**КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ ЗАЩИТЫ ИНФОРМАЦИИ В РАДИОКАНАЛАХ СЕТЕВЫХ СПУТНИКОВЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ АСИММЕТРИЧНЫХ АЛГОРИТМОВ**

**ЦЕЛЬ:** рассмотреть способ защиты информации на космических связях с использованием асимметричных алгоритмов

**Задачи:**

1. Рассмотреть варианты угроз безопасности информации
2. Выделить преимущества использования ассиметричных криптосистем
3. Изучить способ построения асимметричных криптоалгоритмов

Развитие сетевых спутниковых технологий управления и передачи информации приводит к значительному возрастанию информационных потоков в радиоканалах. Информация, циркулирующая по радиоканалам управления и информационного обмена, может иметь критическое значение для пользователя, т. е. раскрытие информации посторонними лицами (в дальнейшем «нарушителем») может привести к значительному ущербу для пользователя. Такая информация является конфиденциальной и требует защиты от различных угроз. Под угрозой безопасности информации будем понимать потенциально возможное воздействие на информацию, которое прямо или косвенно может нанести ущерб её безопасности. Под безопасностью информации будем понимать состояние информации, при котором с требуемой вероятностью обеспечивается защита информации от различных угроз.

Среди множества угроз безопасности информации в сетевых спутниковых системах можно выделить:

* перехват в радиоканале (контроль трафика);
* воздействие преднамеренных помех;
* несанкционированное декодирование и дешифрование информации;
* информационную перегрузку за счёт передачи большого количества фрагментов ложной информации;
* передачу ложной информации (в том числе ложной командно-программной информации), постановку имитирующих помех;
* физическое воздействие на оконечные устройства.

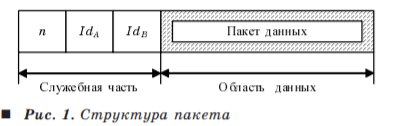
Учитывая пространственную доступность радиоканалов управления и информационного обмена с космическим аппаратом (КА) в сетевых спутниковых системах, значительное внимание необходимо уделять вопросам защиты информации от несанкционированного доступа (НСД) к её смысловому содержанию. Основным инструментом защиты информации в этом случае является криптографическая защита, построенная на основе различных алгоритмов шифрования. Кроме того, при осуществлении передачи конфиденциальной информации по сетевым спутниковым системам принципиально необходимо выполнение процедуры аутентификации – подтверждения подлинности абонента. В сетевых спутниковых системах целесообразнее использовать асимметричные криптосистемы, которые обладают следующими преимуществами:

* в сетях с большим количеством абонентов часто возникают ситуации, когда абоненты не могут доверять друг другу, а асимметричные криптосистемы позволяют строить эффективные алгоритмы аутентификации;
* использование для защиты информации в сетях с большим количеством абонентов только симметричных криптосистем требует распространения большого числа ключевой информации, а асимметричные криптосистемы свободны от данного недостатка

В общем случае системы управления и информационного обмена с КА могут быть разнородными и использовать различные протоколы на различных уровнях модели взаимодействия открытых систем. В таких сетях могут быть использованы различные каналы передачи информации, в том числе проводные, радио, оптические и др. Кроме того, в интересах управления и информационного обмена с КА возможно использование сетевых спутниковых систем связи общего пользования. В связи с этим наиболее целесообразно размещать криптографические функции на уровне представления или прикладном уровне семиуровневой модели взаимодействия открытых систем, что аналогично «туннелированию» при создании закрытых каналов в компьютерных сетях. Шифрование всей передаваемой информации в этом случае осуществляется до её поступления в терминальную абонентскую аппаратуру. За счёт этого становится возможной аутентификации абонентов с последующим переходом к информационному обмену в закрытом режиме работы.

Шифрование передаваемых сообщений в этом случае производится только конечными абонентами. Зашифрованный пакет информационного обмена абонентов инкапсулируется в пакет по стандарту, принятому в используемой сети связи

В данном случае пакет будет состоять из служебной части и области данных (рис. 1). В служебной части передаются номер пакета (*n*), адреса абонентов (идентификаторы и ), другая служебная информация (например, флаги). В области данных передаётся зашифрованный пакет информационного обмена абонентов. В случае, если длина зашифрованного пакета превышает размер области данных пакета используемой сети связи, последний может быть разбит на несколько частей в соответствии с принятыми стандартами.



Для построения асимметричных криптоалгоритмов предпочтительнее использовать математические конструкции на эллиптических кривых, как обладающие наибольшей стойкостью и скоростью криптографических преобразований по сравнению с другими типами асимметричных алгоритмов защиты информации.

Рассмотрим математические основы использования эллиптических кривых в криптографических целях. Рассмотрим эллиптическую группу по модулю *p*, где *p* является простым числом. Выберем два неотрицательных целых числа *a* и *b*, меньшие *p* и удовлетворяющие условию

Эллиптическую кривую (ЭК) над конечным полем Галуа можно представить в виде

где – эллиптическая группа по модулю *p*, элементами которой являются пары неотрицательных чисел, меньших *p* и удовлетворяющих уравнению кривой, а также точка в бесконечности *O*.

Операция обращения точки для кривой записывается следующим образом: Групповой закон сложения точек имеет вид где

При получаем

Непосредственно из формул видно, что точка в бесконечности получается при удвоении точки с нулевой координатой *y* либо при сложении двух различных точек с одинаковой координатой *x*.

Чтобы построить криптографическую систему, используя ЭК, нужно найти «вычислительную проблему», которую можно использовать в качестве односторонней функции с секретом.

Пусть *p* – простое число, а *G* – примитивный элемент или генератор аддитивной циклической подгруппы группы точек ЭК; *P* – произвольная точка, принадлежащая данной кривой. Тогда любую точку *P* кривой можно представить как кратную генератору подгруппы в виде

где *n* – кратность данной точки генератору подгруппы; «»– знак групповой операции в группе точек кривой.

Групповой закон сложения точек аддитивной абелевой группы ЭК обладает следующим криптографическим свойством: нахождение числа *n* по двум заданным элементам группы *P* и *G* при является вычислительно сложной задачей. Таким образом, групповой закон сложения точек ЭК рассматривается в качестве функции криптографического преобразования.