ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 621.391

МЕТОДИКА РАНЖИРОВАНИЯ УГРОЗ ФРОДА И DoS В СИСТЕМЕ SIP, ОСНОВАННАЯ НА МЕТОДАХ АНАЛИЗА ИЕРАРХИЙ И АНАЛИЗА ПАР

В.А. Матвеев, руководитель НТК факультета ИУ, заведующий кафедрой «Информационная безопасность» МГТУ им. Н.Э. Баумана, д.т.н., проф.; v.a.matveev@bmstu.ru

А.М. Морозов, ведущий инженер отдела управления сетями коммутации межрегионального филиала «Москва» ОАО «Ростелеком»; a.m.morozov@gmail.com

Р.А. Бельфер, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, с.н.с., к.т.н.; a.belfer@yandex.ru

Предложена методика расчета уровней угроз фрода и DoS в находящейся в эксплуатации системе SIP оператора связи, основанная на методах анализа иерархий (Analytic Hierarchy Process, AHP) и анализа пар (Set Pairs Analysis, SPA). В расчетах по этой методике, как и по предложенным авторами двум другим методикам (*см. «ЭС» № 6, 2014, с. 35),* учитываются уровни защищенности от угроз безопасности. Эти значения определяются по результатам тестирования с имитацией угроз на действующей сети оператора связи.

Ключевые слова: *информационная безопасность, сеть программного коммутатора (Softswitch Network), программный коммутатор, гибкий коммутатор, метод анализа иерархий, метод анализа пар, фрод, протокол установления сеансов (SIP), уровень риска угрозы, сети связи нового поколения (NGN), угроза, «отказ в обслуживании», передача голоса по IP-сетям (VoIP).*

Введение. В работе [1] авторов настоящей статьи предложены две методики оценки уровней угроз безопасности фрода и DoS в системе сигнализации SIP, действующей на сети VoIP. Достоверные результаты ранжирования угроз безопасности по уровню (степени) риска позволяют повысить информационную безопасность (ИБ) системы SIP, если предпринять первоочередные меры по защите от угроз с наиболее высоким уровнем риска безопасности. Расчеты по этим методикам ранжирования угроз предусматривают использование субъективного экспертного метода.

Одна из этих методик ранжирования угроз (назовем ее методикой 1 ранжирования угроз безопасности по уровню риска, или просто методикой 1 ранжирования угроз) основана на теории нечетких множеств и нечеткой логики. Она включает экспертные данные, свойственные этому математическому аппарату, а также экспертные данные характеристик вероятности реализации угрозы и ущерба при реализации, по которым производится расчет уровня риска угроз. Проведенный в [2] анализ показал высокую вероятность недостоверной оценки уровней угроз безопасности в зависимости от состава экспертных данных математического аппарата методики 1 ранжирования угроз. При этом экспертные данные вероятности реализации угрозы и ущерба от ее реализации оставались неизменными.

Предложенная в работе [1] другая методика ранжирования угроз (назовем ее методикой 2 ранжирования угроз безопасности, или просто методикой 2 ранжирования угроз) для получения значения уровня угрозы безопасности не предусматривает никакого математического аппарата, кроме экспертного метода. Сравнить эти две методики ранжирования по достоверности результатов оценки уровней угроз безопасности не представляется возможным, так как в них используются экспертные данные различных характеристик.

В настоящей работе для оценки уровней безопасности угроз фрода в системе SIP рассматривается методика 3 ранжирования угроз безопасности, основанная на другом математическом аппарате — методах анализа иерархий (Analytic Hierarchy Process, AHP) и анализа пар (Set Pairs Analysis, SPA). Этот математический аппарат предложен специалистами лаборатории Пекинского университета связи [3] для оценки уровня риска угроз безопасности DoS в сетях с использованием программного коммутатора (некоторые исследователи называют его также гибким коммутатором, или Softswitch). Программный коммутатор обеспечивает подключение систем сигнализации различных протоколов (SIP/SIP-T, H.248 и др.) через сеть IP. Далее для упрощения такую сеть будем называть сетью программного коммутатора (Softswitch Network), как это принято в [3].

Актуальность работы. Необходимость повышения ИБ системы SIP, находящейся в эксплуатации на сетях операторов связи общего пользования (ССОП), покажем на примере угрозы фрода.

