ВестКолл
САНКТ-ПЕТЕРБУРГ

Безопасность VoIP:

Схемы и рекомендации по повышению безопасности.

СОДЕРЖАНИЕ

VoIP. Новые возможности и новые угрозы.

В отличие от традиционной телефонной сети общего пользования, технология **VoIP** для передачи голоса использует IP-сети. Обмен данными по IP-сетям в незащищенном виде становится привлекательной целью для злоумышленников, особенно, когда речь идет о голосовых данных. Соответственно, инфраструктурам VoIP угрожают те же опасности, что и для сетей передачи данных. Однако результаты успешной атаки на сеть передачи голосовых данных могут быть более серьезными: задержанное на несколько минут электронное письмо или медленно работающий веб-браузер редко приводят к тяжелым последствиям, в отличие от прерывания телефонного разговора или полного выхода из строя системы коммуникаций.

1. Возможные сценарии взлома и незаконного использования оборудования или учетных записей.

Прямые вызовы через взломанную IP АТС

Злоумышленник, используя автоматизированное программное обеспечение (например, SIP-сканер), сканирует сеть в поисках VoIP-оборудования. Как только злоумышленник обнаружил VoIP-устройство (например, IP АТС), начинается подбор логина и пароля. После успешного подбора пароля злоумышленник пробует осуществить вызовы через взломанное оборудование. Если вызовы через скомпрометированную IP АТС успешно проходят, то на неё направляется VoIP-трафик на дорогие, обычно международные направления, такие как Коста-Рика, Кот-д'Ивуар, Сомали, Куба. При этом злоумышленник пытается максимально загрузить все имеющиеся каналы станции, так что за короткое время может быть потрачено огромное число исходящих минут. Суммы счетов для взломанного пользователя обычно исчисляются десятками и сотнями тысяч рублей, даже с учетом оплаты такого трафика по операторским тарифам. Бывает, что владельцы АТС узнают о взломе только через несколько дней или недель, когда сумма счета уже становится огромной. Помимо взлома с использованием подбора пароля, злоумышленник может использовать уязвимость в программном обеспечении IP АТС, использовать инсайдерскую информацию или получить физический доступ к оборудованию.

Несанкционированные вызовы через DISA (Direct Inward System Access)

DISA – это функция прямого доступа к конкретному абоненту внутренней телефонной сети. Переведя свой телефон в тональный режим, звонящий по городской линии (VoIP-транку) может набрать внутренний номер сервиса DISA, ввести PIN-код для авторизации на станции и как внутренний абонент совершать исходящие вызовы за счет компании. Злоумышленник может вычислить, что на станции работает DISA и подобрать PIN для авторизации, а затем направить телефонный трафик на дорогие направления, как и в предыдущем случае. Такой метод взлома используется не часто, но имеет место.

Хищение информации об учетных записях с целью последующего использования в личных целях

Этот вид мошенничества довольно часто используется для SIP-линий (или SIP-аккаунтов), которые можно использовать из любой точки мира, имея доступ в интернет. Все, что необходимо злоумышленнику - получить информацию о SIP-сервере, имени пользователя (userID), имени для аутентификации (authID) и пароле учетной записи. Располагая этой информацией, можно

зарегистрироваться на любом SIP-устройстве и совершать вызовы от имени владельца номера, чаще всего на максимально дорогие направления.

Инъекция аудиоданных

Это вид атаки, когда злоумышленник добавляет в вызов свои аудиоданные, чтобы скомпрометировать стороны. Это возможно, например, после получения доступа и перенастройки IP АТС.

Кража или незаконное прослушивание аудиозаписей разговоров пользователей

Если на IP АТС хранятся записи разговоров, они могут быть похищены, а информация, которая в них содержится, может быть незаконно использована.

Незаконный сбор информации о вызовах

Если злоумышленник получил доступ к IP АТС, он может собирать информацию о вызовах и использовать её в своих целях.

Атака типа «отказ в обслуживании» (Denial Of Service) оборудования

Распространённый и очень опасный вид атак «отказ в обслуживании», который может вывести из строя VoIP-оборудование компании на длительное время, и тем самым полностью парализовать телефонию. Если IP АТС подключена к оператору связи через интернет (например, через VoIP-транк) и никак не защищена, то она уязвима к атакам такого типа. Например, с различных IP-адресов на IP-адрес оборудования начинает приходить огромное число бессмысленных сообщений. Тем не менее, эти сообщения должны обрабатываться VoIP-оборудованием, формируя ответные сообщения об ошибках. Если сообщений становится слишком много, система не справляется, ее производительность резко снижается, и оборудование перестает отвечать на любые сообщения или отвечает очень медленно.

