Управление Безопасностью (SM)

Костюкович А.Е.

СибГУТИ, Новосибирск

Тел. 8-(383)-269-82-42,

E-mail: kostuk@sibsutis.ru

Обзор существующих методов обеспечения информационной безопасности (ИБ)

Множество существующих методов обеспечения информационной безопасности можно классифицировать по разным признакам.

Только уместная комбинация этих методов позволит сетевому администратору обеспечить информационную безопасность.

В целом все методы можно разделить на два класса:

1. **Организационно-правовые методы**, включая воспитание у пользователей отношения недопустимости и нетерпимости к нарушениям ИБ.

2. **Организационно-технические методы**

Правовые методы нашли отражение в серии документов международных и национальных организаций, регламентирующих все аспекты обеспечения ИБ.

1. Организационно-правовые методы

Главная цель мер, предпринимаемых на управленческом уровне — сформировать программу работ в области ИБ и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой этой программы является политика безопасности, отражающая подход организации к защите своих информационных ресурсов.

1. Организационно-правовые методы

Политика безопасности

Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информационных ресурсов.

Политикой безопасности называют и простые правила использования сетевых ресурсов, и детальные описания всех соединений и их особенностей, занимающие сотни страниц.

Стандарт RFC 2196 описывает политику безопасности следующим образом:

«Политика безопасности — это формальное изложение правил, которым должны подчиняться лица, получающие доступ к сетевым технологиям и информации».

1. Организационно-правовые методы

Правильная политика безопасности даже без выделенных средств защиты дает лучшие результаты, чем средства защиты без политики безопасности

1. Организационно-правовые методы

Профиль защиты

Профилем защиты называют набор требований, предъявляемых заказчиком к обеспечению ИБ.

Это может быть типовой набор требований, взятый из «Общих критериев» или детально сформулированное ТЗ на ИБ, отражающее всю специфику ИБ у заказчика

При обеспечении ИБ следует помнить:

Управление ИБ – это **непрерывный, эволюционный процесс**, развивающийся в конкуренции со средствами нарушения ИБ.

Этот процесс никогда не закончится, т.к. совершенствуются и методы нарушения ИБ.

Основополагающие документы в области информационной безопасности

1. Рекомендации ITU-T X.800
2. Оранжевая книга TCSEC
3. Интерпретация оранжевой книги
4. Гармонизированные критерии Европейских стран ITSEC
5. Концепция защиты от НСД Гостехкомиссии при президенте РФ
6. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» ("Общие критерии")

Подробнее – в Лаборат. Работе!

Распределение функций безопасности по уровням ЭМВОС (ISO-OSI)

Функции безопасности	Уровень модели OSI						
	1	2	3	4	5	6	7
1. Аутентификация	-	-	+	+	-	-	+
2. Управление доступом	-	-	+	+	-	-	+
3. Конфиденциальность соединения	+	+	+	+	-	+	+
4. Конфиденциальность вне соединений	-	+	+	+	-	+	+
5. Избирательная конфиденциальность	-	-	-	-	-	+	+
6. Конфиденциальность трафика	+	-	+	-	-	-	+
7. Целостность с восстановлением	-	-	-	+	-	-	+
8. Целостность без восстановления	-	-	+	+	-	-	+
9. Избирательная целостность	-	-	-	-	-	-	+
10. Целостность вне соединения	-	-	+	+	-	-	+
11. Неотказуемость	-	-	-	-	-	-	+

Обзор существующих методов (механизмов) обеспечения информационной безопасности (ИБ)

Для реализации функций безопасности могут использоваться следующие механизмы и их комбинации.

1. **Шифрование.**
2. **Электронная (цифровая) подпись.**
3. **Механизмы управления доступом.**
   - Пароли или иная аутентификационная информация.
   - Токены, билеты или иные удостоверения.
   - Метки безопасности, ассоциированные с субъектами и объектами доступа.
   - Время запрашиваемого доступа.
   - Маршрут запрашиваемого доступа.
   - Длительность запрашиваемого доступа.
4. **Механизмы контроля целостности данных.**
5. **Механизмы аутентификации.**
6. **Механизмы дополнения трафика.**
7. **Механизмы управления маршрутизацией.**
8. **Механизмы нотаризации.**

Обзор существующих методов (механизмов) обеспечения информационной безопасности (ИБ)

В Таб. 4 сведены функции и механизмы безопасности.

Таблица показывает, какие механизмы (по одиночке или в комбинации с другими) могут использоваться для реализации той или иной функции.

Обзор существующих методов (механизмов) обеспечения информационной безопасности (ИБ)

Механизмы/ Функции безопасности	Шифрование подписи	Электронный трафик	Управление доступом	Целостность	Аутентификация	Дополнение	Управление маршрутизацией	Нотариация
Аутентификация партнеров	+	+	-	-	+	-	-	-
Аутентификация источника	+	+	-	-	-	-	-	-
Управление доступом	-	-	+	-	-	-	-	-
Конфиденциальность	+	-	-	-	-	-	+	-
Избирательная конфиденциальность	+	-	-	-	-	-	-	-
Конфиденциальность трафика	+	-	-	-	-	+	+	-
Целостность соединения	+	-	-	+	-	-	-	-
Целостность вне соединения	+	+	-	+	-	-	-	-
Неотказуемость	-	+	-	+	-	-	-	+

Классификация угроз

Под угрозами ИБ систем (сетей) связи принято понимать “воздействия нарушителя ИБ на информационную сферу, которые будучи не предотвращенными, не обнаруженными и не ликвидированными могут привести к снижению качества услуг и нарушению функционирования сети связи и, как следствие, нанесению ущерба государству, пользователям и (или) поставщикам услуг.

Классификация угроз

Различают **три вида источников угроз** ИБ, обусловленные:

- **действием злоумышленников;**
- **техническими средствами;**
- **стихийными явлениями.**

Классификация угроз

Международные организации стандартизации классифицируют угрозы по типам, видам и категориям.

При этом классификация угроз распространяется на три уровня:

- **инфраструктуру сети,**
- **услуги связи,**
- **приложения.**

Первый из этих уровней охватывает информацию пользователей,

второй — услуги сети,

третий — приложения, в том числе телематические службы, организуемые на базе сетей.

Классификация угроз

По характеру воздействия, угрозы разделяются на

- **случайные и преднамеренные,**
- **активные и пассивные**.

Классификация угроз

По месту возникновения выделяют:

Внутренние угрозы — это угрозы со стороны внутренних пользователей.

Большинство угроз происходит изнутри корпоративной сети. Потенциальными источниками таких угроз являются

- обиженные сотрудники,
- промышленные шпионы,
- посетители и
- беспечные пользователи, допускающие ошибки.

Внешние (сетевые) угрозы

Угрозы подключенным к Интернет системам общего доступа. Эти системы являются потенциальными объектами внешних атак.

Типовые сетевые (внешние) угрозы

По типу воздействия на ИБ угрозы можно разделить на:

- **Несанкционированный доступ;**
- **Хакерская разведка сети;**
- **Атаки на пароли;**
- **IP-спуфинг (подмена IP-адресов);**
- **Сниффинг (перехват и анализ) пакетов;**
- **Злоупотребление доверием.**
- **Вирусы и приложения типа «троянский конь»**
- **Переадресация портов.**
- **Отказ в обслуживании (DoS)**
- **Раскрытие сетевой топологии**
- **Атаки на уровне приложений**