

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ НА КОММЕРЧЕСКИХ ПРЕДПРИЯТИЯХ: КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА И ИХ ПРИМЕНЕНИЕ

Ибраева Анна Павловна

студент, Российский университет транспорта, РФ, г. Москва

Аннотация. В статье рассмотрены способы применения криптографических и программно-аппаратных средств защиты информации на коммерческих предприятиях.

Ключевые слова: информационная безопасность, средства криптографической защиты информации (СКЗИ), криптопровайдер, электронно-цифровая подпись (ЭЦП).

Деятельность любого предприятия в той или иной степени связана с обработкой, хранением и передачей информации, разглашение которой способно привести к значительным экономическим потерям, в том числе и к краху фирмы. Существуют различные средства для обеспечения информационной безопасности (ИБ), они представлены на рисунке 1.

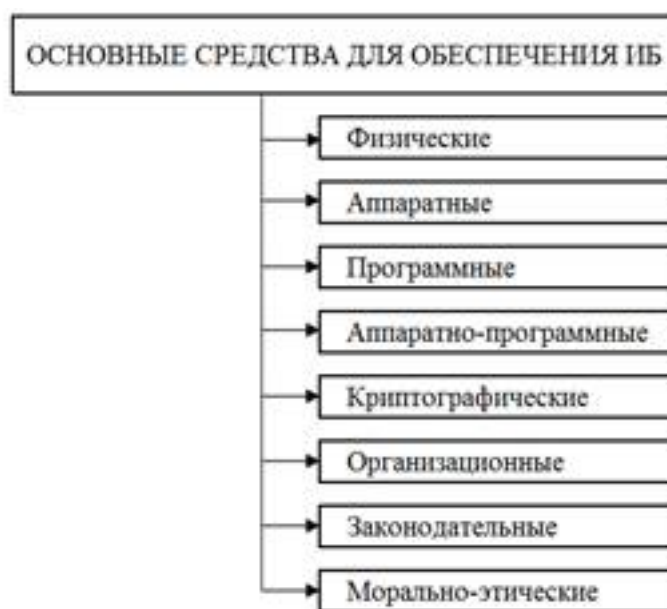


Рисунок 1. Основные средства обеспечения ИБ

В сетях ЭВМ наиболее эффективными являются криптографические способы защиты информации. Если физические способы защиты могут быть преодолены путем, например, дистанционного наблюдения, подключения к сети или подкупа персонала, правовые не всегда сдерживают злоумышленника, а управление доступом не гарантирует от проникновения

изошренных «хакеров», то криптографические методы, если они удовлетворяют соответствующим требованиям, характеризуются наибольшей надежностью. [1. С.29]

Под современной системой криптографической защиты информации (СКЗИ) понимают программно-аппаратный компьютерный комплекс, который обеспечивает защиту информации по следующим параметрам:

1. Конфиденциальность – отсутствие возможности прочесть информацию лицам, не имеющим соответствующих прав доступа. Основным элементом обеспечения конфиденциальности является ключ, который состоит из уникальной комбинации букв и чисел, необходимой для доступа пользователя в определенный информационный блок.
2. Целостность – невозможность редактирования и удаления информации, а также иных несанкционированных изменений.
3. Аутентификация – проверка и подтверждение подлинности информации, отправителей и получателей.
4. Авторство – свидетельство факта совершенных пользователями действий. Наиболее популярным в наше время способом подтверждения подлинности является электронная цифровая подпись (ЭЦП).

В настоящее время к средствам криптографической защиты информации (СКЗИ) причисляют следующие (рисунок 2):

