Криптографические протоколы, используемые в сети Интернет

Содержание

1. Понятие криптографического протокола
2. Функции криптографических протоколов
3. Классификация
4. Типы протоколов
5. Криптографические протоколы интернета
6. Свойства, характеризующие безопасность протоколов
7. Перечень наиболее широко известных атак
8. на криптографические протоколы
9. Требования к безопасности протокола

Понятие криптографического протокола

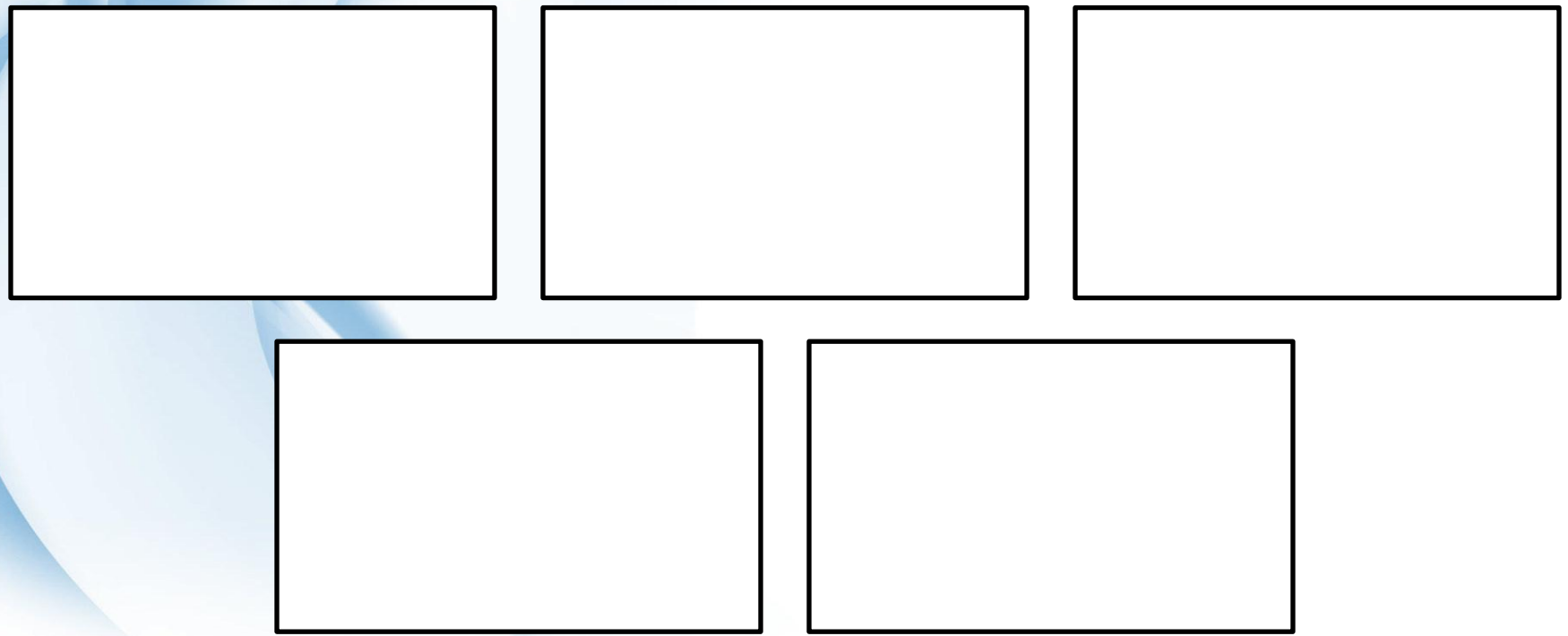
- В основе протокола лежит набор правил
- регламентирующих использование криптографических преобразований
- и алгоритмов в информационных процессах.

- Протокол, обеспечивающий поддержку хотя бы одной из функций-сервисов безопасности, называется защищённым протоколом обеспечения безопасности (security protocol).
- Защитные механизмы либо дополняют, либо встраиваются в коммуникационный протокол.