Голосовой спам SPIT (spam over IP telephony)

Например, IP АТС настроена таким образом, что любые вызовы с любого IP-адреса отправляются на голосовое меню в дневное время и на автоответчик в ночное время. Этим могут воспользоваться злоумышленники, чтобы рассылать голосовой спам. Днем спам-вызовы могут приходить на случайного сотрудника или на секретаря, а ночью на голосовую почту.

Перехват информации и перехват сеанса

Вид атаки, когда трафик между VoIP-оборудованием компании и VoIP-оборудованием оператора

перехватывается злоумышленником. Это позволяет ему собирать информацию о вызовах или модифицировать их.

Все источники угроз могут быть внешними и внутренними:

Внешние источники - неавторизованные лица, пытающиеся получить доступ к оборудованию физически или из внешней сети, например, из интернета.

Внутренние источники связаны с информацией, которую могут получить авторизованные лица, например, сотрудники или администраторы, а затем использовать её для незаконного доступа к учетным записям пользователей, информации о вызовах, оборудованию компании и прочее.

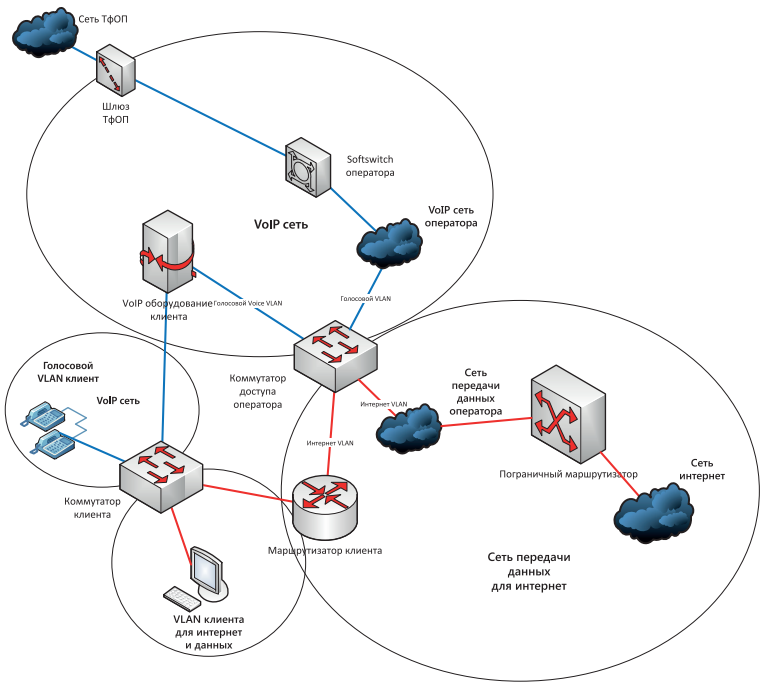
2. Общие рекомендации по повышению безопасности.

Запросите у оператора VoIP возможность использовать выделенный голосовой VLAN

(аббр. от англ. Virtual Local Area Network) — логическая («виртуальная») локальная компьютерная сеть для подключения VoIP-транка к оборудованию оператора, вместо подключения через сеть интернет.

