Введение в информационную безопасность

14.12.2012

Основные определения

Защищаемой информацией называют информацию, являющуюся предметом собственности и подлежащую защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации.

Ценность информации является критерием при принятии любого решения о ее защите и для выбора метода защиты. В денежном выражении затраты на защиту информации не должны превышать возможные потери.

Основные определения

Принято следующее разделение информации по уровню важности:

– *жизненно важная, незаменимая информация*, наличие которой необходимо для функционирования организации;

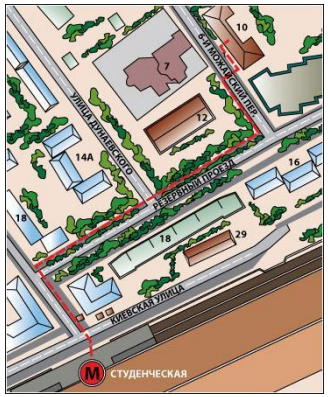
– *важная информация* – информация, которая может быть заменена или восстановлена, но процесс восстановления очень труден и связан с большими затратами, в том числе косвенными;

– *полезная информация* – информация, которую трудно восстановить, однако организация может эффективно функционировать некоторое время и без нее;

– *несущественная информация* – информация, которая не имеет значения для организации.

Основные определения

Уровень секретности – это административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов. Такой информацией может быть государственная, военная, коммерческая, служебная или личная тайна.



Основные угрозы информационной безопасности

- Деятельность человека, непосредственно и опосредовано влияющая на информационную безопасность и являющаяся основным источником угроз.
- Отказы и неисправности средств информатизации.
- Стихийные бедствия и катастрофы.

Внешние угрозы информационной безопасности

Внешние угрозы исходят от природных явлений, катастроф, а также от субъектов, не входящих в состав пользователей и обслуживающего персонала системы, разработчиков системы, и не имеющих непосредственного контакта с информационными системами и ресурсами.

Источники внешних угроз:

- недружественная политика сторонних лиц и организаций в области распространения информации и новых информационных технологий;
- преступные действия групп, формирований и отдельных лиц, направленные против экономических интересов организации;
- стихийные бедствия и катастрофы.

Внутренние угрозы информационной безопасности

Внутренние угрозы исходят от пользователей и обслуживающего персонала системы, разработчиков системы, других субъектов, вовлеченных в информационные процессы и имеющих непосредственный контакт с информационными системами и ресурсами, как допущенных, так и не допущенных к конфиденциальным сведениям.

Источники внутренних угроз:

- противозаконная деятельность сотрудников, отделов и служб в области формирования, распространения и использования информации;
- нарушения установленных регламентов сбора, обработки и передачи информации;
- преднамеренные действия и непреднамеренные ошибки персонала информационных систем;
- отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах.

Информационные способы нарушения информационной безопасности

- противозаконный сбор, распространение и использование информации
- манипулирование информацией (дезинформация, сокрытие или искажение информации)
- незаконное копирование, уничтожение данных и программ
- хищение информации из баз и банков данных;
- нарушение адресности и оперативности информационного обмена
- нарушение технологии обработки данных и информационного обмена

Программно-математические способы нарушения информационной безопасности

- внедрение вредоносных (в том числе самовоспроизводящихся) программ

- внедрение программных закладок на стадии проектирования или эксплуатации системы и приводящих к компрометации системы защиты информации

Физические способы нарушения информационной безопасности

- уничтожение, хищение и разрушение средств обработки и защиты информации, средств связи, целенаправленное внесение в них неисправностей
- уничтожение, хищение и разрушение машинных или других оригиналов носителей информации
- хищение ключей средств криптографической защиты информации, программных или аппаратных ключей средств защиты информации от несанкционированного доступа
- воздействие на обслуживающий персонал и пользователей системы с целью создания благоприятных условий для реализации угроз информационной безопасности
- диверсионные действия по отношению к объектам информационной безопасности

