КАК БЕЗОПАСНО ПЕРЕНЕСТИ **КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ НА СМЕННЫЕ НОСИТЕЛИ?**

Совместное решение компаний «Конфидент» и «Актив», сертифицированное ФСТЭК России на соответствие требованиям к средствам контроля съёмных машинных носителей информации уровня отчуждения (переноса) информации.

Сменные носители информации - это накопители информации, подключаемые к компьютеру, как правило, через USB-порт. Если на АРМ пользователя информационной системы имеется свободный USB-порт, то существует риск преднамеренной или непреднамеренной утечки информации. Пользователи переносят информацию на внешние носители информации для использования на других компьютерах организации, «берут работу на дом», делают резервные копии важных документов или баз данных. Утечка информации через сменные накопители грозит финансовыми и репутационными потерями.

ИСПОЛЬЗОВАНИЕ ВНЕШНИХ НАКОПИТЕЛЕЙ → **РИСКИ УТЕРИ/ХИЩЕНИЯ ИНФОРМАЦИИ** → **ФИНАНСОВЫЕ И РЕПУТАЦИОННЫЕ ПОТЕРИ**

Приказы ФСТЭК России № 17, № 21, №31 и №239

По требованиям законодательства РФ в сфере защиты информации:

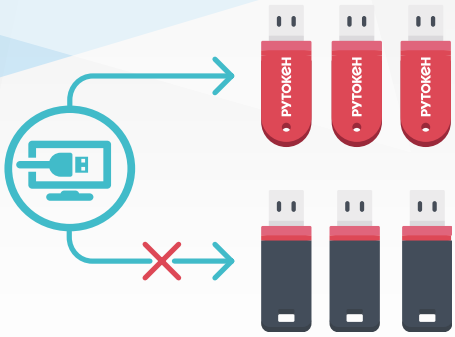
- оператором должно обеспечиваться исключение возможности несанкционированного ознакомления с содержанием (чтения) информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах («ЗНИ.4»);
- должен осуществляться контроль ввода (вывода) информации на машинные носители информации («ЗНИ.6»).

Для контроля переноса информации применяются DLP-системы и другие средства:

- DLP-системы. Достаточно сложны во внедрении и при настройке. Несмотря на богатую функциональность, возможны ложные срабатывания, из-за которых конфиденциальная информация бесконтрольно переносится на сменный накопитель. Нет легитимного способа записать конфиденциальную информацию на носители;
- сертифицированные СКН уровня подключения. Позволяют легитимно разграничивать доступ пользователей информационной системы к сменным накопителям, но не контролируют перенос информации;
- средства шифрования информации. Позволяют гарантированно исключить доступ к записанной на накопитель информации, однако в большинстве случаев не защищают от внутреннего нарушителя, так как пароль и ключ преобразования известны пользователю – они необходимы для шифрования информации.

Модуль СКН уровня отчуждения (переноса) информации в составе **СЗИ от НСД Dallas Lock 8.0** - совместное решение компаний **«Конфидент» и «Актив»**, сертифицированное **ФСТЭК России** на соответствие требованиям к средствам контроля съёмных машинных носителей информации уровня отчуждения (переноса) информации (Сертификат соответствия ФСТЭК России № 2720).

- сертифицирован по профилю защиты ИТ.СКН.Н4.ПЗ и позволяет легитимно переносить конфиденциальную информацию на идентификаторы Рутокен ЭЦП 2.0 Flash со встроенной энергонезависимой памятью. Данные идентификаторы могут быть использованы и для аутентификации пользователя в информационной системе. В основе подхода лежит «прозрачное» для пользователя преобразование информации при её чтении и записи на Рутокен ЭЦП 2.0 Flash. Пользователь даже не подозревает, что информация преобразуется «на лету»;



- ключи преобразования недоступны пользователю информационной системы, что закрывает проблему со внутренним нарушителем. Доступ к информации возможен только на определённых АРМ, разрешённых администратором информационной безопасности. Все прочие сменные накопители не могут быть использованы. Такой подход делает практически невозможной утечку информации через сменные накопители. Дополнительно на каждый накопитель возможно установить пароль пользователя. Злоумышленнику для доступа к информации необходимы: ключи преобразования, пароль пользователя, сам накопитель и СЗИ Dallas Lock 8.0. Такая задача гораздо сложнее, чем с обычными зашифрованными «флешками», когда достаточно договориться только с пользователем;

- Сервер безопасности Dallas Lock в рамках домена безопасности позволяет централизованно управлять ключами преобразования и разграничивать доступ пользователей к накопителям. Если в организации несколько администраторов ИБ, то существует отдельная роль по централизованному управлению накопителями для разграничения доступа привилегированных пользователей к настройкам системы защиты. Есть возможность организовать доступ к информации из разных доверенных доменов безопасности. Это удобно, когда у организации имеются филиалы и удалённые объекты с собственными вычислительными сетями.

DALLAS LOCK + РУТОКЕН

СЕРТИФИЦИРОВАННОЕ РЕШЕНИЕ

Основные сценарии использования:

- легитимный перенос конфиденциальной информации между АРМ, не состоящими в защищённой вычислительной сети, в том числе между территориально разнесёнными подразделениями;
- создание резервных копий документов с конфиденциальной информацией или резервных копий критичных баз данных, например, содержащих персональные данные.

УДОБНОЕ ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Бесплатное тестирование ПО, дополнительная информация, заказ продукта:

- Коммерческий департамент ЦЗИ ООО «Конфидент»: isc@confident.ru
- Отдел продаж компании «Актив»: sales@rutoken.ru