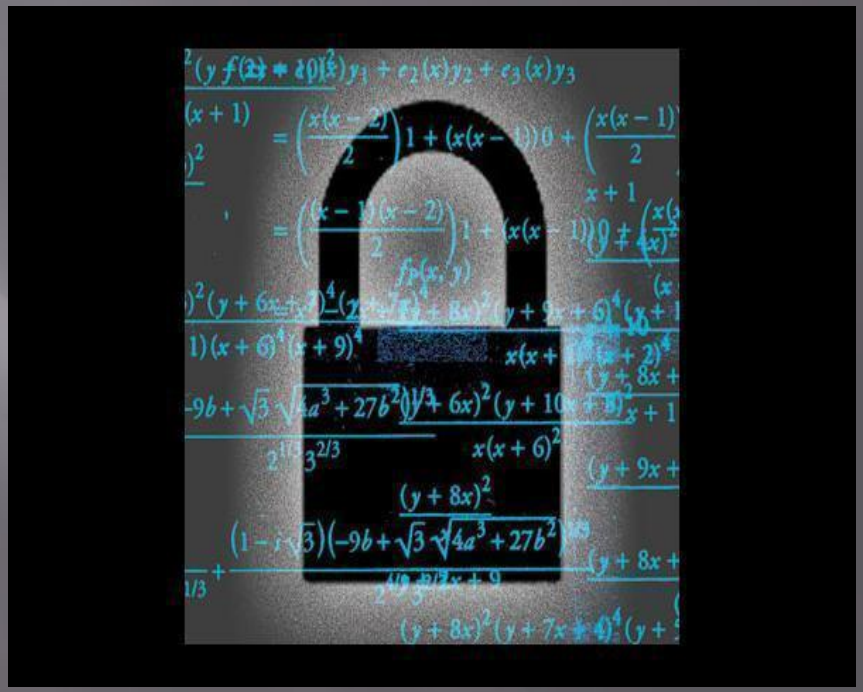
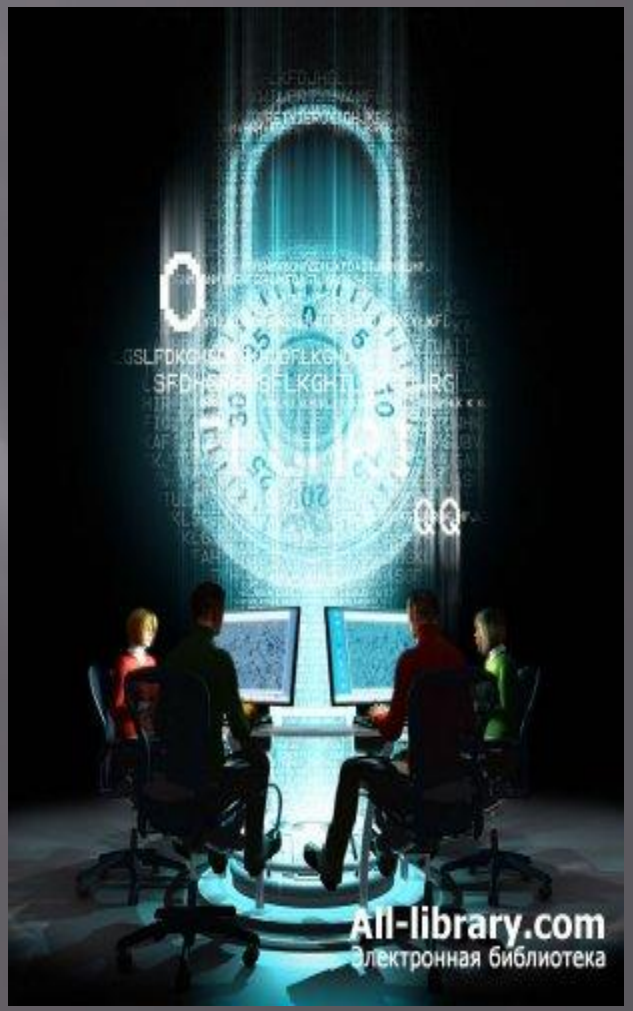
Крипотографические методы защиты

- Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии - ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней индии тому примеры.
- Криптографическое закрытия является специфическим способом защиты информации, оно имеет многовековую историю развития и применения. Поэтому у специалистов не возникало сомнений в том, что эт средства могут эффективно использоваться также и для защиты информации в АСОД, вследствие чего им уделялось и продолжает уделяться большое внимание. Достаточно сказать, что в США еще в 1978 году утвержден и рекомендован для широкого применения национальный стандарт криптографического закрытия информации. Подобный стандарт в 1989 году (ГОСТ 28147-89) утвержден и у нас в стране. Интенсивно ведутся исследования с целью разработки высокостойких и гибких методов криптографического закрытия информации. Более того, сформировалось самостоятельное научное направление - криптология, изучающая и разрабатывающая научно-методологические основы, способы, методы и средства криптографического преобразования информации.



История криптографии

- История криптографии насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии возможно использовать технологические характеристики используемых методов шифрования.
- Первый период (приблизительно с 3-го тысячелетия до н. э.) характеризуется господством моноалфавитных шифров (основной принцип — замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами). Второй период (хронологические рамки — с IX века на Ближнем Востоке (Ал-Кинди) и с XV века в Европе (Леон Баттиста Альберти) — до начала XX века) ознаменовался введением в обиход полиалфавитных шифров. Третий период (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.
- Четвёртый период — с середины до 70-х годов XX века — период перехода к математической криптографии. В работе Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам — линейному и дифференциальному криптоанализу. Однако до 1975 года криптография оставалась «классической», или же, более корректно, криптографией с секретным ключом.
- Современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления — криптография с открытым ключом. Её появление знаменуется не только новыми техническими возможностями, но и сравнительно широким распространением криптографии для использования частными лицами. Правовое регулирование использования криптографии частными лицами в разных странах сильно различается — от разрешения до полного запрета.
- Современная криптография образует отдельное научное направление на стыке математики и информатики — работы в этой области публикуются в научных журналах, организуются регулярные конференции. Практическое применение криптографии стало неотъемлемой частью жизни современного общества — её используют в таких отраслях как электронная коммерция, электронный документооборот (включая цифровые подписи), телекоммуникации и других.

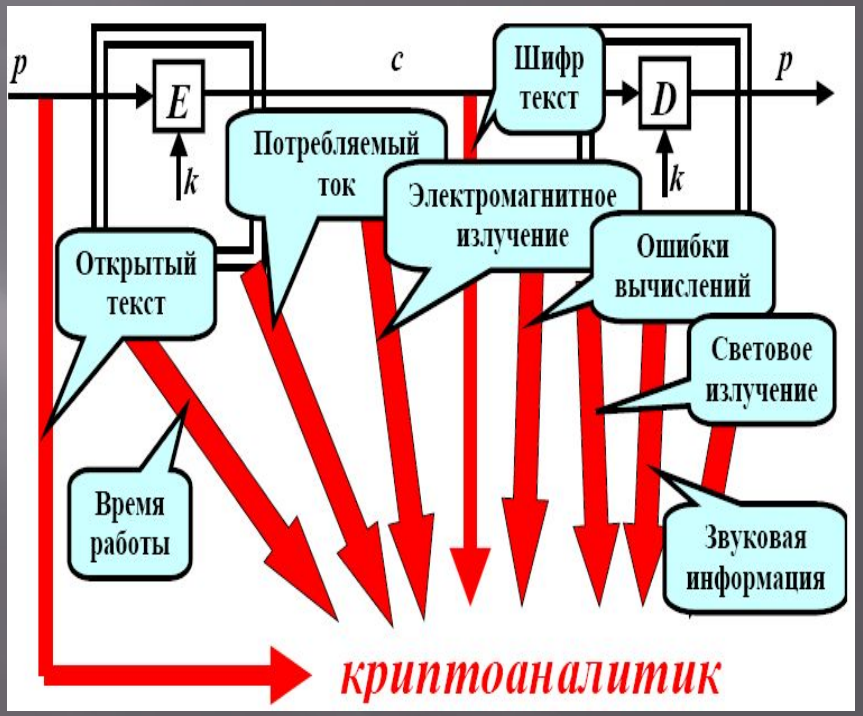


Криптография с симметричным ключом

- Симметри́чные криптосисте́мы (также симметричное шифрование, симметричные шифры) — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Криптоанализ

