**Долгов Александр Иванович**
Ростовский военный институт ракетных войск.
E-mail: dolgov-ai@yandex.ru.
344037, г. Ростов-на-Дону, пр. М. Нагибина, 24/50.
Тел.: +79054392081.

**Кладовой Игорь Игоревич**
E-mail: Little 0504@mail.ru.

**Мартыненко Анатолий Федорович**
E-mail: rvirv@aanet.ru.

**Преснухин Вячеслав Валерьевич**
E-mail: rvirv@aanet.ru.

**Dolgov Aleksandr Ivanovich**
Rostov Military Institute of Rocket Troops.
E-mail: dolgov-ai@yandex.ru.
24/50, M. Nagibina pr., Rostov-on-Don, 344037, Russia.
Phone: +79054392081.

**Kladovoy Igor' Igorevich**
E-mail: Little 0504@mail.ru.

**Presnukhin Vajcheslav Valerievich**
E-mail: rvirv@aanet.ru.

**Martinenko Anatoliy Fedorovich**
E-mail: rvirv@aanet.ru.

УДК 004.056

**Н.В. Рубцов**

## ПРИМЕНЕНИЕ МЕТОДА АНАЛИЗА ИЕРАРХИЙ ДЛЯ ОЦЕНКИ УЯЗВИМОСТЕЙ В СИСТЕМАХ IP-ТЕЛЕФОНИИ

*В данный момент для оценки уязвимостей используются методы, имеющие общий характер и не учитывающие характерные особенности IP-телефонии или приоритеты организации-владельца. В качестве альтернативы предлагается использование метода анализа иерархий как инструмента для оценки уязвимостей в системах IP-телефонии. Приводятся рекомендации по выбору критериев оценки характерных для рассматриваемых систем и процессу оценки в целом.*

*Уязвимость; IP-телефония; SIP; метод анализа иерархий; информационная безопасность; оценка уязвимостей.*

**N.V. Rubtsov**

## USAGE OF ANALYTIC HIERARCHY PROCESS IN VULNERABILITY SCORING PROCESS FOR IP-TELEPHONY SYSTEMS

*At present methods, which are used for vulnerability estimation have the general nature and not considering characteristic features of IP-telephony or priorities of the owner organization. Alternatively, usage of analytic hierarchy process as a tool for vulnerability estimation in IP-telephony systems is offered. Recommendations choice of estimation criteria that are characteristic for considered systems are and whole estimation process are given.*

*Vulnerability; IP-telephony; SIP; analytic hierarchy process; information security; vulnerability estimation.*

В современном мире IP-телефония все чаще заменяет собой классическую телефонную связь. Использование сетей передачи данных зачастую дешевле и проще чем монтаж новых телефонных линий. Но адаптация сетей IP-телефонии на базе протокола SIP ставит перед IT-подразделением организации вопрос об определении уровня безопасности. Особенно актуальной становится процедура поиска и оценки уязвимостей в используемых системах.

Уязвимость – это ошибка, недостаток, слабость или дефект приложения, системы, устройства или службы, который может привести к нарушению конфиденциальности, целостности или доступности [1].

Процедура оценки позволяет определить степень опасности каждой из уязвимостей. Полученные в результате данные могут быть использованы как для последующей процедуры оценки рисков, так и для расстановки приоритетов в последующей работе по устранению существующих уязвимостей. Существующие методики носят общий характер и не учитывают особенностей рассматриваемой в статье области. Еще одно необходимое требование – учет сложившейся ситуации, с целью получения оценки, адекватной текущему состоянию системы.

Оценка уязвимости должна быть рассчитана на основании множества критериев, включающих в себя как результат эксплуатации рассматриваемой слабости системы защиты, так и ее технические характеристики. Описываемый процесс можно рассматривать как процедуру многокриетриального выбора, результатом которой будет являться система приоритетов или оценок. В данном случае возможно использование одного из методов многокритериального выбора – метода анализа иерархий. Данный метод, основанный на представлении поставленной задачи в виде иерархической структуры и попарном сравнении ее элементов, был разработан Т. Саати [2].

Суть метода состоит в попарной оценке нижестоящих элементов по отношению к вышестоящему элементу иерархии. Оценка производится экспертом или группой экспертов – лицами, принимающими решения (ЛПР). Для сравнения используется специально разработанная шкала отношений, приведенная в табл. 1 [2].

Таблица 1

**Шкала отношений Т. Саати [2]**

| Степень важности | Определение | Объяснение |
|---|---|---|
| 1 | Одинаковая значимость | Два действия вносят одинаковый вклад в достижение цели |
| 3 | Некоторое преобладание значимости одного действия перед другим (слабая значимость) | Опыт и суждение дают лёгкое предпочтение одному действию перед другим |
| 5 | Существенная или сильная значимость | Опыт и суждение дают сильное предпочтение одному действию перед другим |
| 7 | Очень сильная или очевидная значимость | Предпочтение одного действия перед другим очень сильно. Его превосходство практически явно |
| 9 | Абсолютная значимость | Свидетельство в пользу предпочтения одного действия другому в высшей степени предпочтительны |
| 2, 4, 6, 8 | Промежуточные значения между соседними значениями шкалы | Ситуация, когда необходимо компромиссное решение |

Результаты попарного сравнения величин вносятся в матрицу парных сравнений. Затем в каждой строке матрицы определяется относительная важность конкретного элемента по отношению к вышестоящему критерию. После нормализации полученных значений получается конечный результат. Конечные результаты используются для получения приоритетов всех альтернатив.