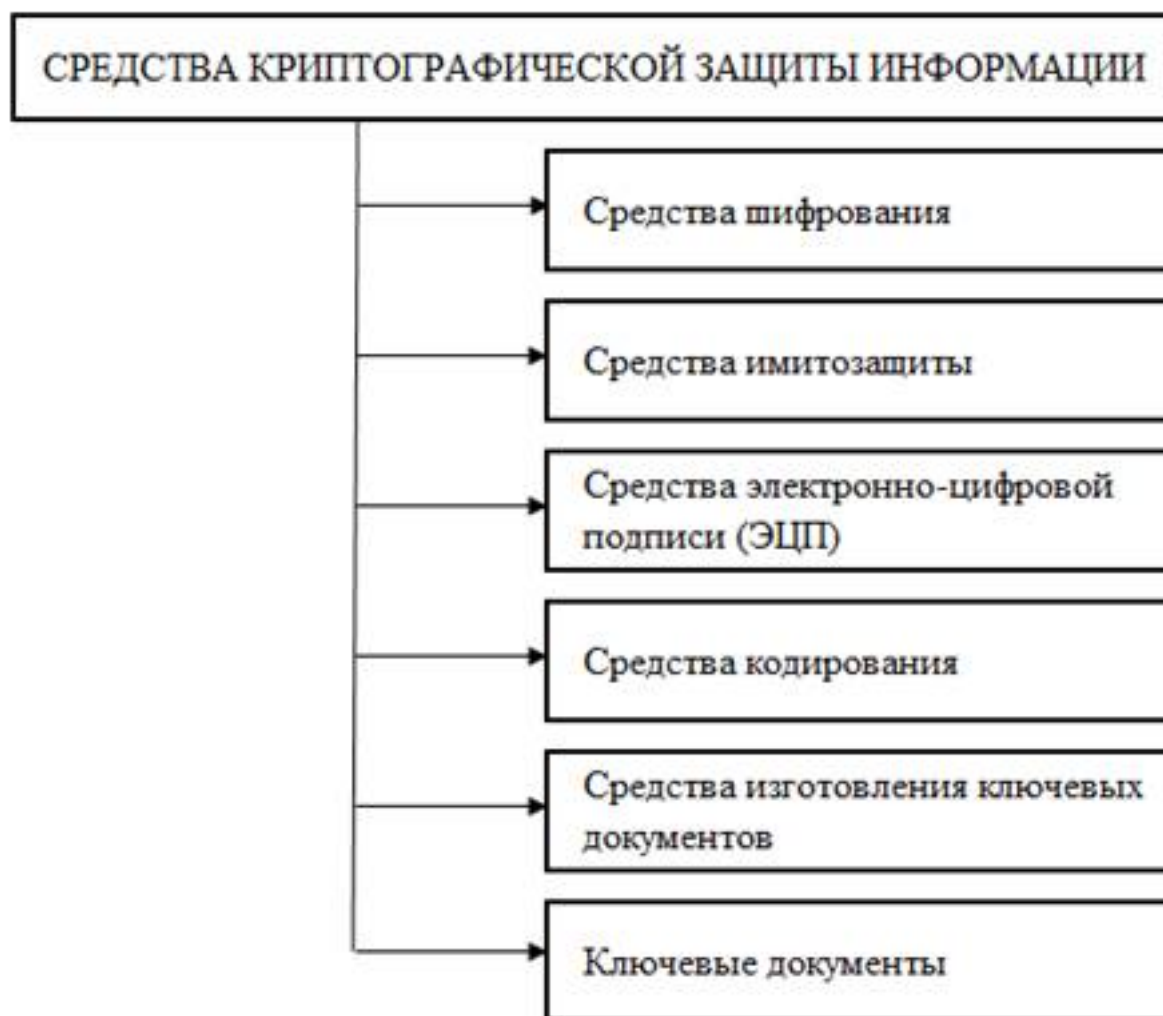


Рисунок 2. Современные средства криптографической защиты информации

Сегодня шифрование и СКЗИ особенно популярны в российских компаниях и организациях в таких направлениях, как:

- защита персональных данных клиентов и сотрудников;
- защита конфиденциальной информации компании;
- шифрование информации, пересылаемой посредством почтовых клиентов или корпоративной почты;
- создание и применение в рабочих процессах цифровых подписей.

Применение криптографии и СКЗИ в российских компаниях

1. Внедрение криптосредств в системы защиты персональных данных.

В наше время законодательство РФ выдвигает все больше и больше требований к обработке и хранению различных категорий персональных данных. Деятельность любой компании невозможна без постоянной доработки и совершенствования процедур, направленных на соблюдение этих требований:

- криптографическое средство должно штатно функционировать совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к нему требований; [2, С.89]
- для обеспечения безопасности персональных данных при их обработке должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства.