Опыт эксплуатации VoIP по протоколу SIP свидетельствует, что риск ИБ от многих угроз остается высоким. Так, например, согласно данным Ассоциации по контролю за мошенничеством (фродом) (Communication Fraud Control Association, CFCA) за 2013 г., ежегодная доля потерь дохода 8,8% операторов сетей превышает 10% [4], причем доля потерь только от специфичных для VoIP угроз фрода составляет 8%. Если принять во внимание, что эти данные не учитывают многие угрозы фрода в SIP, характерные для других технологий сетей, ежегодные потери дохода операторов могут быть значительно выше. CFCA к таким видам фрода относит: мошенничество с подпиской, фрод дилера, перехват или кража подписки, фрод распределения дохода между операторами страны и между операторами разных стран, использование техническим персоналом доступной ему служебной информации с целью мошенничества и др.

В сборе данных за 2011 г. принимали участие 25,9% операторов связи из Западной Европы и 1,7% из России [5]; в 2013 г. в опросе участвовали 31,9% западноевропейских операторов, а по России данных нет. Поэтому так актуальны исследования, нацеленные на повышение ИБ системы SIP, находящейся в эксплуатации на сети связи РФ. Решить эту задачу помогает установление уровней риска

угроз безопасности в сетях, при этом требуется определить угрозы с наибольшим уровнем риска безопасности, что дает возможность принять первоочередные меры по повышению защищенности системы SIP.

Анализ методики ранжирования угроз безопасности на основе методов AHP и SPA в сети программного коммутатора. Проведем анализ методики 3 ранжирования угроз безопасности в сети программного коммутатора на основе AHP и SPA, используемой в работе [3] применительно к угрозам DoS.

Математический аппарат AHP и SPA при ранжировании угроз безопасности так же, как и в методиках ранжирования 1 и 2, использует субъективные экспертные данные. Основная задача достоверного ранжирования угроз в системе SIP заключается в определении слабых мест с точки зрения достоверности используемых экспертных данных и, по возможности, в принятии мер к устранению этих недостатков. Определим такие недостатки методики на основе методов AHP и SPA, чтобы использовать основные положения работы [3] для достоверного ранжирования угроз фрода и DoS находящейся в эксплуатации системы SIP. Рассмотрим также положительные стороны с точки зрения достоверности экспертных данных этой методики, позволяющие использовать их в ранее разработанных для SIP методиках 1 и 2 и, наоборот, реализовать положительные стороны методик 1 и 2 в планируемой методике 3 ранжирования угроз для SIP.

Алгоритм ранжирования угроз DoS в сети программного коммутатора на основе AHP и SPA [3] построен следующим образом: экспертным методом формируются количественные характеристики принятых показателей потерь при функционировании сети. По полученным при эксплуатации данным этих показателей эксперты оценивают их уровень. В качестве примера в [3] приводятся 14 различных показателей потерь, представляющих нижний уровень иерархии AHP и отражающих время задержки в сети, процент задержанных и потерянных сообщений, возможность предоставления услуги в сети или отсутствие такой возможности**.** Эти данные являются косвенными показателями функционирования системы SIP при воздействии угроз безопасности, что отрицательно сказывается на достоверности ранжирования угроз. Метод парных сравнений SPA предусматривает сравнение экспертным методом этих показателей различной размерности по степени важности.

Использование методами анализа AHP и SPA таких экспертных данных для получения достаточно достоверных результатов ранжирования угроз безопасности в системе SIP требует очень высокой компетенции экспертов. Для более достоверного ранжирования угроз фрода и DoS в системе SIP при использовании методов анализа AHP и SPA предлагается устранить эти недостатки на этапе построения иерархической модели последствий угроз. Устранение другого недостатка связано с необходимостью проведения тестирования на действующей системе SIP оператора связи с имитацией угроз безопасности для получения достаточно достоверных экспертных данных уровня защищенности от угроз фрода и DoS. Эти данные в методике ранжирования угроз в системе SIP на основе методов анализа AHP и SPA должны учитываться при использовании в расчетах экспертных характеристик уровней потерь от этих угроз [3].

В работе [1] для использования в системе SIP основных положений методик ранжирования угроз для сети группы стандартов IEEE 802.11 [6] и услуги интеллектуальной сети связи UPT [7] также отмечается необходимость проведения тестирования на действующей системе SIP оператора связи с имитацией угроз безопасности. Экспертные данные уровня защищенности от угроз в методиках 1 и 2 ранжирования угроз фрода и DoS в системе SIP соответственно на основе теории нечетких множеств и нечеткой логики и на основе только экспертного метода должны учитываться при определении экспертами характеристик вероятности реализации угрозы. Примеры такого тестирования на системе SIP, находящейся в эксплуатации на сети одного из операторов связи РФ, приведены в [8–10]. Метод расчета значений уровней защищенности от угроз по результатам тестирования с имитацией угроз в системе SIP в настоящей работе не рассматривается.