- Криптоанализ (от др.-греч. κρυπτός — скрытый и анализ) — наука о методах расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа.
- Термин был введён американским криптографом Уильямом Ф. Фридманом в 1920 году. Неформально криптоанализ называют также взломом шифра.
- В большинстве случаев под криптоанализом понимается выяснение ключа; криптоанализ включает также методы выявления уязвимости криптографических алгоритмов или протоколов.
- Первоначально методы криптоанализа основывались на лингвистических закономерностях естественного текста и реализовывались с использованием только карандаша и бумаги. Со временем в криптоанализе нарастает роль чисто математических методов, для реализации которых используются специализированные криптоаналитические компьютеры.
- Попытку раскрытия конкретного шифра с применением методов криптоанализа называют криптографической атакой на этот шифр. Криптографическую атаку, в ходе которой раскрыть шифр удалось, называют взломом или вскрытием.



Криптографический протокол

- Криптографический протокол (англ. Cryptographic protocol) — это абстрактный или конкретный протокол, включающий набор криптографических алгоритмов. В основе протокола лежит набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах.

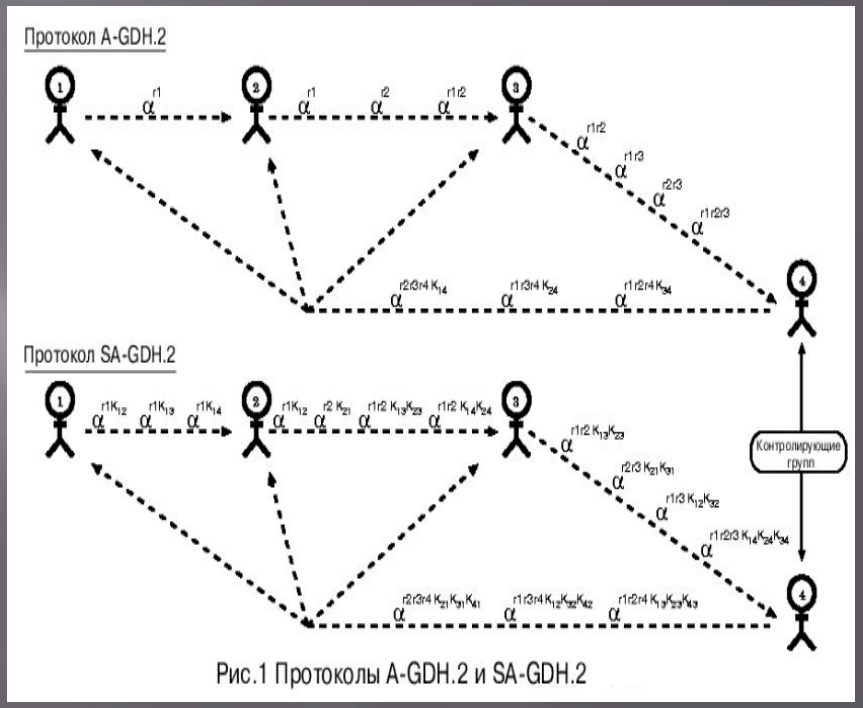
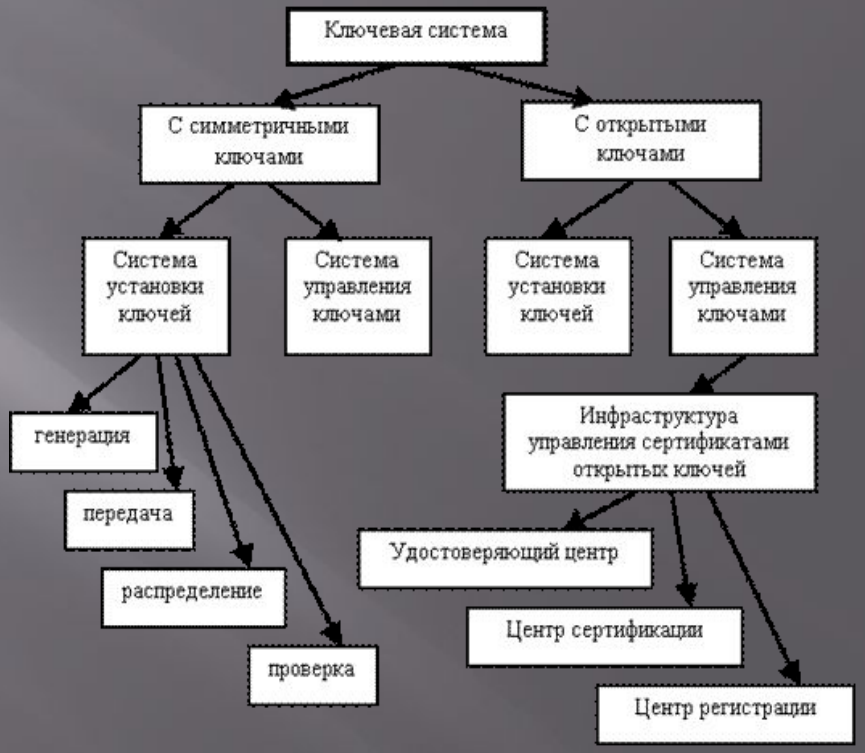


