17. Информационная безопасность

Газизов Тимур Тальгатович,
к.т.н., доцент кафедры информатики ТГПУ

ИНФОРМАЦИОННЫЕ СЕТИ ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

ВВЕДЕНИЕ

- Информационная безопасность не является залогом безопасности вашей компании, информации и компьютерных систем. К сожалению, обеспечить надежную защиту "по взмаху волшебной палочки" нельзя. Но реализовать ее на должном уровне вполне реально, хотя концепции, лежащие в ее основе, не очень-то и просты.
- Информационная безопасность - это система, позволяющая выявлять уязвимые места организации, опасности, угрожающие ей, и справляться с ними. К сожалению, известно много примеров, когда продукты, считающиеся "лекарством на все случаи жизни", на самом деле уводили в сторону от выработки надлежащих способов эффективной защиты. Свою лепту вносили их производители, заявляющие о том, что именно их продукт решает все проблемы безопасности.

ПОНЯТИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- В онлайновом словаре Мерриама_Вебстера (Merriam-Webster) (http://www.m-w.com/) дается следующее определение информации:
  - сведения, полученные при исследовании, изучении или обучении;
  - известия, новости, факты, данные;
  - команды или символы представления данных (в системах связи или в компьютере);
  - знания (сообщения, экспериментальные данные, изображения), меняющие концепцию, полученную в результате физического или умственного опыта.
- Безопасность определяется следующим образом: свобода от опасности, сохранность; свобода от страха или беспокойства.
- Если мы объединим эти два понятия вместе, то получим определение информационной безопасности - меры, принятые для предотвращения несанкционированного использования, злоупотребления, изменения сведений, фактов, данных или аппаратных средств либо отказа в доступе к ним.

СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТИПЫ АТАК

Таблица 4.1. Службы информационной безопасности и типы атак

Атаки	**Службы безопасности**			
	Конфиденциальность	Целостность	Доступность	Идентифицируемость
Доступа	X			X
Модификации		X		X
Отказ в обслуживании			X	
Отказ от обязательств		X		X

КОНФИДЕНЦИАЛЬНОСТЬ

- Служба конфиденциальности обеспечивает секретность информации. Правильно сконфигурированная, эта служба открывает доступ к информации только аутентифицированным пользователям. Ее надежная работа зависит от службы обеспечения идентификации и однозначного определения подлинности лиц. Выполняя эту функцию, служба конфиденциальности ограждает системы от атак доступа. Служба конфиденциальности должна учитывать различные способы представления информации - в виде распечаток, файлов или пакетов, передающихся по сетям

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ФАЙЛОВ

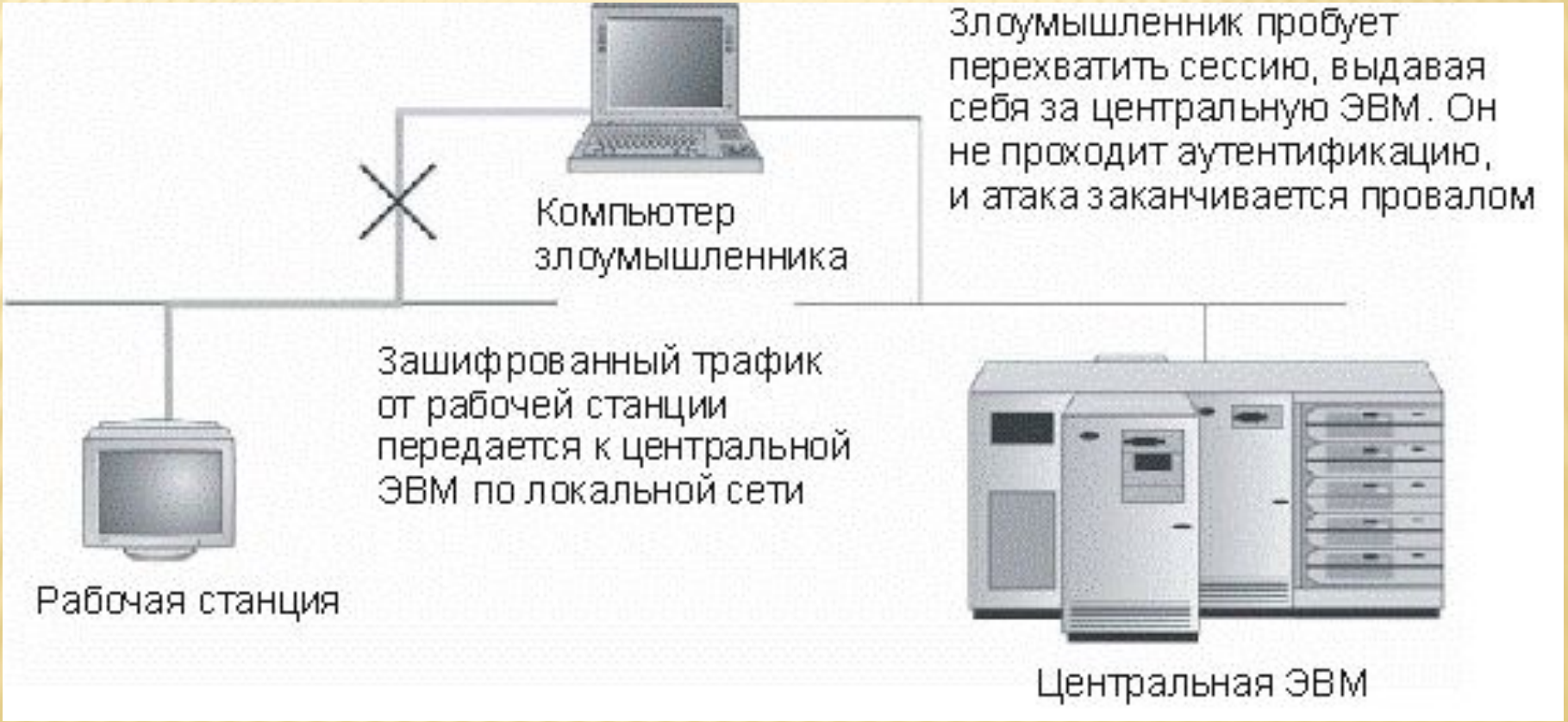
- Существуют различные способы обеспечения секретности документов в зависимости от их вида. Бумажные документы нужно защищать физически, т. е. хранить в отдельном месте, доступ к которому контролируется службой конфиденциальности. Не следует забывать о таких вещах, как запирание картотек и ящиков столов, ограничение доступа в кабинеты внутри офиса или в сам офис.