Применительно к рассматриваемой области необходимо определить, какие параметры занимают определенные места иерархии, так как оценка производится с целью определения относительного уровня опасности каждой из уязвимостей. Таким образом верхнюю ступень иерархии должна занимать цель «Уровень опасности». По результатам оценки уязвимость, имеющая наибольший приоритет, должна признаваться самой опасной и работы по ее устранению должны начаться в первую очередь.

Процесс оценки подразумевает, что в качестве альтернатив выступают сами уязвимости. По результатам исследования существующих уязвимостей и анализа уже сложившихся стандартов оценки предлагается использовать в качестве критериев 1-го уровня следующие параметры уязвимости:

- критерии влияние эксплуатации уязвимости на систему;
- технические критерии;
- критерии устранения уязвимости.

Влияние эксплуатации уязвимостей на систему может быть определено 3 отдельными критериями: влиянием на конфиденциальность, целостность и доступность. В данном случае преимущество метода анализа иерархий состоит в субъективности выставляемой оценки. Производя попарные сравнения для данных критериев, ЛПР или группа ЛПР выставляет значения в соответствии с реальной ситуацией и приоритетами организации.

Технические критерии должны включать в себя как можно более полную характеристику уязвимости в соответствии с особенностями их эксплуатации. Именно в данной группе критериев должна проявляться специфика IP-телефонии. Для уязвимостей систем на базе протокола SIP в данный список можно включить также такие параметры, как: необходимость использования атак типа «Man-in-the-middle» (человек посередине), необходимость использования известной SIP-серверу учетной записи пользователя, используется при атаке отправка запросов только серверу или напрямую пользователю, необходимость наличия на сервере слабых политик маршрутизации SIP-запросов и другие. Список технических критериев этого уровня может динамически изменяться в зависимости от списка анализируемых уязвимостей.

Группа критерий устранения уязвимости в первую очередь может включать в себя такие параметры, как время простоя сервиса, необходимое для устранения (данный параметр зачастую является критичным как для IP-телефонии, так и для других сервисов связи), источник информации о способе устранения и другие. Например, при попарном сравнении альтернатив уязвимость, для устранения которой используется неофициальное решение, будет иметь больший вес, чем уязвимость, для устранения которой используется официальное обновление от разработчика. При сравнении следует учитывать, что уязвимость информации, по устранению которой на данный момент организация не имеет, будет иметь максимальный приоритет по данной группе критериев.

Таким образом, при оценке существующих в системе уязвимостей следует руководствоваться следующими положениями:

1) необходимо четко определять цели и критерии на каждом уровне иерархии;

2) важно верно задавать вопрос при каждом попарном сравнении. В данном случае вопрос, скорее всего, будет иметь форму «Какая из уязвимостей опаснее относительно данного критерия?»;
3) необходимо как можно более полно составить перечень значащих критериев для данного списка, которые будут использоваться при оценке;
4) при построении иерархии следует особое внимание уделять группе технических критериев и особенностям эксплуатации существующих в системе уязвимостей. Данный подход позволит провести оценку с учетом большего числа характерных черт IP-телефонии;
5) чем полнее информация об уязвимостях, тем лучше результат оценки будет описывать текущее состояние системы.

Таким образом, использование метода анализа иерархий при оценке уязвимостей позволяет:

- получить более специфичную и точную оценку, в частности для рассматриваемой области IP-телефонии;
- вследствие субъективности процесса получить оценку, более соответствующую приоритетам и требованиям организации, осуществляющей контроль и управление системой IP-телефонии.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Mell P., Scarfone K., Romanosky S.* CVSS. A Complete Guide to the Common Vulnerability Scoring System. Version 2.0. [Электронный ресурс]/ P. Mell, K. Scarfone, S. Romanoskyю – Режим доступа: http: //www.first.org/cvss/cvss-guide.html. Дата обращения: 11.12.2009.
2. *Саати Т.Г.* Принятие решений. Метод анализа иерархий / Т.Г. Саати; пер. с англ. Р.Г. Вачнадзе. – М.: Радио и связь, 1993. – 320 с.
3. *Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M., Schooler E.* RFC 3261. SIP: Session Initiation Protocol [Электронный ресурс]/ J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler – Режим доступа: http://tools.ietf.org/html/rfc3261. Дата обращения 11.12.2009.

**Рубцов Никита Вячеславович**
Ижевский государственный технический университет.
E-mail: nikizzzz@gmail.com.
426069, г. Ижевск, ул. Студенческая, д. 7.
Тел.: 83412585358.

**Rubtsov Nikita Vyacheslavovich**
Izhevsk State Technical University.
E-mail: nikizzzz@gmail.com.
7, Studencheskaya street, Ijevsk, 426069, Russia.
Phone: +73412585358.

УДК 629.78.05

**Ю.А. Геложе, П.П. Клименко, А.В. Максимов**

## ИССЛЕДОВАНИЕ ПЕРЕХОДНЫХ ПРОЦЕССОВ В НЕЛИНЕЙНОМ АВТОПИЛОТЕ

*Настоящая работа посвящена исследованию процессов управления в нелинейной автоматической системе управления во время больших возмущений.*

*Автопилот; управление; крен.*