Функции криптографических протоколов

- Аутентификация источника данных
- Аутентификация сторон
- Конфиденциальность данных
- Невозможность отказа
- Невозможность отказа с доказательством получения
- Невозможность отказа с доказательством источника
- Целостность данных
- Обеспечение целостности соединения без восстановления
- Обеспечение целостности соединения с восстановлением
- Разграничение доступа

Классификация



Групповые протоколы

Групповые протоколы предполагают одновременное участие групп участников, например:

- протокол разделения секрета — если все группы, имеющие на это право, формируют одинаковые ключи;
- протокол телеконференции — если у различных групп должны быть разные ключи;
- протокол групповой подписи — предполагается одновременное участие заранее определенной группы участников, причем в случае отсутствия хотя бы одного участника из группы формирование подписи невозможно.

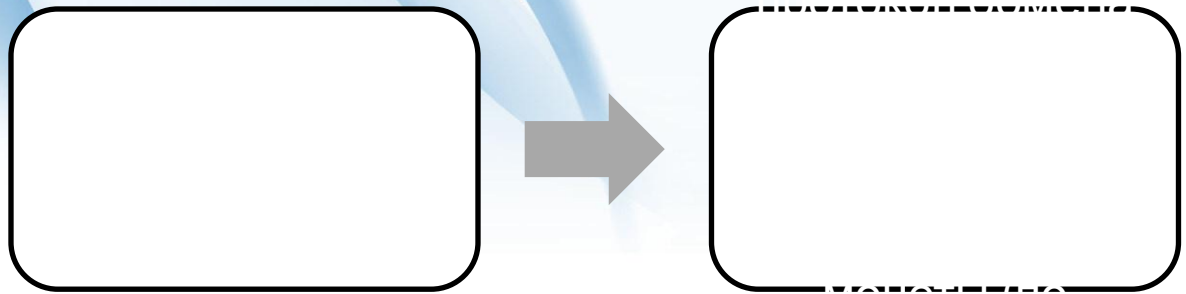
Рис. 1. Классификация криптографических протоколов

Типы протоколов

Таблица 1 - Типы протоколов

Тип протокола	*Краткая характеристика*
по практическому применению	
примитивные	Не имеют самостоятельного применения. Используются как своеобразные «строительные блоки» при разработке прикладных протоколов.
прикладные	Решает конкретную прикладную задачу, которая возникает (или может возникнуть) на практике.
по наличию третьей стороны	
с посредником	Посредник участвует в протоколе и помогает его исполнить двум сторонам. Стороны могут не доверять друг другу, но они полностью доверяют посреднику.
с арбитром	Посредник вступает в протокол только в исключительных случаях - когда между сторонами возникают разногласия.
самодостаточные	Посредник отсутствует - честность сторон гарантируется самим протоколом.

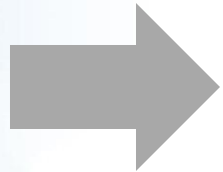
Примитивный криптографический протокол



Прикладной криптографический протокол

Прикладной

криптографических систем.



Такие протоколы, как Ipsec являются большими семействами различных протоколов, включающими много разных вариантов для различных ситуаций и условий применения.

Примерами прикладных протоколов являются:

- Система электронного обмена данными;
- Система электронных платежей;
- Система электронной коммерции;
- Поддержка правовых отношений;
- Игровые протоколы.

Криптографические протоколы интернета

Первой областью применения криптографии в Интернете стала электронная почта.

В ней работали два

OpenPGP.

Netscape изобрела SSL

- Netscape изобрела SSL (Secure Sockets Layer – протокол, гарантирующий безопасную передачу данных по сети; комбинирует криптографическую систему с открытым ключом и блочным шифрованием данных) на заре существования Веб, когда люди захотели заниматься безопасной электронной торговлей при помощи своих браузеров.
- SSL существовал в нескольких воплощениях (он был полем боя во время войны браузеров Netscape и Microsoft и в итоге был назван TLS (Transport Layer Security)).
- Эти протоколы встроены в браузеры и позволяют людям зашифровать секретную информацию, посылаемую на различные веб-сайты.