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ПЕРЕДАЧЕ ДАННЫХ ПО СЕТИ

Шифрование обеспечивает защиту информации при передаче по сетям

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ПЕРЕДАЧЕ ДАННЫХ ПО СЕТИ

Шифрование в сочетании с надежной идентификацией позволяет предотвратить перехват трафика



ЦЕЛОСТНОСТЬ

- Служба обеспечения целостности следит за правильностью информации. При должном уровне организации эта служба дает пользователям уверенность в том, что информация является верной, и ее не изменил никто из посторонних. Подобно службе конфиденциальности, служба обеспечения целостности должна работать совместно со службой идентификации, чтобы осуществлять надежную проверку подлинности. Данная служба является "щитом" от атак модификации. Информация, которую она защищает, может быть представлена в виде бумажных распечаток, в виде файлов либо в виде данных, передаваемых по сети.

ЦЕЛОСТНОСТЬ ФАЙЛОВ

- Как уже говорилось выше, информация может быть представлена в виде бумажных распечаток или в виде файлов. Конечно, легче обеспечить защиту бумажных документов, да и установить факт изменения содержимого такого документа гораздо проще. Ведь злоумышленнику требуется определенный навык, чтобы поддельный документ выглядел достоверно. А компьютерный файл может изменить любой, кто имеет к нему доступ. Существует несколько способов защиты бумажных документов от подделки. Можно ставить подпись на каждой странице, сшивать документы в папки, изготавливать несколько копий документа. Механизмы обеспечения целостности затрудняют подделку документов. Хотя злоумышленники научились копировать подписи, сделать это все же непросто, требуется серьезный навык. Достаточно сложно добавить или удалить документ из общей подшивки. А если копии документов разосланы всем заинтересованным сторонам, то подменить сразу все документы практически невозможно.

