System analysis and synthesis directions for large telescope deformable construction with control elements are considered. The research is based on standards modeling programs.

Key words: control, large telescope, analysis, synthesis, deformable construction.

УДК 004.056

Н. В. Рубцов, аспирант, Ижевский государственный технический университет имени М. Т. Калашникова

КРИТЕРИИ ОЦЕНКИ УЯЗВИМОСТЕЙ В СИСТЕМАХ IP-ТЕЛЕФОНИИ

Оценка уязвимостей в системах IP-телефонии требует системы критериев, предоставляющих возможность гибкой оценки и определения явных различий для специфических уязвимостей данной области. Автором предложена система критериев и методика их применения, удовлетворяющие данным требованиям.

Ключевые слова: уязвимость, IP-телефония, информационная безопасность, информационные система, оценка уязвимостей.

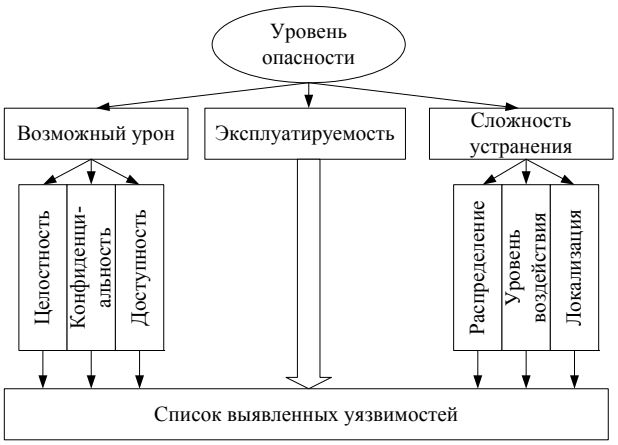
Повышение уровня безопасности любой информационной системы включает в себя следующие этапы: поиск существующих уязвимостей, оценка обнаруженных уязвимостей и принятие мер по отношению к найденным уязвимостям. В данной статье будет рассмотрен метод оценки выявленных в системе уязвимостей.

Уязвимость – это ошибка, недостаток, слабость или дефект приложения, системы, устройства или службы, который может привести к нарушению конфиденциальности, целостности или доступности [1]. Оценка уязвимости представляет собой процесс изучения и ранжирования (приоритезации) уязвимости с целью повышения эффективности и снижения затрат на работы по поднятию уровня безопасности и устранению уязвимостей системы.

Системы IP-телефонии, так же как и другие информационные системы, в ходе аудита безопасности могут быть подвергнуты процедуре оценки уязвимостей. После рассмотрения общих методов оценки уязвимостей возникает вопрос о получении более гибкой и точно соответствующей ситуации оценки. Это связано не только со спецификой уязвимостей сетей и приложений IP-телефонии, но и с различиями в приоритетах разных организаций. С этой целью предлагается альтернативный метод оценки уязвимостей, основанный на методе анализа иерархий [2]. Данный метод легко позволяет автоматизировать обработку результатов оценок экспертов. Для использования метода анализа иерархий была разработана система критериев, представленная на рисунке.

Возможный урон целостности, конфиденциальности и доступности в результате эксплуатации уязвимости оценивается экспертно посредством сравнения результатов отдельных атак на систему для различных уязвимостей.

Параметр «уровень воздействия уязвимости» определяет, имеет ли место уязвимость на аппаратном, программном или уровне настройки системы. Зачастую определить уровень воздействия уязвимости может быть сложно, поэтому при оценке следует руководствоваться типом вмешательства в систему, требуемым для устранения уязвимости. Уязвимость может быть устранена посредством внесения изменений в аппаратную или программную структуру системы, а также изменением настроек системы. Нередки случаи, когда уязвимость может быть устранена различными типами изменений. В этом случае для оценки используется допустимый вариант с наименьшей оценкой. Для сравнения уязвимостей по данному критерию используется табл. 1.



Система критериев для оценки уязвимостей

Таблица 1. **Таблица оценки отношений важности по критерию «уровень воздействия»**

	H	*S*	*C*
H	1	1/5	1/9
S	5	1	1/5
C	9	5	1

H – уязвимости на аппаратном уровне; *S* – уязвимости на программном уровне; *C* – уязвимости на уровне настройки.