Рис.1 Протоколы A-GDH.2 и SA-GDH.2

Управление ключами

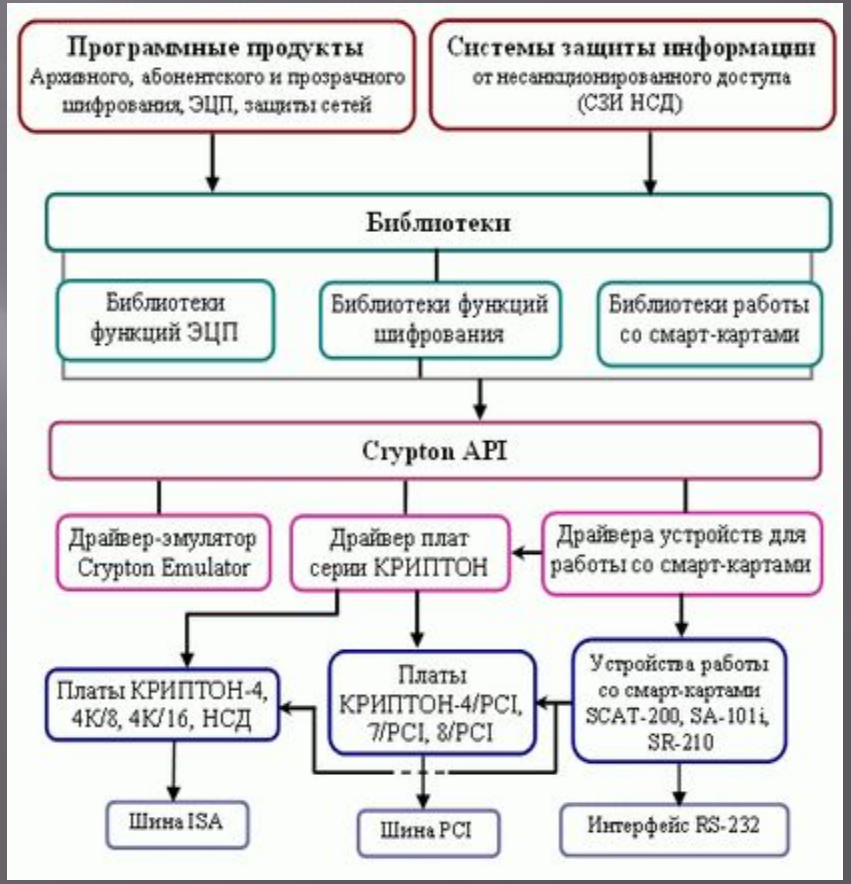
- Управление ключами состоит из процедур, обеспечивающих:
- включение пользователей в систему;
- выработку, распределение и введение в аппаратуру ключей;
- контроль использования ключей;
- смену и уничтожение ключей;
- архивирование, хранение и восстановление ключей.