Рассмотрим дифференцированный подход к ранжированию угроз по типам. Методика ранжирования угроз в сети программного коммутатора на основе методов AHP и SPA предназначена для ранжирования угроз безопасности только DoS. С одной стороны, это является ограничением. В [3] рассматривается ранжирование лишь одного типа угроз — DoS. С другой стороны, такой подход позволяет более достоверно сравнивать уровни типов угроз безопасности, имеющих одинаковую размерность значений ущерба. Для системы SIP при использовании методов AHP и SPA мы предлагаем отдельно ранжировать угрозы фрода и DoS. В результате получаем значения одинаковой размерности: для фрода — финансовый ущерб, для DoS это может быть, например, отказ выполнять функцию по установлению соединений для определенного числа пользователей (или доли/процента от числа пользователей). При условии доработки методик ранжирования 1 и 2 для системы SIP также может быть использован дифференцированный подход к ранжированию угроз по типам, т.е. отдельно для фрода и для DoS.

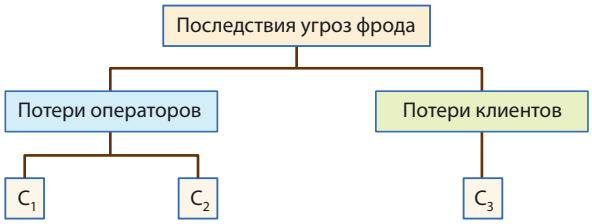
Особенности алгоритма ранжирования угроз фрода и DoS в системе SIP. Покажем, каким образом основные положения методики ранжирования угроз DoS в сети программного коммутатора [3] могут быть использованы в предлагаемой методике 3 ранжирования угроз фрода и DoS в системе SIP [11, 12].

Алгоритм вычисления уровня угроз безопасности в системе SIP с использованием методов AHP и SPA включает два основных этапа [3]:

1. Структуризация задачи в виде иерархической модели AHP с несколькими уровнями.
2. Определение степени связи двух множеств с помощью SPA.

Особенности структуризации задачи в виде иерархической модели AHP. На этом этапе последствия от реализации угроз фрода и DoS выражаются значениями одинаковой размерности. В иерархической модели последствий угроз фрода (рисунок) на верхнем уровне приводится глобальная характеристика последствий угроз фрода, на промежуточном — разделение последствий угроз фрода на потери оператора и потери клиента. Нижний уровень характеризует следующие потери:

- финансовые потери оператора без учета потерь из-за оттока клиентов C_1;
- финансовые потери оператора из-за оттока клиентов к другому оператору C_2. Такое решение клиент принимает при низком показателе качества обслуживания (Quality of Experience, QoE), который показывает, удовлетворен ли пользователь различными характеристиками обслуживания сети оператора при ее эксплуатации. Речь в QoE идет об интегральной характеристике качества обслуживания (integrity of the service) — этот обобщенный показатель вос-



Иерархическая модель последствий угроз фрода

приятия пользователем качества обслуживания оператором сети состоит из нескольких показателей (задержка, джиттер и др.). К числу таких характеристик обслуживания сети относится и обеспечение информационной безопасности — в данном случае характеристики угроз фрода;

- финансовые потери клиентов C_3.

Иерархическая модель последствий угроз DoS отличается только значениями потерь, которые могут выражаться, например, в отказе выполнять функцию по установлению соединений для определенного числа пользователей.

Особенности определения степени связи двух множеств с помощью SPA. Принятая иерархическая модель последствий угроз фрода и DoS одинаковой размерности дает возможность составить более достоверные экспертные данные матриц важности показателей последствий угроз безопасности.

Полученные в результате расчета ранги каждой из анализируемых угроз, выраженные максимальными значениями мощности связи [3], необходимо привести к уровням угроз ИБ. С этой целью для каждого уровня требуется установить диапазон значений максимальной мощности.

Заключение. Предложенная методика, основанная на методах анализа иерархий (AHP) и анализа пар (SPA), может быть использована для оценки уровня угроз фрода и DoS в системе SIP, действующей на сети оператора связи РФ. Сравнить ее с двумя другими методиками, приведенными в [1], по достоверности результатов оценки уровней угроз безопасности не представляется возможным, так как в расчетах каждой из них используются экспертные данные различных характеристик. Авторы считают возможным применение любой из трех предложенных методик — выбор зависит, в частности, от компетенции специалиста в области получения экспертных данных.