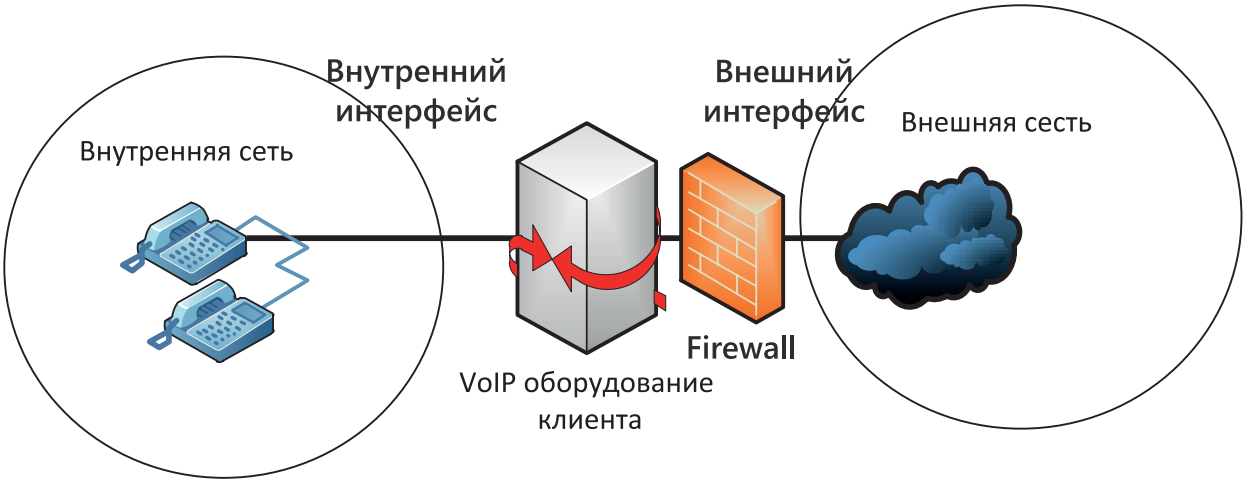
Правильно построенная сеть для VoIP существенно повышает безопасность. Проектировать и внедрять решения VoIP-телефонии должны профессионалы, которые знают, как построить надежную и безопасную сеть.

Используйте VLAN для разделения голосового трафика и трафика передачи данных



Используйте два сетевых интерфейса

Хорошей практикой является использование нескольких сетевых интерфейсов в сервере АТС, где SIP-протокол полностью доступен только на внутреннем сетевом IP-адресе. А, например, объединение офисов осуществляется по SIP-протоколу, с явным открытием на сетевом фильтре только IP-адресов офисов и фильтрацией для всех остальных. В такой конфигурации у злоумышленника отсутствует физическая возможность атаковать оборудование VoIP с использованием уязвимостей VoIP-протоколов.



Используйте сетевой фильтр с возможностью распознавания DoS атак

Если существуют риски атаки типа «отказ в обслуживании» (Denial Of Service – DoS), следует установить специальное оборудование, которое распознает такой тип атак и автоматически блокирует атакующего с уведомлением системного администратора.

Обеспечьте безопасность оборудования VoIP на физическом уровне

Доступ к оборудованию должны иметь только ответственные за него лица.

Отключите любые неиспользуемые сервисы и сетевые службы на оборудовании VoIP

Например, на IP АТС могут работать сервисы snmp, ftp, http или web-сервер. Особенно уязвимы программные IP АТС, работающие под управлением различных Linux или Windows дистрибутивов. Операционная система может запускать различные сервисы, о наличии которых администратор даже не догадывается, но они легко могут быть использованы злоумышленниками для взлома. Например, список сетевых сервисов и открытых портов в Linux легко можно узнать, воспользовавшись командой *netstat -atnup | grep LISTEN*

Ограничьте доступ к открытым портам

Оставив только необходимые службы, рекомендуется также ограничить доступ к ним, используя сетевой экран (в Linux iptables, в Cisco IOS ip acl). Например, разрешить доступ к ftp или tftp серверу только для IP-адресов, которым этот доступ может понадобиться, и запретить для всех остальных. Доступ к web-интерфейсу IP АТС - только с IP-адреса компьютера администратора.

Ограничьте доступ к удаленному управлению

1. С помощью командной строки.

Не используйте протоколы для удаленного доступа без шифрования (например, telnet).
Рекомендуется использовать SSH (Secure SHell).
Чтобы повысить безопасности доступа по SSH, воспользуйтесь рекомендациями:

- изменение порта по умолчанию. Порт 22 используется службой SSH по умолчанию. Если есть возможность, следует изменить номер порта на нестандартный, например, 23465. Многие атаки на устройства в сети начинаются со сканирования стандартных портов с целью определить, прослушивают ли их сетевые сервисы. Если такие порты существуют, вероятность их взлома велика;
- явное перечисление пользователей, имеющих доступ к системе, в директиве *AllowUsers* конфигурационного файла сервера SSH. В том случае, если все же необходимо предоставить доступ к системе ряду доверенных лиц, перечислите их;
- используйте только SSH протокол версии 2;
- запретите прямой доступ к учетной записи пользователя root. Это существенно затруднит и скорее сделает невозможной атаку на перебор пароля, так как пользователю root будет запрещён доступ в систему, даже при введении корректного пароля;
- используйте временное ограничение по вводу пароля или сертификаты. Установка минимально возможного времени для ввода пароля, например, 10 секунд, может хорошо сбить с толку злоумышленника.

