ливается DLP-система, контролируемая из специально созданного центра компетенций. Головной филиал разрабатывает единую политику информационной безопасности компании и инструкции для всех филиалов. Отделы информационной безопасности на местах внедряют политику ИБ и проводят работу с пользователями. В свою очередь центр компетенций ведет аналитическую работу и формирует критерии перехвата DLP-системы и информирует о возникающих инцидентах и нарушениях как филиал, где возник инцидент, так и центр. Для качественного внедрения DLP в распределенной компании необходимо обладать комплексными данными о работе филиалов, их технической оснащенности, наличии подразделений по информационной безопасности на местах и о качестве каналов связи (рис. 5).

Вариантов решений по защите конфиденциальной информации от утечки в распределенных компаниях много, они отличаются и технически, и по ценовому фактору. Следует помнить, что внедрение DLP-системы, особенно в распределенной сети, — процесс сложный и многоуровневый, влияющий на бизнес-процессы компании. Процедуру внедрения можно значительно ускорить и упростить, если правильно к ней подготовиться: уточнить архитектуру системы, составить карту сети с учетом оборудования, улучшить качество каналов связи и разобраться, какие конкретные задачи в компании должна решать DLP-система.

*Александр Александрович СУХАНОВ*
*pr@mfisoft.ru*

# Как эффективно бороться со взломом абонентов сетей VoIP

**А.С. ИВАНОВ, специалист отдела развития и продаж ООО "НТЦ СевенТест"**

Тенденции последних лет, связанные с интенсивным развитием технологии широкополосного доступа, характеризуются не только появлением новых видов услуг, но и заставляют операторов акцентироваться на совершенствовании методов защиты от фрода. На сегодняшний день достаточно уязвимыми для атак злоумышленников являются сети VoIP. По последним данным, предоставляемым ассоциацией по борьбе с мошенничеством CFCA, фрод в сетях данного типа является причиной значительных финансовых потерь для операторов связи.

Для получения несанкционированного доступа к услугам сети VoIP злоумышленники активно применяют следующие методы:

взлом IP-АТС;

взлом VoIP-шлюзов;

взлом терминального оборудования абонентов SIP.

Во всех случаях мошенники активно пользуются услугами связи за чужой счет или автоматически генерируют звонки по наиболее дорогим междугородным и международным направлениям. Поскольку изначально VoIP-решения ориентировались в основном на бизнес-сегмент, то наиболее часто жертвами злоумышленников становились крупные корпоративные клиенты оператора. Однако высокие темпы распространения и удешевления услуг широкополосного доступа привели к активному использованию технологии VoIP обычными абонентами.

По этой причине, помимо получения нелегального доступа к корпоративным IP-АТС, в последнее время участились случаи "взлома" VoIP-оборудования физических лиц. "Взломав" большое количество таких абонентов, мошенники получают доходы, сопоставимые с атаками на корпоративных клиентов.

Как правило, пострадавшие абоненты отказываются оплачивать счета за услуги, которыми они не пользовались, а дальнейшие судебные разбирательства складываются в основном не в пользу операторов связи.

В результате операторы вынуждены самостоятельно покрывать ущерб от взлома, что отрицательно влияет на их финансовые показатели. В случае значительных финансовых потерь от фрода у компании не только снижается инвестиционная привлекательность, но и "падает" имидж в глазах абонентов. Поэтому операторам необходимо уделять проблеме мошенничества в сетях VoIP особое внимание.

## Борьба со взломом

Поскольку мошенники постоянно совершенствуют методы получения нелегального доступа к сетям VoIP, то ни один из операторов не может быть стопроцентно защищен от их атак. В такой ситуации необходимы специализированные информационные системы, позволяющие своевременно обнаруживать и блокировать источники нелегального трафика.

Решить поставленную задачу позволяет система противодействия мошенничеству в сетях связи СПАЙДЕР-FMS, которая обладает следующими возможностями:

автоматическое обнаружение мошенничества;

пресечение новых попыток нелегального доступа лиц, однажды уличенных в мошенничестве;

