, проекты готовящихся договоров и коммерческих предложений, готовые инженерные и технологические решения, научные разработки, электронные сообщения (e-mail) Вашей компании, фотографии, аудио и видеофайлы). Это - упрощённый способ защиты информации, который, однако, позволяет получить хороший уровень безопасности Ваших данных. Нет необходимости в подключении к интернету. Используется шифрование 1-ой ступени, с криптографической надёжностью шифрования (время необходимое специалистам для дешифровки файла на современных компьютерах) около 6 месяцев.

2. Сохранение конфидециальности данных при внезапных проверках государственными органами ("маски-шоу"). В таких ситуациях достаточно одному из ваших сотрудников успеть нажать на иконку висящую в трее и вся информация, находящаяся в заранее подготовленном списке значимых файлов, будет зашифрована. Изъятие компьютеров или жёстких дисков госорганами не даст им доступ к защищённой информации! Это - стандартный способ защиты вашей информации, который гарантирует, что даже при аресте и изъятии ваших компьютеров, информация не окажется у ваших конкурентов (как часто бывает при таких, инициированных из вне, проверках). Нет необходимости в подключении к интернету. Используется шифрование 2-ой ступени, с криптографической надёжностью шифрования (время необходимое специалистам для дешифровки файла на современных компьютерах) около 5 лет. Шифрование 2-й ступени не декодируется программами 1-ой ступени шифрования, но может создавать кодированные файлы, воспринимаемые программами 1-ой ступени.

3. При высокой степени защиты информации все базы данных, и значимые файлы (индивидуальный список) изначально храняться в зашифрованном виде (как на рабочих дисках, так и на файлах резервного копирования), локальные копии данных при архитектуре клиент-сервер также шифруются. При этом, для рядового пользователя, процесс работы с привычными программами (Word, Exel, "1-С бухгалтерия") абсалютно не меняется. Декодирование скопированных данных возможно только при знании ключевой фразы и зарегистрированной на Вашу фирму копии программы декодирования (доступ в интернет обязателен). Ведутся логи запросов на копирование информации. Используется шифрование 3-ей ступени, с криптографической надёжностью шифрования (время необходимое специалистам для дешифровки файла на современных компьютерах) около 20 лет. Шифрование 3-й ступени не декодируется программами более низкой ступени шифрования, но может создавать кодированные файлы, воспринимаемые программами с более низкой ступенью шифрования.

4. При полной защите данных становится **невозможным их копирование на любые носители** в незашифрованном виде (хотя внешне процесс копирования никак не изменяется), а также идёт привязка данных к конкретному компьютеру (скопировав данные с сервера на работе вы не сможите расшифровать их на личном ноутбуке, даже если правильно укажите ключевую фразу и у Вас есть зарегистрированная копия программы). Любые запросы на копирование защищённой информации с сервера требуют ручного подтверждения и заносятся в лог-файлы, которые, в свою очередь, так же зашифрованны и не допускают ручной корректировки. Удалённый доступ к данным сервера или к виртуальному диску Вашей компании привязан к конкретному носителю или компьютеру (вход на ваш сервер без аттестованной флеш-карты или компьютера становится невозможен). Используется шифрование 3-ей ступени, с криптографической надёжностью шифрования (время необходимое специалистам для дешифровки файла на современных компьютерах) около 20 лет. В определённых случаях доступ в интернет обязателен (технология раздельного хранения), это обеспечивает дополнительную защиту Вашей информации, т. к. для дешифровки требуется часть кода хранящаяся на нашем сервере, при этом **мы не знаем** ни вашу ключевую фразу, ни зашифрованную с её помощью информацию. Клавиатурные шпионы в данном случае становятся бесполезны, поскольку часть информации для кодирования-декодирования находится на нашем сервере и остаётся недоступной для злоумышленников. По сути это - технология распознавания свой-чужой, успешно применяемая военными уже много лет.

В прилагаемом архиве находится демо-версия программы и инуструкции по установке и эксплуатации. Бесплатная версия программы предназначена для одного компьютера и рассчитана на 100 циклов шифровки-дешифровки или на 50 дней использования и требует выход в интернет на этапе идентификации. Она позволяет Вам создать шифрованную копию выбранного вами файла (например для конфиденциальной отправки по электронной почте), при этом сохраняя сам исходный файл, а также позволяет сформировать список файлов, которые необходимо зашифровать при внештатной ситуации, исходные файлы также сохраняются, их зашифрованные копии имеют расширение *.cdc и сохраняются в тех же дирректориях где и исходные файлы. Контроль свободного места для создания копий не ведётся, поэтому убедитесь, что на диске достаточно места для

создания копий шифруемых файлов (размеры зашифрованных файлов практически совпадают с размером исходных файлов)! Используется **полный** протокол шифрования 1-ой ступени. Криптографическая надёжность шифрования (время необходимое специалистам для дешифровки файла на современных компьютерах) около 6 месяцев.

С уважением, генеральный директор ООО «Новые современные технологии» Самсонов А. В.