Радиоэлектронные способы нарушения информационной безопасности

- перехват информации в технических каналах ее утечки;
- перехват и дешифрование информации в сетях передачи данных и линиях связи
- внедрение электронных устройств перехвата информации в технические средства и помещения
- навязывание ложной информации по сетям передачи данных и линиям связи
- радиоэлектронное подавление линий связи и систем управления с использованием одноразовых и многоразовых генераторов различных видов электромагнитной энергии

Организационно-правовые способы нарушения информационной безопасности

- закупка несовершенных, устаревших или неперспективных средств информатизации и информационных технологий
- невыполнение требований законодательства и задержки в разработке и принятии необходимых нормативных правовых и технических документов в области информационной безопасности

Результаты реализации угроз информационной безопасности

- нарушение секретности (конфиденциальности) информации (разглашение, утрата, хищение, утечка и перехват и т.д.)
- нарушение целостности информации (уничтожение, искажение, подделка и т.д.)
- нарушение доступности информации и работоспособности информационных систем (блокирование данных и информационных систем, разрушение элементов информационных систем, компрометация системы защиты информации и т.д.)

Классификация уровней нарушителя информационной безопасности

1-ый уровень – внешний нарушитель (группа внешних нарушителей), самостоятельно осуществляющий создание методов и средств реализации угроз, а также реализующий угрозы (атаки)

2-ой уровень – внутренний нарушитель, не являющийся пользователем информационных систем (группа нарушителей, среди которых есть по крайней мере один указанный выше внутренний нарушитель), самостоятельно осуществляющий создание методов и средств реализации угроз, а также реализующий угрозы (атаки)

3-ий уровень – внутренний нарушитель, являющийся пользователем информационных систем (группа нарушителей, среди которых есть по крайней мере один указанный выше внутренний нарушитель), самостоятельно осуществляющий создание методов и средств реализации угроз, а также реализующий угрозы (атаки)

Классификация уровней нарушителя информационной безопасности

4-ый уровень – группа нарушителей (среди которых есть внутренние, являющиеся пользователями информационных систем), осуществляющая создание методов и средств реализации угроз, а также реализующая их с привлечением отдельных специалистов, имеющих опыт разработки и анализа средств защиты информации, используемых в информационных системах таможенных органов