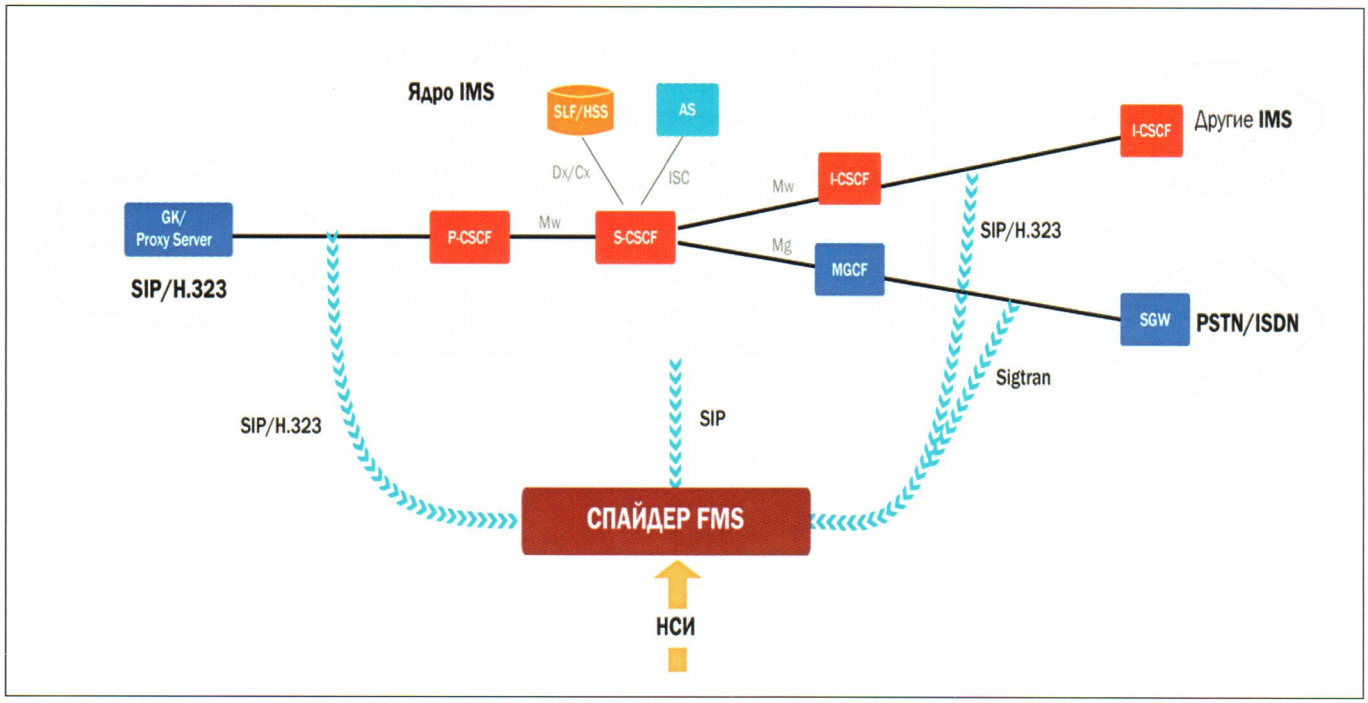


**Схема подключения СПАЙДЕР-FMS к сети VoIP**

предоставление полной информации по источникам, типам и числу попыток совершения мошенничества.

Основным источником данных для системы являются записи xDR, формирующиеся в режиме реального времени на основе сигнальной информации.

Анализ сигнальной информации осуществляется пробниками, которые подключаются к исследуемой сети пассивно и не оказывают влияния на ее работу.

Использование пробников позволяет зафиксировать данные для 100 % вызовов, включая неуспешные попытки, что значительно повышает эффективность обнаружения фрода.

На рисунке представлена схема подключения системы к сети VoIP. Такая схема дает возможность малым количеством пробников контролировать всех абонентов оператора.

Проверяя входные данные на соответствие встроенным профилям поведения абонентов, система в режиме реального времени выявляет аномалии в активности пользователей сети и заблаговременно информирует об этом оператора, формируя записи о нарушениях.

Профиль представляет собой набор простых или сложных критериев, позволяющий создавать модель аномального поведения абонента (группы абонентов, пула номеров и т. п.) во время одного вызова или в течение заданного интервала времени.

Разные группы абонентов могут проверяться на соответствие разным профилям, в том числе и нескольким.

## Методики обнаружения взлома

Для эффективного выявления фактов взлома в системе применяется несколько методик, по каждой из которых можно независимо обнаружить возникшие аномалии. Для повышения вероятности обнаружения взлома рекомендуется применять данные методики совместно.

Первая методика основана на прямых фрод-критериях, которые используются в профилях аномального поведения абонентов.

В качестве таких критериев применяются различные параметры, которыми можно охарактеризовать взлом в сетях VoIP (высокая интенсивность вызовов, большая длительность отдельных фаз соединения и др.).

Фрод-критерии также могут содержать “черные” и “белые” списки абонентов, которым запрещен или разрешен доступ к услугам связи.

Для работы в сетях VoIP в системе имеется список преднастроенных профилей, созданных на основе прямых фрод-критериев. Имеется также гибкий инструментарий, который позволяет создать собственные профили или кастомизировать существующие под конкретные требования.

Вторая методика основана на статическом и динамическом профилировании абонентов. Данная функция позволяет задать объемы потребляемых услуг, которые являются стандартными для абонента. При статическом профилировании пользователь системы сам задает эти значения, в случае динамического профилирования допустимые значения автоматически вычисляются системой на основании собранной статистики.

В обоих вариантах система круглосуточно отслеживает объемы услуг, которые потребляются абонентом, и в случае выхода этих объемов за пределы заданных значений немедленно генерирует запись о нарушении.

Третий метод основан на выявлении звонков на номера повышенной стоимости (PRS). Обнаружение таких номеров осуществляется по результатам анализа списка тарифных зон оператора связи, в рамках которого выявляются направления, отличающиеся повышенной стоимостью в пределах контролируемого региона. Данные направления добавляются системой в "черные" списки и автоматически попадают под мониторинг.

## Дополнительные возможности

Применение общих правил, описывающих нарушения, к большим объемам данных приводит к появлению ложных срабатываний. Для минимизации количества ложных нарушений и выделения из их числа наиболее вероятных случаев фрода в системе применяются следующие методы:

использование информации из внешних источников данных, которые могут представлять собой как независимые информационные системы (система биллинга, CRM), так и отдельные локальные справочники (абонентской информации, "черные" и "белые" списки и т. д.);

применение технологии CASE-Management, которая заключается в группировке нарушений, имеющих одинаковые значения определенных полей (например, номер А или номер Б). Нарушения группируются в дела, в которых отображается количество срабатываний, поле группировки и т. д. Данная методика позволяет выделить источники и типы трафика с наибольшим объемом фрода. Таким образом осуществляется приоритизация обработки нарушений, а также анализируется история по источнику трафика. Существует возможность закрепить дело за любым пользователем, который будет им заниматься.

По факту обнаруженного нарушения предусмотрена возможность отправки e-mail или SMS, генерация уведомления для блокировки источника нелегального трафика, а также выполнение других действий в зависимости от задач, стоящих перед операторами.

*Андрей Сергеевич ИВАНОВ*
*a.ivanov@seventest.ru*