МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«МИРЭА – Российский технологический университет»**
**РТУ МИРЭА**

# ЛЕКЦИОННЫЕ МАТЕРИАЛЫ

## Методы обеспечения целостности информации

*(наименование дисциплины (модуля) в соответствии с учебным планом)*

| | |
|---|---|
| Уровень | бакалавриат |
| | *(бакалавриат, магистратура, специалитет)* |
| Форма обучения | очная |
| | *(очная, очно-заочная, заочная)* |
| Направление(-я) подготовки | 09.03.02 «Информационные системы и технологии» |
| | *(код(-ы) и наименование(-я))* |
| Институт | кибербезопасности и цифровых технологий (ИКБ) |
| | *(полное и краткое наименование)* |
| Кафедра | Разработка программных решений и системное программирование |
| | *(полное и краткое наименование кафедры, реализующей дисциплину (модуль))* |
| Лектор | К.т.н. Ермакова Алла Юрьевна |
| | *(сокращенно – ученая степень, ученое звание; полностью – ФИО)* |

Используются в данной редакции с учебного года 2023/24

*(учебный год цифрами)*

Проверено и согласовано «____» _____2023_г.

*(подпись директора Института/Филиала с расшифровкой)*

Москва 2023 г.

# Лекция 3. Защита целостности при транспортировке информации (первая часть)

Средства контроля целостности должны обеспечивать защиту от несанкционированного изменения информации нарушителем при ее передаче по каналам связи.

При транспортировке информации следует защищать как целостность, так и подлинность информации.

В простейшей модели передачи сообщений представлено три участника:

• отправитель А;

• получатель В;

• злоумышленник С.

Задача отправителя А заключается в формировании и отправке сообщения Х получателю В. Задача получателя В заключается в получении сообщения Х и в установлении его подлинности.

Ниже перечислены способы обмана (нарушения подлинности сообщения) при условии, что между участниками модели А, В, С отсутствует сговор.

*Способ А:* отправитель А заявляет, что он не посылал сообщение Т получателю В, хотя в действительности его посылал (подмена отправленного сообщения или отказ от авторства).

*Способ В1:* получатель В изменяет полученное от отправителя А сообщение Т и заявляет, что данное измененное сообщение он получил от отправителя А (подмена принятого сообщения).

*Способ В2:* получатель В сам формирует сообщение и заявляет, что получил его от отправителя А (имитация принятого сообщения).

*Способ С1:* злоумышленник С искажает сообщение, которое отправитель А передает получателю В (подмена передаваемого сообщения).

*Способ С2:* злоумышленник С формирует и посылает получателю В сообщение Т от имени отправителя А (имитация передаваемого сообщения).

*Способ С3:* злоумышленник С повторяет ранее переданное сообщение, которое отправитель А посылал получателю В (повтор ранее переданного сообщения).

Схема контроля целостности данных подразумевает выполнение двумя сторонами – *источником* и *приемником* – некоторых (возможно, разных) криптографических преобразований данных. Источник преобразует исходные данные и передает их приемнику вместе с некоторым приложением, обеспечивающим избыточность шифрограммы.

Приемник обрабатывает полученное сообщение, отделяет приложение от основного текста и проверяет их взаимное соответствие, осуществляя таким образом контроль целостности. Контроль целостности может выполняться с *восстановлением* или *без восстановления* исходных данных.

Целостность отдельного сообщения обеспечивается имитовставкой, ЭЦП или зашифрованием, целостность потока сообщений – соответствующим механизмом целостности.

***Имитовставка***

Для обеспечения целостности в текст сообщения часто вводится некоторая дополнительная информация, которая легко вычисляется, если секретный ключ известен, и является трудновычислимой в противном случае. Если такая информация вырабатывается и проверяется с помощью одного и того же секретного ключа, то ее называют *имитовставкой* (в зарубежных источниках используется термин *код аутентификации сообщений* – Message Authentication Code (MAC) – поскольку помимо целостности может обеспечиваться еще и аутентификация объекта). Имитовставкой может

служить значение хэш-функции, зависящей от секретного ключа, или выходные данные алгоритма зашифрования в режиме сцепления блоков шифра.