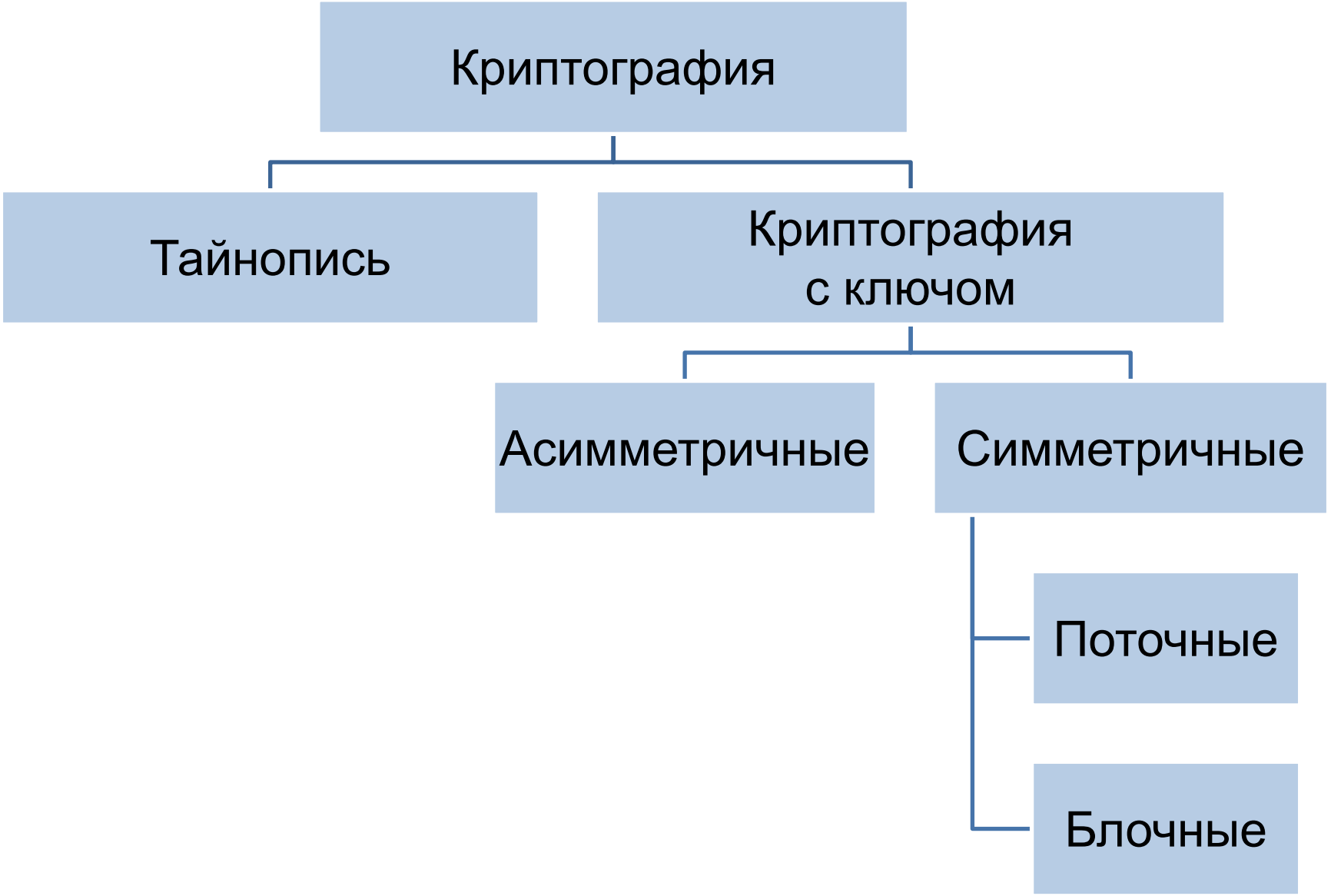
5-ый уровень – группа нарушителей (среди которых есть внутренние, являющиеся пользователями информационных систем), осуществляющая создание методов и средств реализации атак, а также реализующая атаки с привлечением научно- исследовательских центров, специализирующихся в области разработки и анализа средств защиты информации (включая специалистов в области использования для реализации угроз (атак) недокументированных средств прикладного программного обеспечения)

