

## Информационная безопасность, безопасная передача информации

### TrustPort Tools

Любая информация, передаваемая по каналам связи, может быть перехвачена — аксиома.

Рассмотрим вариант безопасной передачи информации. Для безопасной передачи информации используется шифрование. Обычному пользователю может показаться, что шифрование информации – сложный и долгий процесс. Это не так. Время, которое необходимо для шифрования документа, составляет доли секунды.

Есть масса всевозможного программного обеспечения, которое умеет шифровать информацию, но в данном случае (военные действия в Крыму, массированная информационная война) мы не можем использовать программное обеспечение недружественной страны. Программное обеспечение от Лаборатории Касперского и иных российских производителей использовать нельзя по понятным причинам - никто не может дать гарантию, что российское ПО не используется россиянами против нас.

Рассмотрим вариант использования специального программного обеспечения для шифрования от чешской компании [TrustPort](#). Программа [TrustPort Tools](#) способна шифровать: короткие сообщения, текст электронных писем, любые документы любого размера, разделы жёсткого диска компьютера.

Процесс шифрования программой [TrustPort Tools](#) может освоить даже школьник младших классов, шифрование обеспечивается синхронным методом с криптоустойчивым алгоритмом и ключом 256-бит. При шифровании документа пользователь должен ввести определённый код, этот же код необходимо будет использовать для расшифровки зашифрованного документа. Код для шифрования должен иметь размер не менее 8 знаков (рекомендуется) и быть сложным (цифры, буквы латинского алфавита различного регистра, специальные символы).

Откуда брать коды для шифрования? Коды для шифрования должны выдаваться службой безопасности для всех сотрудников, которые передают информацию по открытым каналам связи. Чем чаще меняются коды для шифрования, тем лучше. В идеале коды для шифрования должны меняться каждый день.

Важно понимать, что у разных сотрудников будет разный уровень доступа к информации. Некоторые сотрудники являются носителями особо важной информации. Таким сотрудникам для передачи информации друг другу необходимо выдавать уже два кода для шифрования – первый код для шифрования обычной информации и пересылки рядовым сотрудникам, а второй код для шифрования особо важной информации и пересылке её сотрудникам, которые имеют соответствующий доступ к особо важной информации. Такая организация ограничения доступа позволяет обеспечить более высокий уровень защиты от инсайдеров (шпионов).

При более сложной структуре организации возможно наличие не двух уровней доступа, а трёх и более. Каждая категория сотрудников будет иметь свой код для шифрования и коды для шифрования документов с более низким уровнем секретности.

*Пример.* В организации есть три вида документов с грифами: «особой важности», «совершенно секретно» и «секретно».

*В этом случае весь персонал делится на три категории, каждая из которых имеет доступ к «своей» группе документов и к документам с более низким уровнем секретности. Так персонал с доступом к документам «особой важности» (первая форма допуска) будет иметь доступ к своим документам и к документам «совершенно секретно» и «секретно». Такая категория служащих получает три кода для шифрования. Персонал с доступом к документам «совершенно секретно» (вторая форма допуска) будет иметь доступ к своим документам и к документам с грифом «секретно». Такая категория служащих получает два кода для шифрования. Персонал с доступом к документам «секретно» (третья форма допуска) будет иметь доступ только к своим документам. Такая категория служащих получает один код для шифрования. Персонал, который не работает с секретной информацией, коды для шифрования не получает.*

*Служащие с первой формой допуска получают три кода:*

- 1: (78w5Fl\*tc%64\_ - для особо важных документов*
- 2: 5/#RrQ<Oi-wes – для совершенно секретных документов*
- 3: L0)T\_Yn+\$3sAv-8 – для секретных документов*

*Служащие со второй формой допуска получают два кода:*

- 2: 5/#RrQ<Oi-wes – для совершенно секретных документов*
- 3: L0)T\_Yn+\$3sAv-8 – для секретных документов*

*Служащие с третьей формой допуска получают один код:*

- 3: L0)T\_Yn+\$3sAv-8 – для секретных документов*

*Все вышеуказанные коды приведены для примера...*

Мы рассмотрели «лёгкий» вариант с использованием программы с синхронным шифрованием, но есть и более мощная программа для шифрования с более «серьёзным» уровнем шифрования – [TrustPort eSign Pro](#) с асинхронным шифрованием.