Стандарты информационной безопасности распределенных систем

Введение

- **Цели изучения темы**
- ознакомиться с основными положениями стандартов по обеспечению информационной безопасности в распределенных вычислительных сетях.
- **Требования к знаниям и умениям**
- Студент должен знать:
- основное содержание стандартов по информационной безопасности распределенных систем;
- основные сервисы безопасности в вычислительных сетях;
- наиболее эффективные механизмы безопасности;
- задачи администрирования средств безопасности.
- Студент должен уметь:
- выбирать механизмы безопасности для защиты распределенных систем.
- **Ключевой термин**
- Ключевой термин: распределенная информационная система.
- Распределенная информационная система – совокупность аппаратных и программных средств, используемых для накопления, хранения, обработки, передачи информации между территориально удаленными пользователями.
- **Второстепенные термины**
- сервис безопасности;
- механизм безопасности.

Сервисы безопасности в вычислительных сетях

- В последнее время с развитием вычислительных сетей и в особенности глобальной сети Интернет вопросы безопасности распределенных систем приобрели особую значимость. Важность этого вопроса косвенно подчеркивается появлением чуть позже "Оранжевой книги" стандарта, получившего название **"Рекомендации X.800"**, который достаточно полно трактовал вопросы информационной безопасности распределенных систем, т. е. вычислительных сетей.
- Рекомендации X.800 выделяют следующие сервисы (функции) безопасности и исполняемые ими роли:

- **Аутентификация**. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. **Аутентификация партнеров по общению** используется при установлении соединения и периодически во время сеанса. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).
- **Управление доступом** обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.
- **Конфиденциальность данных** обеспечивает защиту от несанкционированного получения информации. Отдельно выделяется **конфиденциальность трафика** – это защита информации, которую можно получить, анализируя сетевые потоки данных.
- **Целостность данных** подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры – с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.
- **Неотказуемость** (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки.

Механизмы безопасности

В X.800 определены следующие сетевые механизмы безопасности:

- шифрование;
- электронная цифровая подпись;
- механизм управления доступом;
- механизм контроля целостности данных;
- механизм аутентификации;
- механизм дополнения трафика;
- механизм управления маршрутизацией;
- механизм нотаризации (заверения).

Следующая таблица иллюстрирует, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для реализации той или иной функции.

Таблица - Взаимосвязь функций и механизмов безопасности

Функции	Механизмы							
	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Аутентификация партнеров	+	+	-	-	+	-	-	-
Аутентификация источника	+	+	-	-	-	-	-	-
Управление доступом	-	-	+	-	-	-	-	-
Конфиденциальность	+	-	+	-	-	-	+	-
Избирательная конфиденциальность	+	-	-	-	-	-	-	-
Конфиденциальность трафика	+	-	-	-	-	+	+	-
Целостность соединения	+	-	-	+	-	-	-	-
Целостность не соединения	+	+	-	+	-	-	-	-
Неотказуемость	-	+	-	+	-	-	-	+

"+" механизм используется для реализации данной функцию безопасности;
"-" механизм не используется для реализации данной функции безопасности.
Так, например, "Конфиденциальность трафика" обеспечивается "Шифрованием", "Дополнением трафика" и "Управлением маршрутизацией".

Администрирование средств безопасности

- В рекомендациях X.800 рассматривается понятие **администрирование средств безопасности**, которое включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Например, распространение криптографических ключей.
- Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:
- администрирование информационной системы в целом;
- администрирование сервисов безопасности;
- администрирование механизмов безопасности.

- **Администрирование информационной системы** в целом включает *обеспечение* актуальности политики безопасности, *взаимодействие* с другими административными службами, реагирование на происходящие события, *аудит* и *безопасное восстановление*.
- **Администрирование сервисов безопасности** включает в себя *определение* защищаемых объектов, *выработку правил* подбора механизмов безопасности (при наличии альтернатив), *комбинирование механизмов* для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.
- **Администрирование механизмов безопасности** включает:
- управление криптографическими ключами (генерация и распределение);
- управление шифрованием (установка и синхронизация криптографических параметров);
- администрирование управления доступом (распределение информации, необходимой для управления – паролей, списков доступа и т. п.);
- управление аутентификацией (распределение информации, необходимой для аутентификации – паролей, ключей и т. п.);
- управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений – частоту отправки, размер и т. п.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

- В 1987 г. Национальным центром компьютерной безопасности США была опубликована интерпретация "Оранжевой книги" для сетевых конфигураций. Данный документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.
- Интерпретация отличается от самой "Оранжевой книги" учетом динамичности сетевых конфигураций. В интерпретациях предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами корректности функционирования друг друга, а также присутствие средств оповещения администратора о неполадках в сети.

- Среди защитных механизмов в сетевых конфигурациях на первое место выдвигается **криптография**, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость реализации механизмов управления ключами.
- В интерпретациях "Оранжевой книги" впервые систематически рассматривается вопрос обеспечения доступности информации.
- Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей.

- Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:
- внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т. п.);
- наличие средств реконфигурирования для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;
- рассредоточенность сетевого управления, отсутствие единой точки отказа;
- наличие средств нейтрализации отказов (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);
- выделение подсетей и изоляция групп пользователей друг от друга.

Выводы по теме

- Стандарты информационной безопасности предусматривают следующие сервисы безопасности:
  - аутентификация;
  - аутентификация источника;
  - управление доступом;
  - конфиденциальность;
  - конфиденциальность трафика;
  - целостность соединения;
  - целостность вне соединения;
  - неотказуемость.
- Механизмы безопасности:
  - шифрование;
  - электронная цифровая подпись;
  - механизм управления доступом;
  - механизм контроля целостности данных;
  - механизм аутентификации;
  - механизм дополнения трафика;
  - механизм управления маршрутизацией;
  - механизм нотаризации (заверения).

Выводы по теме

- **Администрирование средств безопасности** включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Например, распространение криптографических ключей.
- Администратор средств безопасности решает следующие задачи:
  - администрирование информационной системы в целом;
  - администрирование сервисов безопасности;
  - администрирование механизмов безопасности.

Вопросы для самоконтроля

- Дайте характеристику составляющих "информационной безопасности" применительно к вычислительным сетям.
- Перечислите основные механизмы безопасности.
- Какие механизмы безопасности используются для обеспечения конфиденциальности трафика?
- Какие механизмы безопасности используются для обеспечения "неотказуемости" системы?
- Что понимается под администрированием средств безопасности?
- Какие виды избыточности могут использоваться в вычислительных сетях?