Пример настроек /etc/ssh/sshd_config для Linux:

/etc/ssh/sshd_config
AllowUsers vasya petya borya
Port 23465
Protocol 2
LoginGraceTime 10s
PermitRootLogin no

2. Через Web-интерфейс.

Администраторам следует не забывать изменить пароль по умолчанию и ограничить доступ к

web-интерфейсу списком конкретных IP-адресов. Также рекомендуется использовать SSL шифрование для протокола http.

Используйте нестандартные порты для сигнальных протоколов

Назначьте в качестве слушающего порта для SIP, например, порт 9966 вместо стандартного 5060. Обычно первым этапом при сканировании диапазона IP-адресов в интернете с целью выявить устройства VoIP для последующего взлома является поиск открытых сигнальных портов SIP, H.323 и т.д.

Принимайте входящие вызовы только с IP адресов вашего провайдера

Особенно это актуально, если между вашей IP АТС и оператором сконфигурирован статический VoIP-транк. Это позволит избежать вероятности:

1. Совершения вызовов через вашу IP АТС, если злоумышленник знает ваш АОН (CALLER ID) и знает, каким образом набрать номер вызываемого абонента, чтобы вызов был отправлен по исходящему каналу.

Для Cisco IOS системный администратор легко произведет настройки, используя встроенные ACL.

В новых версиях IOS Cisco в конфигурации по умолчанию во всех ACL есть строка deny any. Это означает, что по умолчанию сетевые подключения закрыты для всех IP-адресов и следует открывать доступ только для конкретных сетей и хостов.

Если у вас IP АТС Asterisk, попросите вашего системного администратора произвести настройки с помощью ACL в Linux, например, используя сетевой экран iptables.

Например: Разрешить входящие пакеты на порт 5060 только для указанных хостов и сетей, всем остальным запретить:

```
922  iptables -A INPUT -s 71.25.103.0/24 -p udp --dport 5060 -j ACCEPT
923  iptables -A INPUT -s 71.25.79.150 -p udp --dport 5060 -j ACCEPT
924  iptables -A INPUT -s 71.25.66.206 -p udp --dport 5060 -j ACCEPT
925  iptables -A INPUT -s 71.25.73.38 -p udp --dport 5060 -j ACCEPT
926  iptables -A INPUT -s 71.25.66.106 -p udp --dport 5060 -j ACCEPT
927  iptables -A INPUT -s 71.157.120.91 -p udp --dport 5060 -j ACCEPT
928  iptables -A INPUT -p udp --dport 5060 -j DROP
```

На самом Asterisk используйте строки “permit=” и “deny=” в файле sip.conf

2. Отправки спам-вызовов (массовая рассылка коммерческой, политической и рекламной информации или иного вида сообщений лицам, не выражавшим желания их получать) на вашу IP АТС из интернета.

Ограничьте регистрации пользователей

Если ваши сотрудники могут регистрироваться на корпоративной IP АТС прямо из сети интернет (что рекомендуется только с использованием защищенного канала VPN), не принимайте сообщения о регистрации REGISTER с любого IP-адреса без необходимости. Вам следует ограничить список IP-адресов, с которых могут регистрироваться сотрудники. Настоятельно рекомендуется использовать для доступа к корпоративной сети VoIP защищенную сеть VPN.

Например, для Asterisk: строки "*permit=" and "deny=*" для пользователей в файле sip.conf

Если все же вы вынуждены открыть регистрацию для заранее неизвестного списка IP-адресов, используйте *Set "alwaysauthreject=yes"* в файле sip.conf. Это позволит избежать «утечки» информации о пользователях. Опция yes позволяет отклонять запросы об аутентификации для существующих пользователей с такой же причиной, как и для несуществующих. Таким образом, атакующий не сможет определить существующих на IP АТС пользователей, и вероятность получить доступ к пользователю перебором паролей существенно снижается.

Используйте сложные пароли из случайных чисел

Использование простых паролей, например , «0000», «12345» или его отсутствие, является наиболее частой причиной взлома учетных записей пользователей. Простые пароли легко угадать. Используйте программы для генерирования паролей, например, Pwgen. Рекомендуется использовать пароли, содержащие не менее 12 символов и включающие цифры, буквы в нижнем и верхнем регистре.

Рекомендуется ограничить число одновременных вызовов для учетных записей

Если злоумышленник сумеет получить доступ к учетной записи, количество одновременных вызовов на учетную запись будет ограничено. Тогда он меньше «назвонит» до момента, когда будет обнаружен.