- Управление ключами играет важнейшую роль в криптографии как основа для обеспечения конфиденциальности обмена информацией, идентификации и целостности данных. Важным свойством хорошо спроектированной системы управления ключами является сведение сложных проблем обеспечения безопасности многочисленных ключей к проблеме обеспечения безопасности нескольких ключей, которая может быть относительно просто решена путем обеспечения их физической изоляции в выделенных помещениях и защищенном от проникновения оборудовании. В случае использования ключей для обеспечения безопасности хранимой информации субъектом может быть единственный пользователь, который осуществляет работу с данными в последовательные промежутки времени. Управление ключами в сетях связи включает, по крайней мере, двух субъектов — отправителя и получателя сообщения.



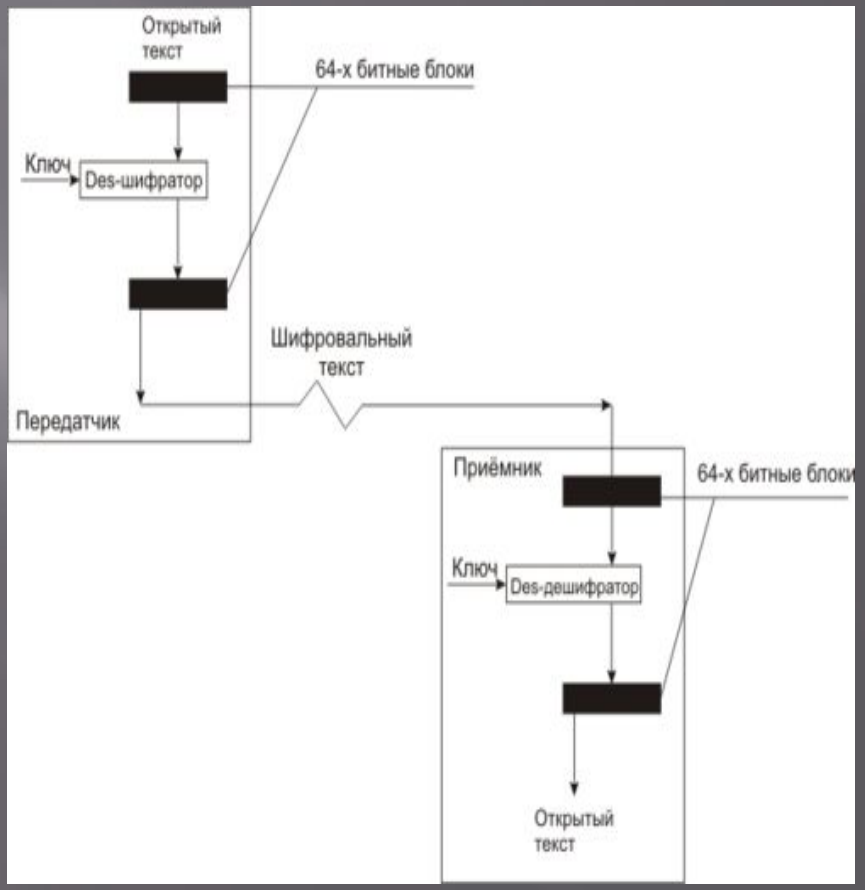
Криптографические примитивы

- Построение криптостойких систем может быть осуществлено путём многократного применения относительно простых криптографических преобразований (примитивов). В качестве таких примитивов Клод Шеннон предложил использовать подстановки (substitution) и перестановки (permutation). Схемы, реализующие эти преобразования, называются SP-сетями. Часто используемыми криптографическими примитивами являются также преобразования типа циклический сдвиг или гаммирование.



