

Методики обеспечения Информационной Безопасности (ИБ) IP-АТС Asterisk

1. Источники возникновения угроз ИБ

- Конфигурирование IP-АТС Asterisk с настройками «по умолчанию»;
- Использование паролей учетных записей абонентов, неустойчивых к атакам путем прямого перебора;

2. Методики противодействия угрозам ИБ

2.1. Изменение настроечных параметров IP-АТС и ОС Linux

- В конфигурационном файле sip.conf устанавливаются параметры: allowguests=no, alwaysauthrequest=yes;
- Опционально, во встроенном фильтре сетевых пакетов Linux устанавливаются запреты на подключения к порту 5060;

2.2. Установка специализированного ПО

- Принудительно используется утилита fail2ban - блокирующая любые запросы с IP-адреса после нескольких неудачных попыток авторизации на сервере телефонии;

2.3. Ограничения на уровне запрета звонков по направлениям;

- Предусмотрена возможность создания групп пользователей, обладающих разными правами на исходящие звонки (городские номера, Москва+Петербург, стационарные по России, мобильные по России и т.д.);
- Для операторов Центра Обработки Вызовов может быть установлен запрет любых исходящих вызовов до авторизации;

2.4. Ограничения на уровне количества одновременных звонков по направлениям;

- Предусмотрена возможность задания максимального количества одновременных звонков на определенный транк или префикс (например, 1 одновременный звонок по международному коду 8810)

2.5. Ограничения на уровне длительности телефонных переговоров

- Предусмотрена возможность автоматического прерывания звонка по истечению заданного промежутка времени (например, звонок по международному коду 8810 длится не более 10 минут);

3. Контактная информация

На все вопросы, связанные с данным документом,
Вам с удовольствием ответит **Марков Вадим**, технический директор ЗАО «Линия 24».

vadim@line24.ru

тел.: (812) 448-53-78, (495) 721-84-69 (доб. 700)