Используйте имена пользователей (Username) отличные от имени для аутентификации AuthorizationID (если такая возможность есть на клиентской АТС)

Это затруднит злоумышленнику доступ к учетной записи. Ведь он не знает не только пароль, но и AuthorizationID пользователя

Разрешайте зоновые, междугородние и международные вызовы только тем пользователям, которым необходимо звонить по этим направлениям

В случае взлома или хищения информации об учетных записях пользователей, вероятность совершения дорогих вызовов снижается.

Используйте уведомления о лимитах

Если ваша IP АТС или оператор связи позволяют включить сервис, уведомляющий о превышении установленного лимита по счёту для пользователя или канала междугородних и международных вызовов за определенное время, обязательно проверяйте эти уведомления для своевременного предотвращения взлома.

---

3. Профилактические меры.

В качестве профилактических мер пользуйтесь следующими рекомендациями.

Логирование всех событий в системе

Используйте журналы всех событий в системе. Желательно, чтобы логи (журналы) о событиях в системе записывались удаленно. Это связано с тем, что злоумышленник, получив доступ к устройству, в частности к IP АТС, пытается скрыть свое присутствие и свои действия путем удаления всех событий из файлов журналов. Если логи будут отправляться на удаленный сервер, это затруднит или сделает невозможным для злоумышленника скрыть свое присутствие.

Ведение журналов CDR (Call Detail Record)

В журналах детализированной информации о вызовах может содержаться информация, которая укажет, что оборудование незаконно используется.

Периодически просматривайте и анализируйте журналы и статистику о вызовах

Очень полезно периодически просматривать журналы и статистику вызовов. Если ваше VoIP-оборудование используется кем-то еще, это легко обнаружить, анализируя статистику.

Регулярно обновляйте прошивки или пакеты операционной системы

Рекомендуется следить за найденными уязвимостями и ошибками для оборудования, которое вы

используете, и своевременно обновлять программное обеспечение.

Храните информацию о настройках учетных записей SIP и VoIP-транков в надежном месте

Помните, что чем больше людей имеют доступ к этой информации, тем выше вероятность того, что информация об учетной записи будет похищена и незаконно использована. Например, если учётные данные SIP-линии хранятся в электронном почтовом сообщении, то при взломе ящика эти данные могут быть похищены и использованы.

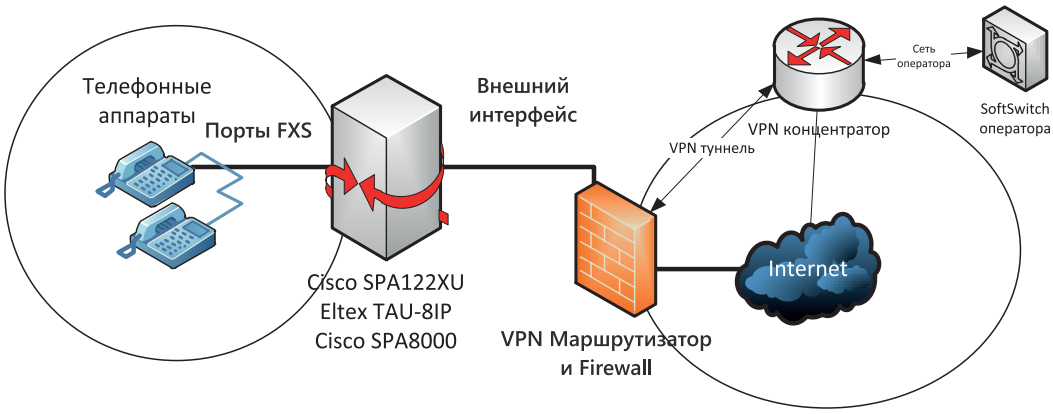
Используйте антивирусы на компьютерах и серверах, где установлены программные телефоны или IP АТС

Вирусы, черви или трояны могут находить данные учетных записей SIP на компьютерах пользователей и передавать её злоумышленнику или незаметно звонить на дорогие направления прямо с зараженного компьютера. При этом пользователь может даже не подозревать об этом.

Используйте VPN

При подключении услуг телефонии через публичные сети (интернет) настоятельно рекомендуется использовать VPN-подключение к телефонной сети оператора связи. При такой схеме подключения клиент покупает или арендует VPN-маршрутизатор, который обеспечивает надежную защиту телефонной сети клиента и высокую стабильность работы. Весь голосовой трафик и все VoIP-устройства будут скрыты внутри VPN-туннеля и не будут доступны из публичных сетей.