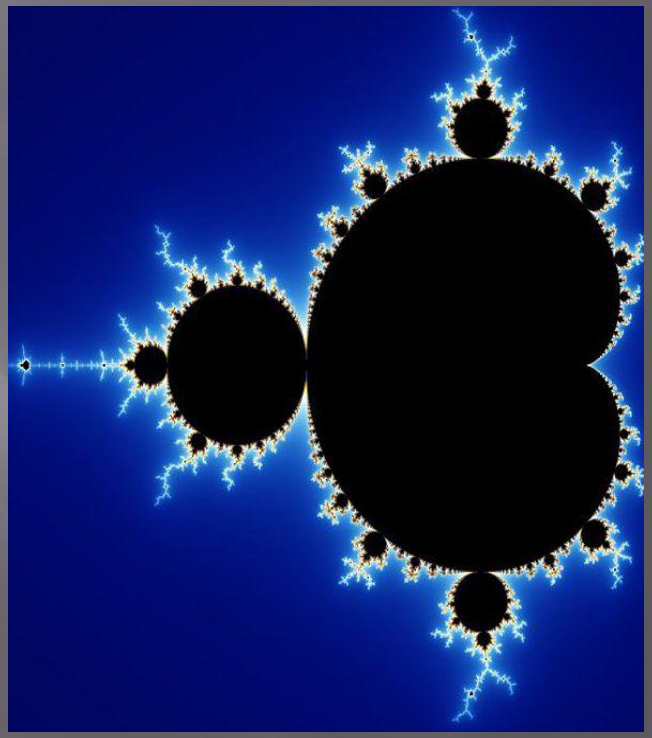
Криптосистема с открытым ключом

- Криптографическая система с открытым ключом (или Асимметричное шифрование, Асимметричный шифр) — система шифрования и/или электронной цифровой подписи (ЭЦП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭЦП и для шифрования сообщения. Для генерации ЭЦП и для расшифровки сообщения используется секретный ключ.[1] Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH. Также используется в PGP, S/MIME.



Криптоанархизм

- Криптоанархизм — философия, которая призывает к использованию сильной криптографии на основе публичных ключей для защиты приватности и индивидуальной свободы.
- Термин впервые появился в журнале «Тайм» за март 1994 г[1].
- Криптоанархисты создают виртуальные сообщества. Каждый участник сообщества остаётся анонимным до тех пор, пока сам не пожелает себя раскрыть.
- Совершенствование методов слежки и расширение интернет-коммуникаций открывает огромные возможности для компьютерной слежки за людьми. Криптоанархисты считают, что защитой от этого явления может быть разработка и использование криптографии. Они и шифрпанки (англ. Cypherpunk) считают, что законы математики сильнее человеческих законов, и поэтому криптоанархизм бессмертен.



Управление цифровыми правами

- Технические средства защиты авторских прав (ТСЗАП; англ. DRM — Digital rights management, неофициально иногда Digital restrictions management) — программные или программно-аппаратные средства, которые затрудняют создание копий защищаемых произведений (распространяемых в электронной форме), либо позволяют отследить создание таких копий.
- Хотя DRM призваны воспрепятствовать лишь неправомерному копированию произведений, как правило, они не допускают, либо ограничивают любое копирование, в том числе добросовестное, поскольку пока невозможно техническими средствами автоматически отличить «законное» копирование от «незаконного». Такое ограничение возможностей пользователя вызывает критику DRM со стороны правозащитников.
- Обычно средства DRM сопровождают защищаемые произведения (файлы, диски), а также встраиваются в средства воспроизведения (программы-оболочки для просмотра, карманные цифровые плееры, DVD-проигрыватели) и записи (DVD-рекордеры, Video Capture cards).
- В отличие от защиты от копирования, под DRM подразумеваются более общий класс технологий, которые могут позволять ограниченное копирование, а также могут налагать другие ограничения, такие как ограничение срока, в течение которого возможен просмотр или воспроизведение защищаемого произведения. При этом под DRM понимаются именно технические средства защиты, в то время как защита от копирования может включать также организационные, юридические и другие меры.