Необходимым условием практического применения предложенных методик является проведение расчетов, в которых должны учитываться значения уровней защищенности от угроз, полученные при тестировании с имитацией угроз на действующей сети оператора связи. Для этого необходимо разработать метод тестирования с целью получения уровней защиты от анализируемых угроз фрода и DoS в системе SIP, стенды тестирования для имитации угроз фрода и DoS в системе SIP оператора связи, метод анализа результатов тестирования.

ЛИТЕРАТУРА

1. **Матвеев В.А., Морозов А.М., Бельфер Р.А.** Оценка уровня риска угрозы безопасности фрода в сети VoIP по протоколу SIP // Электросвязь.— 2014.— № 6.— С. 35–39.
2. **Бельфер Р.А., Калюжный Д.А., Тарасова Д.В.** Анализ зависимости уровня риска угроз безопасности сетей связи от экспертных данных при расчетах с использованием теории нечетких множеств //Вопросы кибербезопасности.— 2014.— № 1 (2).— С. 61–67.
3. **Yao Jiang, KangFeng Zheng.** Evaluation Model for DoS Attack Effect in Softswitch Network /International Conference on Communications and Intelligence Information Security, 2010.— P. 88–91.
4. Communications Fraud Control Association (CFCA). 2013 Global Fraud Loss Survey.— Электронный ресурс: www.cfca.org.
5. Communications Fraud Control Association (CFCA). 2011 Global Fraud Loss Survey.— Электронный ресурс: www.cfca.org.
6. **Щербаков В.Б., Ермаков С.А.** Безопасность беспроводных сетей: стандарт IEEE 802.11.— М.: РадиоСофт, 2010.— 255 с.
7. ETSI ETR 083. Universal Personal Telecommunication (UPT); General UPT security architecture, 1993.
8. **Морозов А.М.** Анализ уязвимостей сети SIP к угрозам фрода // Электросвязь.— 2013.— № 7.— С. 10–13.
9. **Матвеев В.А., Морозов А.М.** Анализ результатов испытаний действующей сети нового поколения NGN на уязвимость к атакам DoS //Вестник МГТУ им. Н.Э. Баумана, сер. «Приборостроение».— 2013.— Вып. № 5 «Информатика и системы управления».— С. 43–57.
10. **Морозов А.М.** Анализ уязвимостей сети VoIP на базе NGN к угрозам нелегитимных сигнальных и медиасообщений //Электросвязь.— 2013.— № 4.— С. 33–35.
11. **Sisalem D.** [and others]. SIP security.— N.Y. Wiley, 2009.— 355 p.
12. **Матвеев В.А., Морозов А.М., Бельфер Р.А.** Фрод и угрозы в сети IP-телефонии по протоколу SIP //Вестник МГТУ им. Н.Э. Баумана, сер. «Приборостроение».— 2012.— Спец. вып. № 5 «Информатика и системы управления».— С. 236–248.

Получено 15.06.14

ИНФОРМАЦИЯ

«РОСТЕЛЕКОМ» ПОСТРОИТ 200 КМ ОПТИКИ В 24 СЕЛАХ СТАВРОПОЛЬЯ

В ходе встречи руководства «Ростелекома» с временно исполняющим обязанности губернатора Ставропольского края **В. Владимировым** был дан старт строительству ВОЛС в хуторе Фельдмаршальский Новоалександровского района. Присутствующим были продемонстрированы возможности компании по обеспечению жителей села современными услугами связи: метод горизонтально-направленного бурения при прокладке линии под автодорогой, лаборатория для «варки» оптоволокна и др.

«В начале июня 2014 г. правительство края и «Ростелеком» подписали соглашение о развитии телеком-инфраструктуры в регионе. И мы уверены, что наше партнерство с «Ростелекомом», в том числе в проекте по устранению «цифрового неравенства», окажет положительное влияние на социально-экономическое развитие края. А всем его жителям — как в больших городах, так и на селе — даст возможность беспрепятственно пользоваться государственными и муниципальными услугами, ресурсами Интернета, предоставит доступ к современному контенту»,— отметил В. Владимиров.

По мнению вице-президента ОАО «Ростелеком», директора макрорегионального филиала «Юг» **А. Шипулина**, строительство современной телекоммуникационной сети в сельской местности — это не только инфраструктурный проект, но и огромная социальная составляющая. Все развитые страны стремятся уравнять права граждан в доступе к инфокоммуникационным ресурсам, и мы — не исключение.

Только на Ставрополье в 2014 г. предстоит провести 200 км оптики в 24 села. Без преувеличения это — важнейший для России проект. Не менее масштабные работы ведутся в других субъектах ЮФО и СКФО.