Криптографические средства можно классифицировать в зависимости от уровня защиты, который они обеспечивают. Такая классификация представлена на рисунке 3.

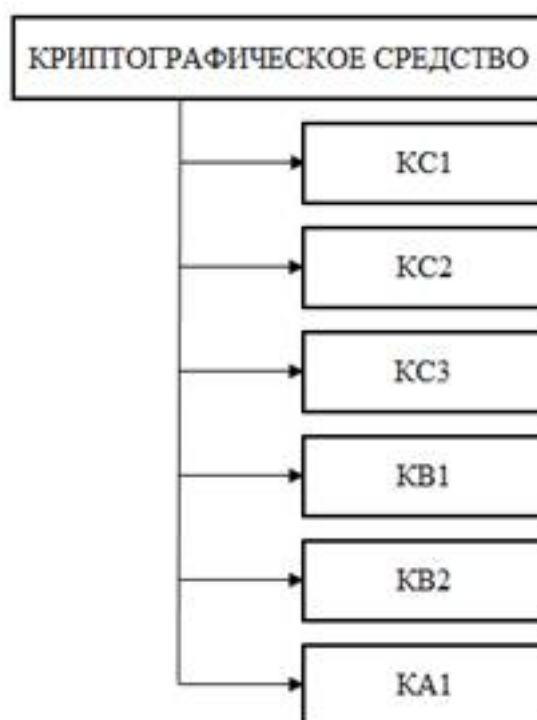


Рисунок 3. Классификация криптографических средств в зависимости от обеспечиваемого им уровня защиты

Внедрение криптосредства того или иного класса в систему защиты обуславливается категорией нарушителя (субъекта атаки), которая определяется оператором в модели угроз.

2. Защита корпоративной информации.

Как мы уже выяснили, законодательство РФ имеет большое влияние в сфере применения СКЗИ для защиты персональных данных. Если говорить про защиту корпоративной информации, то первым заинтересованным лицом здесь будет само руководство компании. Функции программ шифрования изображены на рисунке 4.



Рисунок 4 . Основные функции программы для шифрования в корпоративной среде

Средство шифрования, поддерживающее вышеперечисленные возможности, способно обеспечить достаточно надежную защиту, однако непременно должно использоваться как составляющая комплексного подхода к защите информации.

Составляющие комплексного подхода представлены на рисунке 5.



Рисунок 5. Комплексный подход к защите информации

3. Электронная подпись

Электронная подпись (ЭП) сегодня является полноценным аналогом собственноручной подписи и может быть использована юридическими и физическими лицами для того, чтобы обеспечить документу в цифровом формате юридическую силу. Применение ЭП в электронных системах документооборота значительно увеличивает скорость заключения коммерческих сделок, уменьшает объем бумажных бухгалтерских документов, экономит время сотрудников. [1, С.115]

4. Шифрование электронной почты

Для большинства компаний электронная почта является основным средством коммуникации между сотрудниками. Ни для кого не секрет, что по корпоративной электронной почте сегодня пересылается огромное количество конфиденциальной информации: договора, счета, сведения о продуктах и ценовых политиках компании, финансовые показатели, поэтому защита корпоративной почты - крайне важная составляющая в обеспечении информационной безопасности компании, реализация которой становится возможной также благодаря использованию криптографии и средств шифрования. Большинство почтовых клиентов, таких как Outlook, Thunderbird, The Bat! позволяют настроить обмен зашифрованными сообщениями на основе сертификатов открытого и закрытого создаваемых при помощи средств криптографической защиты. [4]

Таким образом, можно сделать вывод, что защита информации на коммерческих предприятиях является многогранным процессом, осуществляемым благодаря различным средствам обеспечения безопасности. Наиболее надежным методом защиты в сетях ЭВМ является применение криптографических средств. Применение СКЗИ для защиты персональных данных обусловлено как требованиями законодательства Российской Федерации, так и высокой эффективностью данных средств.

Список литературы:

1. Гатченко Н.А, Исаев А.С, Яковлев А.Д, «Криптографическая защита информации» - СПб: НИУ ИТМО, 2012. - 142 с.

2. Криптографическая защита информации : учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с
3. Положение об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденное Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.
4. Официальный сайт КriptoПРО – Режим доступа: <https://www.cryptopro.ru>