- Более новые криптографические протоколы разработаны для защиты пакетов IP.
- Среди них Microsoft Point-to-Point Tunneling Protocol (PPTP, у которого есть грубые дефекты), Layer Two Tunneling Protocol (L2TP) и IPsec (он существенно лучше, хотя и слишком сложен). IKE (Internet Key Exchange) – это, как видно из названия, протокол обмена ключами.
- Сегодня эти протоколы используются преимущественно для того, чтобы обеспечить работу виртуальных частных сетей (VPN). Тем не менее протоколы безопасности Интернета «умеют» намного больше, чем протоколы VPN.
- У них есть возможность обеспечивать безопасность большей части трафика. Со временем, может быть, эта возможность реализуется.

Существуют также и другие интернет-протоколы.

- SET – разработанный компаниями Visa и MasterCard для защиты операций с кредитными картами во Всемирной паутине.
- Протокол SSH (Secure Shell – защитная оболочка) используется для шифрования и идентификации команд для удаленных соединений.
- Другие протоколы имеют дело с сертификатами открытых ключей и инфраструктурой сертификатов: PKIX, SPKI и им подобные. Microsoft использует свои протоколы для защиты Windows NT.

Свойства, характеризующие безопасность протоколов

- Криптографическая система может обеспечивать различные функции безопасности, для реализации которых применяются разнообразные криптографические протоколы.
- Свойств, характеризующих безопасность криптографического протокола, также достаточно много.
- Обычно свойства протоколов, характеризующие их стойкость к различным атакам, формулируют как цели (goals) или требования к протоколам. Трактовка этих целей со временем меняется и уточняется.
- Наиболее полное и современное толкование этих целей дается в документах международной организации IETF.
- Под свойствами (целями, требованиями) безопасности в документах IETF в настоящее время понимаются следующие 20 целей, сгруппированные в 10 групп.

Таблица 2 - Свойства безопасности протоколов

№	Код	Название
1	G1 G2 G3	Аутентификация субъекта Аутентификация сообщения Защита от повтора
2	G4 G5	Неявная (скрытая) аутентификация получателя Аутентификация источника
3	G6	Авторизация (доверенной третьей стороной)

Таблица 2 - Свойства безопасности протоколов (продолжение)

№	Код	Название
4	G7 G8 G9 G10 G11	Аутентификация ключа Подтверждение правильности ключа Защищенность от чтения назад Формирование новых ключей Защищенная возможность договориться о параметрах безопасности
5	G12	Конфиденциальность
6	G13 G14	Обеспечение анонимности при прослушивании (несвязываемость) Обеспечение анонимности при работе с другими участниками

Таблица 2 - Свойства безопасности протоколов (продолжение)

№	Код	Название
7	G15	Ограниченная защищенность от атак типа отказ в обслуживании
8	G16	Неизменность отправителя
9	G17 G18 G19	Подотчетность Доказательство отправки Доказательство получения
10	G20	Безопасное временное свойство

(G1) Аутентификация субъекта

- Проверка с подтверждением подлинности одной из сторон наличия или полномочий (посредством представленных доказательств и/или документов) идентичности второй стороны, участвующей в выполнении протокола, а также того, что она действительно принимает участие в выполнении текущего сеанса протокола.
- Обычно она осуществляется посредством набора данных, который мог быть сгенерирован только вторым участником (как отклик на запрос, например).
- Обычно аутентификация субъекта предполагает, что некоторые данные могут быть безошибочно возвращены некоторому субъекту, что предполагает аутентификацию источника данных (Data Origin Authentication).

(G2) Аутентификация сообщения

- Обеспечение аутентификации источника данных и целостности передаваемого сообщения.
- Аутентификация источника данных (Data Origin Authentication) означает, что протокол должен обеспечивать средства гарантии того, что полученное сообщение или часть данных были созданы некоторым участником в некоторый момент времени, предшествующий получению сообщения, и что эти данные не были искажены или подделаны, но без предоставления гарантий однозначности и своевременности.
- Поскольку уверенность в том, что данные были созданы некоторым участником, без гарантии того, что они не были модифицированы, не представляет практического интереса, то обычно полагают, что требование аутентификации сообщения влечет требование его целостности.