Классификация средств защиты данных

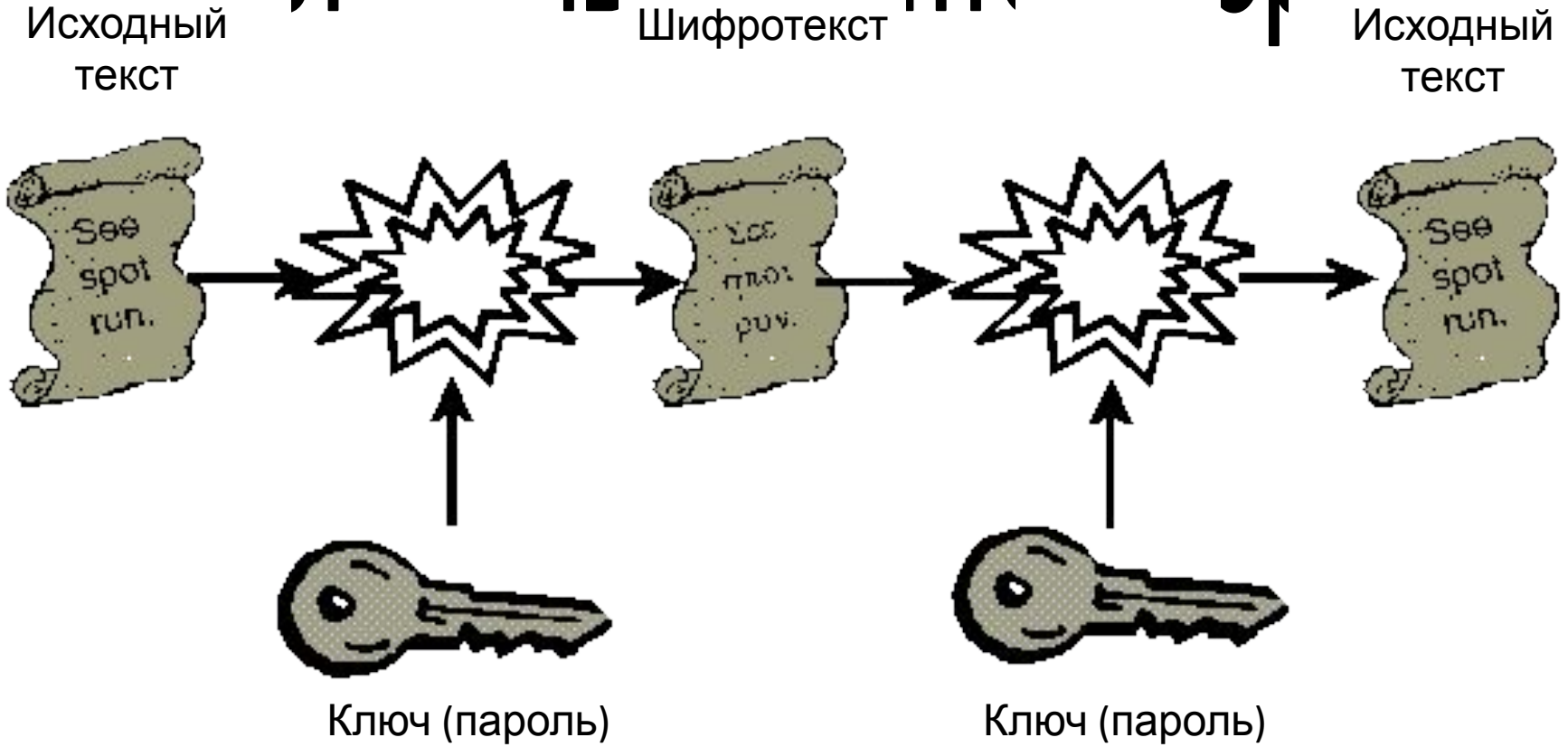
Способы аутентификации пользователя

Пароль «Мама мыла раму!»