Распределение уязвимых объектов в сети определяется процентом уязвимых объектов от всех сетевых объектов сети (в расчет берутся серверы, клиентские рабочие станции, шлюзы, регистраторы,

Получено 28.11.11

прокси-серверы и т. д.). Использование данного критерия связано с трудоемкостью устранения уязвимости на большом количестве узлов. Отношение может быть вычислено следующим образом:

$$Q = \frac{P_{V1}}{P_{V2}},$$

где P_{V1}, P_{V2} – количеств узлов (объектов) сети, подверженных уязвимостям V_1 и V_2 соответственно. Оценка рассчитывается исходя из того, что $V_1 > V_2$. В случае если это не верно, применяется обратное отношение. Полученный результат парного сравнения Q округляется до ближайшего целого. В случае если $Q > 9$, значение принимается $Q = 9$.

Локализация уязвимости – критерий, характеризующий, где была локализована уязвимость. Определяет, требует ли устранение уязвимости вмешательства в настройки, программное или аппаратное обеспечение на стороне клиента или на стороне сервера и серверного оборудования. Возможны ситуации, когда полное устранение уязвимости требует принятия мер и на сервере, и на стороне клиента. Наилучшим образом данный критерий характеризуется как простой сервиса голосовой связи. Для оценки используется табл. 2.

Таблица 2. **Таблица оценки отношений важности по критерию «локализация уязвимости»**

	C	*S*	*B*
C	1	1/5	1/9
S	5	1	1/5
B	9	5	1

C – уязвимость устраняется вмешательством на стороне клиента; *S* – уязвимость устраняется вмешательством на стороне сервера и серверного оборудования; *B* – для устранения уязвимости требуется вмешательство как на стороне сервера, так и на стороне некоторых клиентов.

Эксплуатируемость уязвимости – критерий, определяющий знания, включая знания о структуре конкретной системы, умения и техническое обеспечение, доступные злоумышленнику, минимально необходимые для эксплуатации оцениваемой уязвимости. В случае если отсутствует адекватная сложившейся ситуации модель злоумышленника, возможно предположение о доступности злоумышленнику всех необходимых навыков, умений и технических средств. Таким образом, относительная эксплуатируемость V_{exi} определяется как

$$V_{exi} = \begin{cases} V_{ex1} = \ldots = V_{exi-1} = V_{exi+1} = \ldots = V_{exn} = 1/n, \\ \qquad\qquad\qquad\qquad \text{если } M = 1, \\ V_{\exp i}, \qquad\qquad\qquad \text{если } M = 0, \end{cases}$$

где M – логическая величина, принимающая истинное значение при допущении о максимально возможных обеспечении ресурсами и квалификации злоумышленника, и ложное – во всех остальных случаях; величина V_{expi} – относительная эксплуатируемости уязвимости, полученная путем экспертной оценки на основе разработанной в организации модели злоумышленника.

Возможный урон от эксплуатации уязвимости предлагается определять исходя из приоритетов организации на основе важности отдельных аспектов безопасности: целостности, конфиденциальности и доступности.

Сложность устранения уязвимости оценивается на основе сравнения критериев уровня воздействия, локализации уязвимости и распределения уязвимых объектов в сети. Данные критерии при оценке следует понимать в контексте технической сложности устранения, простоя сервиса или его элементов и сложности, связанной с географическим распределением уязвимых узлов.

Критерии первого уровня – эксплуатируемость, сложность устранения и возможный урон от уязвимости – зачастую имеют равную значимость. Тем не менее по решению оценивающего эксперта или группы экспертов могут быть установлены различные приоритеты.

Данная система критериев предоставляет достаточный уровень гибкости и адекватности при оценке уязвимостей, что позволяет более рационально распределять ресурсы на этапе принятия мер.

Библиографические ссылки

1. *Mell P.*, *Scarfone K.*, *Romanosky S.* CVSS. A Complete Guide to the Common Vulnerability Scoring System. Version 2.0. – URL: http://www.first.org/cvss/cvss-guide.html (дата обращения: 10.11.2011).

2. *Саати Т. Л.* Принятие решений. Метод анализа иерархий : пер. с англ. Р. Г. Вачнадзе. – М. : Радио и связь, 1993. – 320 с. : ил.

N. V. Rubtsov, Postgraduate Student, Kalashnikov Izhevsk State Technical University

IP-Telephony Vulnerability Rating Criteria

Vulnerability rating in IP-telephony systems requires existence of the flexible criteria system, which is capable of detecting differences between specific VoIP vulnerabilities. Author offers the criteria system and their application method that fulfill above mentioned requirements.

Key words: vulnerability, IP-telephony, information security, information system, vulnerabilities rating.