***Зашифрование***

Целостность данных можно обеспечить и с помощью их зашифрования симметричным криптографическим алгоритмом при условии, что подлежащий защите текст обладает некоторой избыточностью. Последняя необходима для того, чтобы нарушитель, не зная ключа зашифрования, не смог создать шифрограмму, которая после расшифрования успешно прошла бы проверку целостности.

Избыточности можно достигнуть многими способами. В одних случаях текст может обладать достаточной естественной избыточностью (например, в тексте, написанном на любом языке разные буквы и буквосочетания встречаются с разной частотой). В других можно присоединить к тексту до зашифрования некоторое контрольное значение, которое, в отличие от имитовставки и цифровой подписи, не обязательно должно вырабатываться криптографическими алгоритмами, а может представлять собой просто последовательность заранее определенных символов.

***Контроль целостности потока сообщений***

Контроль целостности потока сообщений помогает обнаружить их повтор, задержку, переупорядочение или утрату. Предполагается, что целостность каждого отдельного сообщения обеспечивается зашифрованием, имитовставкой или цифровой подписью. Для контроля целостности потока сообщений можно, например:

• присвоить сообщению *порядковый номер целостности* (ПНЦ);

• использовать в алгоритмах зашифрования *сцепление* с предыдущим сообщением.

При использовании ПНЦ, который может включать в себя порядковый номер сообщения и имя источника, приемник хранит последний номер принятого сообщения каждого источника. Для контроля целостности приемник проверяет, например, что ПНЦ текущего сообщения от данного источника *S* на единицу больше номера предыдущего сообщения: ПНЦ(*s*)*i* = ПНЦ(*s*)*i*-1 +1. Если в качестве ПНЦ используется время отправки сообщения, то проверяется, действительно ли время отправки и время приема близки друг к другу сточностью до задержки сообщения в канале связи и разности хода часов источника и приемника.

***Электронно-цифровая подпись***

Термин ЭЦП используется для методов, позволяющих устанавливать подлинность автора сообщения при возникновении спора относительно авторства этого сообщения. ЭЦП применяется в информационных системах, в которых отсутствует взаимное доверие сторон (финансовые системы, системы контроля за соблюдением международных договоров и др.).

Концепцию цифровой подписи для аутентификации информации предложили Диффи и Хеллман в 1976 г. Она заключается в том, что каждый абонент сети имеет личный секретный ключ, на котором он формирует подпись и известную всем другим абонентам сети проверочную комбинацию, необходимую для проверки подписи (эту проверочную комбинацию иногда называют открытым ключом). Цифровая подпись вычисляется на основе сообщения и секретного ключа отправителя. Любой получатель, имеющий соответствующую проверочную комбинацию, может аутентифицировать сообщение по подписи.

ЭЦП в цифровых документах играет ту же роль, что и подпись, поставленная от руки в документах, которые напечатаны на бумаге: это данные, присоединяемые к передаваемому сообщению и подтверждающие, что отправитель (владелец подписи) составил или заверил данное сообщение. Получатель сообщения или третья сторона с помощью цифровой подписи

может проверить, что автором сообщения является именно владелец подписи (т. е. аутентифицировать источник данных) и что в процессе передачи не была нарушена целостность полученных данных.

Таким образом, при разработке механизма ЭЦП возникают следующие основные задачи:

• создать подпись таким образом, чтобы ее невозможно было подделать

• иметь возможность проверки того, что подпись действительно принадлежит указанному владельцу.

• предотвратить возможность отказа от подписи, т. е. подпись должна быть построена таким образом, чтобы отправитель, подписавший сообщение, не смог затем отрицать перед получателем или третьей стороной факт подписания, утверждая, что подпись подделана.