(G3) Защита от повтора

- Гарантирование одним участником того, что аутентифицированное сообщение не является старым.
- В зависимости от контекста, это может иметь разный смысл:
- — сообщение было сгенерировано в данном сеансе протокола;
  — сообщение было сгенерировано в течение известного промежутка времени;
- — сообщение не было принято ранее.

(G5) Аутентификация источника

- законные группы участников должны быть способны аутентифицировать источник и содержание информации или групповой коммуникации.
- Это относится к случаям, когда группы участников не доверяют друг другу

(G7) Аутентификация ключа

- Это свойство предполагает, что один из участников получает подтверждение того, что никакой другой участник, кроме заранее определенного второго участника (и, возможно, других доверенных участников), не может получить доступа ни к одному секретному ключу.

(G8) Подтверждение правильности ключа

- Один из участников получает подтверждение того, что второй участник (возможно, неопределенный) действительно обладает конкретным секретным ключом (либо имеет доступ ко всем ключевым материалам, необходимым для его вычисления).

G9) Защищенность от чтения назад

- Протокол обладает этим свойством, если компрометация долговременных ключей не приводит к компрометации старых сеансовых ключей.

(G12) Конфиденциальность

- Свойство, состоящее в том, что специфический набор данных (обычно посылаемый или полученный как часть «защищенного» сообщения, а также сформированный на основе данных, полученных в результате обмена) не станет доступным или раскрытым для неавторизованных субъектов или процессов, а останется неизвестным противнику

Таблица 3 - Примеры свойств безопасности, характеризующих протоколы

Протокол \ Цель G	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
EAP-IKEv2	×	×	×			×	×			×					×
EKE	×	×										×			
IKE	×	×	×				×		×	×	×		×	×	×
IKEv2	×	×	×				×		×	×	×				×
DHCP-IPSec-tunnel	×	×										×			
kerberos	×	×	×			×	×			×					
SSH	×	×	×				×			×	×				
TLS	×	×	×				×			×	×		×		
TLS-v1.1	×	×	×				×			×	×		×		
TLS-SRP	×	×	×				×			×	×		×		
tls-sharedkeys	×	×	×				×			×	×		×		
SET	×	×	×										×		

Перечень наиболее широко известных атак на криптографические протоколы

- ***1. Подмена (impersonation)*** — попытка подменить одного пользователя другим. Нарушитель, выступая от имени одной из сторон и полностью имитируя ее действия, получает в ответ сообщения определенного формата, необходимые для подделки отдельных шагов протокола.

Методы противодействия состоят в:

- — сохранении в тайне от противника информации, определяющей алгоритм идентификации;
- — использование различных форматов сообщений, передаваемых на разных шагах протокола;
- — вставка в них специальных идентификационных меток и номеров сообщений.

- В протоколах с использованием третьей стороны возможны атаки, основанные на подмене доверенного сервера.
- Например, одна из сторон, имеющая доверительные отношения с сервером, выступает от его имени, подменяет его трафик обмена с другими сторонами и в результате получает возможность раскрывать значения генерируемых центром ключей.
- Эта атака может быть успешной для протоколов, в которых аутентификация при доступе к серверу основана только на идентификаторах сторон и случайных числах, генерируемых при каждом взаимодействии.
- Для защиты от таких атак применяют средства привязки ключей не к одной, а к обеим взаимодействующим сторонам путем передачи обоих идентификаторов в зашифрованном виде.

- ***2. Повторное навязывание сообщения (replay attack)*** — повторное использование ранее переданного в текущем или предыдущем сеансе сообщения или какой-либо его части в текущем сеансе протокола. Например, повторная передача информации ранее проведенного протокола идентификации может привести к повторной успешной идентификации того же самого или другого пользователя.
- В протоколах передачи ключей данная атака часто применяется для повторного навязывания уже использованного ранее сеансового ключа — атака на основе новизны.
- Методы противодействия состоят в обеспечении целостности сеанса и невозможности вставки в него лишних сообщений.