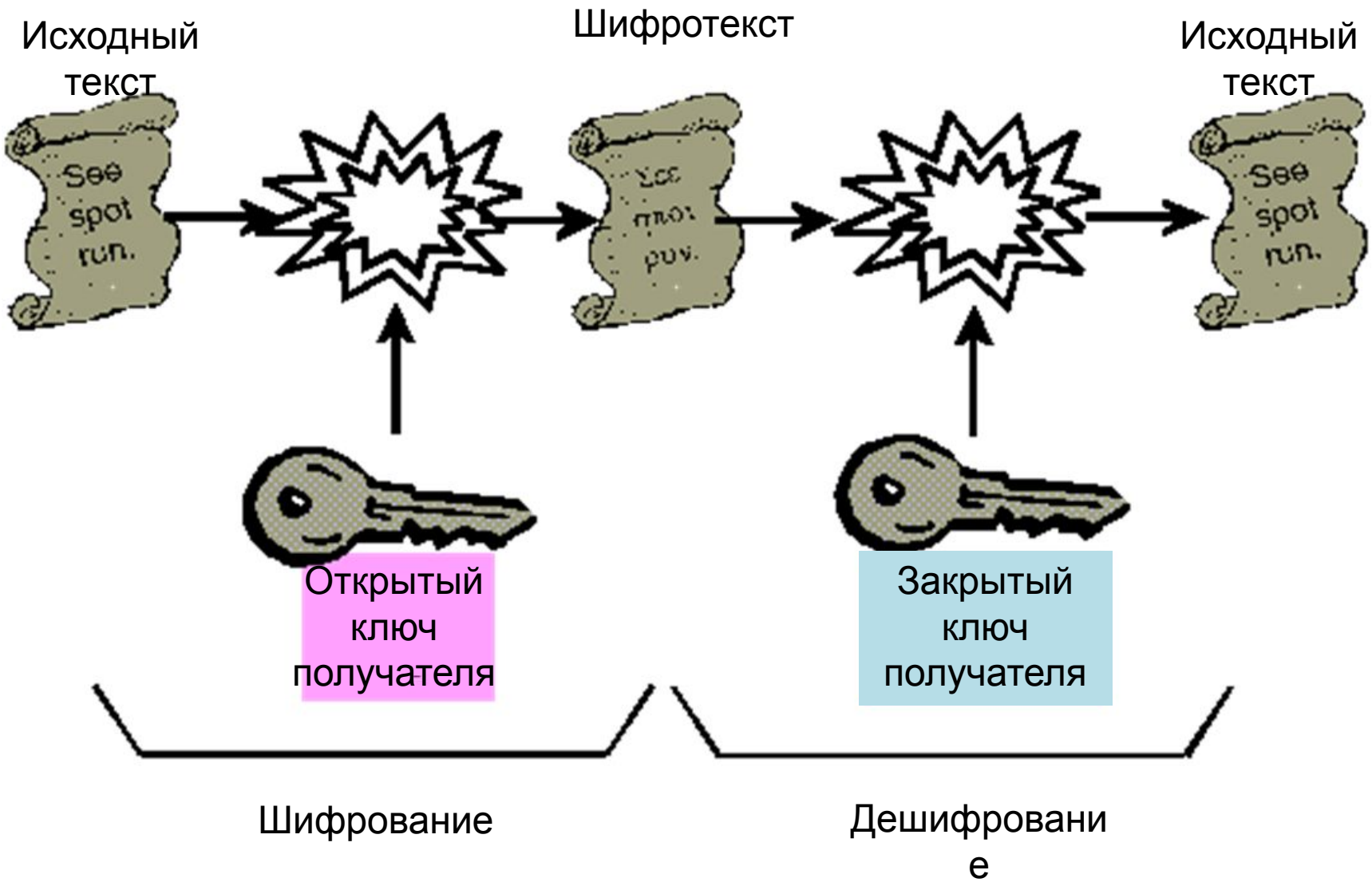
Криптографические средства защиты



Симметричные криптоалгоритмы



Асимметричные криптоалгоритмы

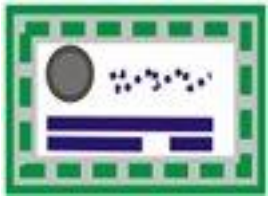


Компоненты необходимые для работы с электронной цифровой подписью

Ключевая пара - связанные между собой открытый и закрытый ключ. С помощью закрытого ключа производится подписание документов этот ключ является секретным, доступ к нему должен быть только у владельца ключа. Открытый ключ доступен для всех, с помощью открытого ключа происходит идентификация владельца ЭЦП, т.е. подтверждается владелец электронной цифровой подписи, которой подписан документ. Также открытый ключ используется для шифрования документов.

Ключевой носитель для хранения ключевой пары электронной цифровой подписи – закрытого ключа и открытого ключа. Как правило, это похожий внешне на флэш-диск носитель

Компоненты необходимые для работы с электронной цифровой подписью



Сертификат открытого ключа подписи.
Сертификаты выпускает уполномоченный удостоверяющий центр (УЦ).
Сертификат подтверждает данные о владельце ЭЦП и его полномочия

Криптопровайдер СКЗИ КриптоПро CSP - программа, предназначенная для формирования и проверки электронной цифровой подписи в соответствии с отечественными стандартами; а также для обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования

Хеширование

Бесконечная область определения

Конечная область значений

Свойства хеш-функции

Изменение 1 бита на входе меняет около половины бит выхода

Необратимость