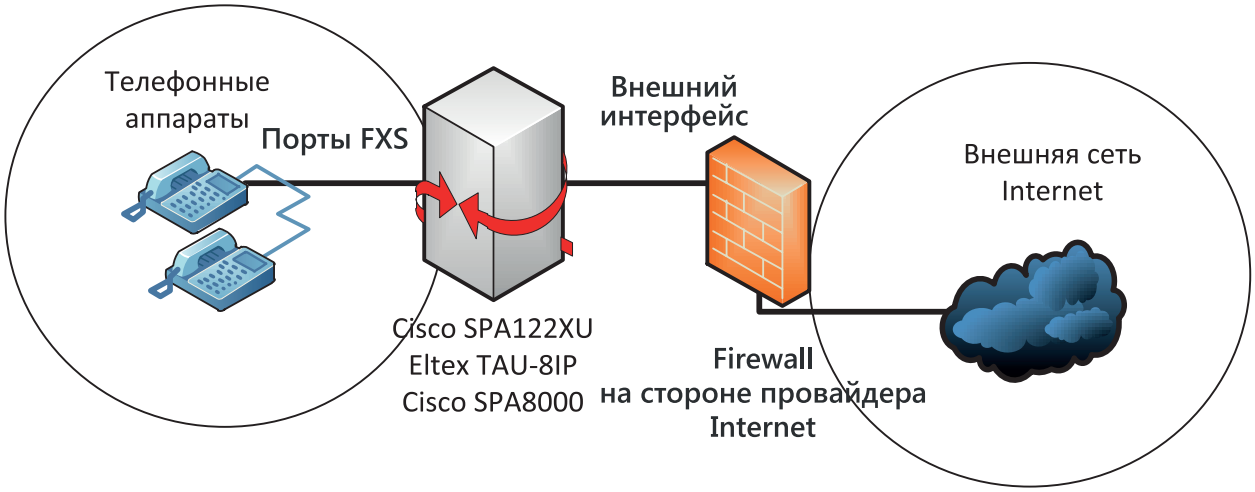
Общая схема сети:



Запрещайте доступ к оборудованию из Сети

Как показывает практика, VoIP-устройства (ATA-шлюзы, IP-телефоны и т.д.) сами по себе имеют уязвимости. Крайне не рекомендуется использовать такие устройства с внешними («белыми») IP-адреса-

ми. Если другой возможности нет или наличие внешнего IP-адреса требуется для улучшения качества работы телефонии, то требуйте от вашего провайдера услуг интернет ограничить доступ к IP-адресам телефонных устройств, разрешая только для серверов телефонии.



Используйте нестандартные порты для SIP-терминалов

Если нет возможности ограничить доступ к оборудованию из сети, настоятельно рекомендуется изменить порты SIP и управления. К примеру, шлюз Cisco SPA122XU по умолчанию использует 80/tcp для управления и 5060, 5061/udp для телефонии.
Рекомендуется изменить все порты в диапазоне 21000 – 65000. Изменение порта отсеивает до 90% атак на оборудование телефонии.

Используйте преимущество статического IP-адреса

Если провайдер интернет предоставляет статический внешний IP-адрес, рекомендуется сообщить об этом оператору IP-телефонии для установки ограничения использования услуги только с этого IP-адреса. Это ограничит возможность пользования телефонией при получении зло умышленниками данных учетной записи SIP (логин, пароль, IP-адрес для регистрации). Обычно такое происходит при взломе почтового ящика, куда были отправлены настройки SIP, при взломе IP-АТС, или другого SIP-терминала, где пароль хранится недостаточно надежно.

Не подключайте услуги международной связи без необходимости

Если вы не совершаете звонков за пределы РФ, попросите оператора связи запретить международные вызовы. Это максимально обезопасит и вас, и оператора от возможных финансовых потерь. На сегодняшний день многие операторы связи позволяют своим клиентам самостоятельно выбирать разрешенные телефонные направления, используя, например, личный кабинет.

Подытоживая, хотим обратить ваше внимание на то, что в связи с постоянным развитием технологий, как со стороны злоумышленников, так и со стороны провайдеров, указанные меры могут быть дополнены иными способами защиты, а применение всех или части из указанных мер не сводит вероятность воздействия на ваше оборудование со стороны злоумышленников к нулю.