Для этого используется:

- — техника типа «запрос — ответ»;
- — вставка в передаваемые сообщения временных меток, случайных чисел или возрастающих последовательностей чисел.

- 3. Еще один тип подобных атак связан с обратной передачей адресату ранее переданных им сообщений и получил название атака отражением (reflection attack).
- Часто атаки данного типа относят к классу атак с повторным навязыванием сообщения.
- Для защиты от таких атак протоколы специально делают несимметричными, включая в зашифрованные сообщения идентификаторы сторон либо изменяя процедуры так, чтобы стороны должны были выполнять разные действия, вводят в протокол идентификационную информацию, используют различные ключи для приема и передачи сообщений.

- ***4. Задержка передачи сообщения (forced delay)*** — перехват противником сообщения и навязывание его в более поздний момент времени. Это также разновидность атаки с повторным навязыванием сообщения. Методы противодействия включают использование случайных чисел совместно с ограничением временного промежутка для ответа, использование временных меток.
- ***5. Комбинированная атака (interleaving attack)*** — подмена или другой метод обмана, использующий комбинацию данных из ранее выполненных протоколов, в том числе протоколов, ранее навязанных противником. Метод противодействия состоит в обеспечении целостности сеансов протоколов и отдельных сообщений.

- 6. Атака с использованием специально подобранных текстов — атака на протоколы типа «запрос — ответ», при которой противник по определенному правилу выбирает запросы с целью получить информацию о долговременном ключе доказывающего.
- Эта атака может включать специально подобранные — открытые тексты, если доказывающий должен подписать или зашифровать запрос, — шифрованные тексты, если доказывающий должен расшифровать запрос.
- Методы противодействия этой атаке состоят: во включении случайных чисел в запросы или ответы, а также — в использовании протоколов с нулевым разглашением.

- 7. Использование противником своих средств в качестве части телекоммуникационной структуры — атака, при которой в протоколе идентификации между A и B противник входит в телекоммуникационный канал и становится его частью при реализации протокола между A и B.
- При этом противник может подменить информацию, передаваемую между A и B. Эта атака особенно опасна в случае формирования участниками A и B общего ключа по протоколу Диффи — Хеллмана.
- Она известна как «противник в середине» и заключается в полной подмене всех сообщений между сторонами.