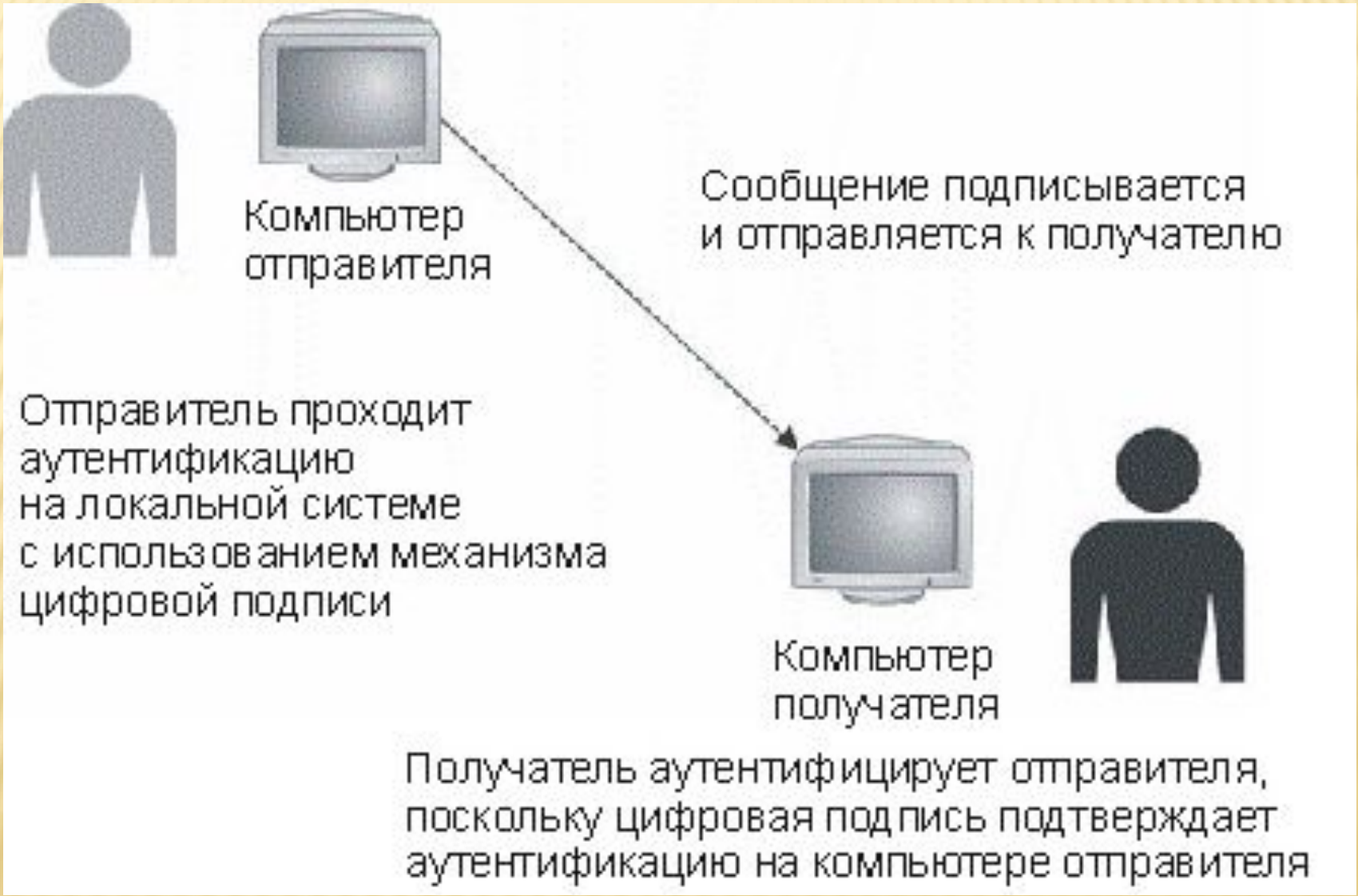
ДОСТУПНОСТЬ

- Служба обеспечения доступности информации поддерживает ее готовность к работе, позволяет обращаться к компьютерным системам, хранящимся в этих системах данным и приложениям. Эта служба обеспечивает передачу информации между двумя конечными пунктами или компьютерными системами. В данном случае речь идет в основном об информации, представленной в электронной форме (но подходит и для обычных документов).

ИДЕНТИФИЦИРУЕМОСТЬ

- Про службу идентификации часто забывают, когда речь идет о безопасности. Главная причина в том, что сама по себе эта служба не позволяет предотвратить атаки. Она должна работать совместно с другими службами, чтобы увеличивать их эффективность. Если рассматривать эту службу отдельно, то мы увидим, что она усложняет систему безопасности и повышает ее стоимость. Однако без работы службы идентификации и служба обеспечения целостности, и служба обеспечения конфиденциальности обречены на неудачу.

РАБОТА МЕХАНИЗМА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ В СОЕДИНЕНИИ УДАЛЕННОГО ДОСТУПА



АУДИТ

- Аудит позволяет фиксировать происходящие события. Записи аудита связывают пользователя с действиями, которые он выполняет в системе. Без надежной службы идентификации и аутентификации аудит становится бесполезным, поскольку нет гарантии, что зафиксированные действия на самом деле выполнены указанным лицом.
- Аудит в реальной жизни осуществляется с помощью журналов регистрации, ведомостей пропусков на выход, видеозаписей. Его задачей является отчет о выполненных действиях. Служба целостности должна гарантировать, что информация в журнале аудита не изменялась, иначе ее достоверность ставится под сомнение.
- В компьютерных системах аудит ведется с помощью журналов, в которые записываются действия пользователя. Если служба идентификации и аутентификации работает должным образом, то эти события можно отождествить с определенным пользователем. Электронные журналы аудита тоже необходимо защищать от любых изменений.