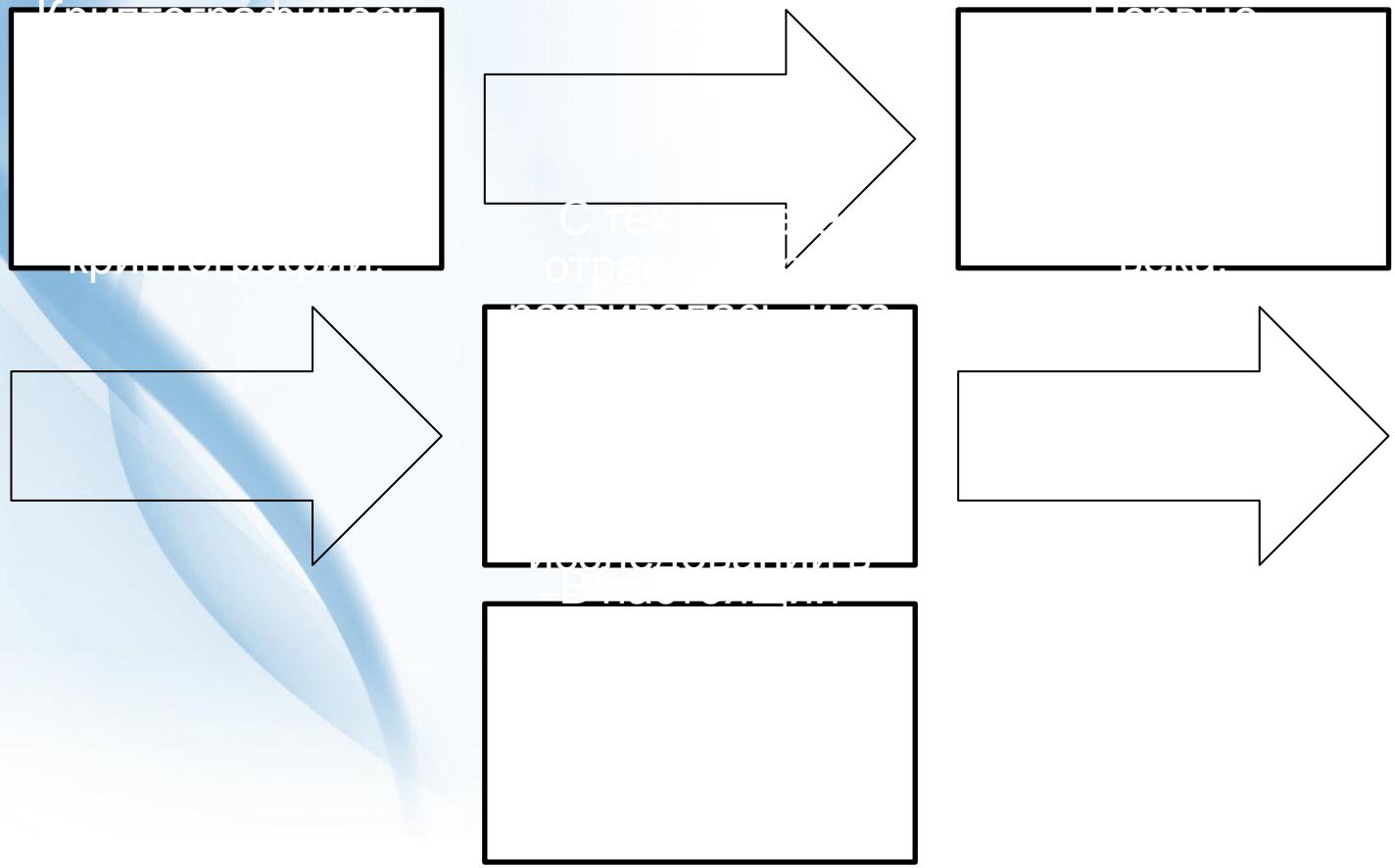
Требования к безопасности протокола

1. Аутентификация (нешироковещательная):
   - аутентификация субъекта
   - аутентификация сообщения
   - защита от повтора
2. Аутентификация при рассылке по многим адресам или при подключении к службе подписки/уведомления:
   - неявная (скрытая) аутентификация получателя
   - аутентификация источника
3. Авторизация (доверенной третьей стороной)
4. Свойства совместной генерации ключа:
   - аутентификация ключа
   - подтверждение правильности ключа
   - защищенность от чтения назад
   - формирование новых ключей
   - защищенная возможность договориться о параметрах безопасности
5. Конфиденциальность

Требования к безопасности протокола

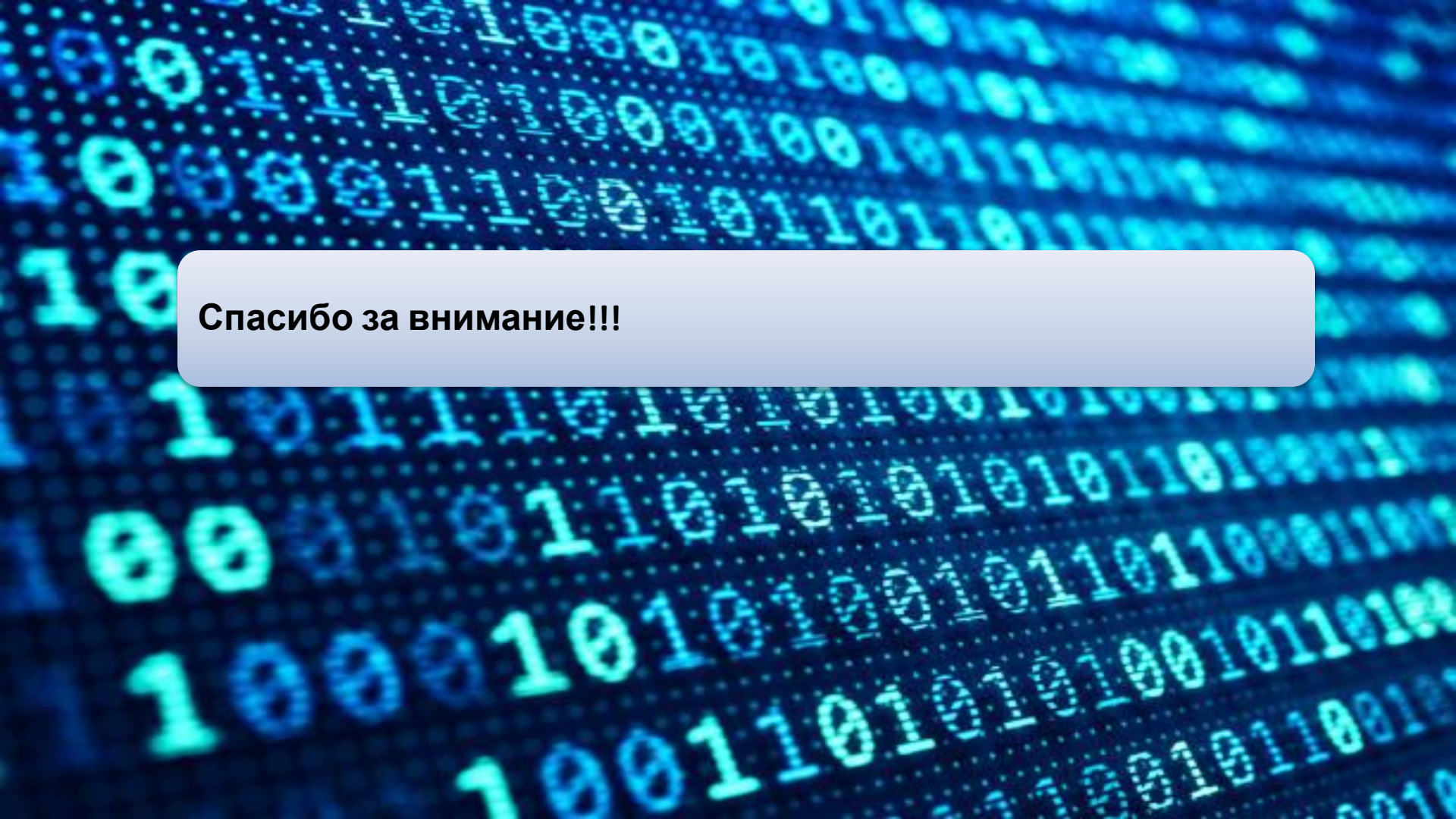
6. Анонимность:
   - защита идентификаторов от прослушивания (несвязываемость)
   - защита идентификаторов от других участников
7. Ограниченная защищенность от атак типа «отказ в обслуживании»
8. Инвариантность отправителя
9. Невозможность отказа от ранее совершенных действий:
   - подотчётность
   - доказательство источника
   - доказательство получателя
10. Безопасное временное свойство

Вывод



Список литературы и источников

1. Здор, С. Е. Кодированная информация. От первых природных кодов до искусственного интеллекта / С.Е. Здор. - М.: Либроком, 2012. - 168 с.
2. Литвинская О. С. Основы теории передачи информации. Учебное пособие / О.С. Литвинская, Н.И. Чернышев. - М.: КноРус, 2015. - 168 с.
3. Лапонина О. Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия / О.Р. Лапонина. - Москва: Высшая школа, 2013. - 536 с.
4. https://cyberleninka.ru/article/n/kriptograficheskie-protokoly-osnovnye-svoystva-i-uyazvimosti/viewer
5. https://r3al.ru/bezopasnost/kriptograficheskie_protokoly_inte.htm


Спасибо за внимание!!!