УДК 004.056

Н.В. Рубцов

ВЛИЯНИЕ МОДЕЛИ ЗЛОУМЫШЛЕННИКА НА ПРОЦЕСС ОЦЕНКИ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Оценка уровня опасности уязвимостей позволяет оптимизировать процесс их устранения и снизить материальные затраты. Существующие методы ранжирования уязвимостей не всегда могут быть адаптированы к сложившейся на практике ситуации. Как один из альтернативных методов оценки уязвимостей, выявленных в информационной системе, может быть использован метод анализа иерархий. Данный метод требует создания системы критериев оценки. Предлагается обратиться к модели злоумышленника для упрощения данного процесса, и в некоторых случаях, снижения временных затрат.

Уязвимость; информационная безопасность; оценка уязвимостей; информационная система; модель злоумышленника; метод анализа иерархий.

N.V. Rubtsov

INFLUENCE OF MALICIOUS USER MODEL ON INFORMATIONAL SYSTEM VULNERABILITY SCORING PROCESS

Vulnerability danger level scoring allows optimizing process of their elimination and to lower expenses. Existing methods of vulnerability estimation not always can be adapted for current practical situation. Analytic hierarchy process may be used as one of the alternative scoring methods for vulnerabilities, which have been found in informational system. This method demands building a criterion scoring system. It is proposed to address the malicious user model in order to simplify building process and reduce time costs.

Vulnerability; information security; vulnerability estimation; informational system; malicious user model; analytic hierarchy process.

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

Оценка уязвимостей является важной процедурой, исполняемой в процессе оценки уровня защищенности информационной системы. Результаты оценки также оказывают существенное влияние на выбор средств обеспечения информационной безопасности и менеджмент безопасности в целом.

Входные данные для процесса оценки опасности уязвимостей информационной системы определяются следующими параметрами:

- список уязвимостей $V=\{v_1, v_2, \dots, v_n\}$;
- относительная сложность устранения для каждой уязвимости $V_{Pd}=\{V_{Pd1}, V_{Pd2}, \dots, V_{Pdn}\}$;
- возможный урон информационной системе в результате эксплуатации уязвимости $V_{Dm}=\{V_{Dm1}, V_{Dm2}, \dots, V_{Dmn}\}$;
- относительная сложность эксплуатации уязвимости $V_{Ex}=\{V_{Ex1}, V_{Ex2},\dots, V_{Exn}\}$.

Таким образом, формальная модель процесса имеет вид, представленный на рис. 1.

Данная модель позволяет провести сравнительную оценку выявленных уязвимостей, целью которой будет определить: какие из уязвимостей требуют наибольших материальных и временных затрат для устранения, могут нанести наибольший потенциальный урон системе, являются наиболее простыми в эксплуатации и часто используемыми. Для этого может быть использован метод анализа иерархий [3].

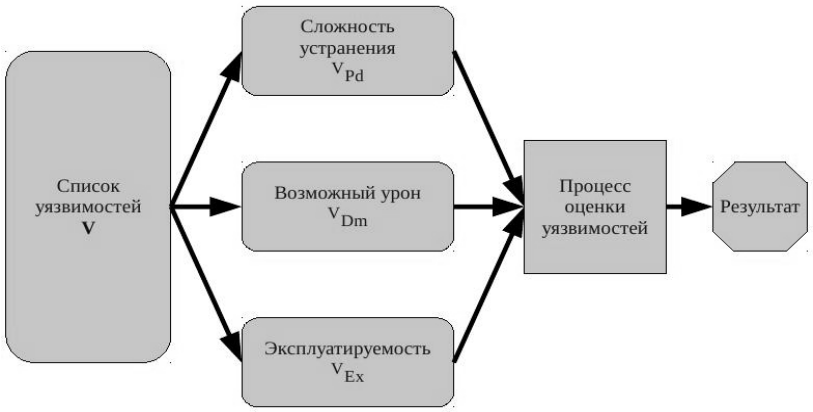

Рис. 1. Схема получения оценки опасности уязвимостей

Метод анализа иерархий подразумевает объединение сравниваемых альтернатив и выбранных критериев сравнения в древовидную структуру с конечной целью анализа в корне. Альтернативы и критерии попарно сравниваются друг с другом группой экспертов по отношению к критериям вышестоящего уровня. При этом критерии первого уровня сравниваются друг с другом относительно цели. Результаты сравнения объединяются. Значения, полученные путем применения метода анализа иерархий, описывают влияние альтернатив на цель. Его применение позволяет не только получить конечную относительную оценку для каждой из уязвимостей, но и адаптировать ее в соответствии с нуждами и приоритетами организации. Недостатком применения данного метода являются значительные временные и вычислительные затраты на расчет с участием экспертов при значительном количестве альтернатив.

В соответствии с моделью, применяя метод анализа иерархий, относительный уровень опасности для каждой из уязвимостей определяется по формуле

$$V_{Gi} = V_{Dmi} \times G_{Dm} + V_{Pdi} \times G_{Pd} + V_{Exi} \times G_{Ex}, \quad (1)$$

где G_{Dm}, G_{Pd}, G_{Ex} – относительный уровень влияния параметров возможного урона, сложности устранения и эксплуатируемости уязвимостей на итоговые значения опасности для каждой уязвимости. Итоговые значения удовлетворяют условию

$$V_{G1} + V_{G2} + \ldots + V_{Gn} = 1. \quad (2)$$

Указанные параметры, в соответствии с методом анализа иерархий, определяются путем экспертной оценки.

Перечисленные выше относительные уровни определяются классами дочерних параметров, различными для каждого из них. Таким образом, представленные на схеме группы включают в себя перечни входных параметров. Так, для группы V, перечнем входных параметров будет являться перечень обнаруженных и не устраненных на момент оценки уязвимостей.

Сложность процесса оценки состоит в необходимости определения данных групп входных параметров, достаточно полно характеризующих каждый из аспектов уязвимости.

Особенный интерес представляет группа входных параметров V_{Ed} – относительная эксплуатируемость уязвимости. Данная группа входных параметров описывает требования к злоумышленнику, предпринимающему попытку эксплуата-

ции конкретной уязвимости. Представив описание группы в виде такой формулировки, можно сделать вывод, что процесс оценки уязвимости в аспекте ее эксплуатируемости также можно свести к процессу оценки возможностей злоумышленника. То есть эксплуатируемость уязвимости напрямую связана с возможностями злоумышленника во время данного процесса.

Построение модели злоумышленника требует классифицировать возможного нарушителя по статусу относительно информационной системы [2]. Анализ статуса злоумышленника позволяет составить список характеризующих его параметров. Данный список может включать в себя:

- положение злоумышленника по отношению к защищаемой системе: внутренний или внешний;
- квалификация или профессиональный уровень злоумышленника;
- обеспечение злоумышленника ресурсами (время также является ресурсом при рассмотрении некоторых уязвимостей);
- возможности доступа злоумышленника по отношению к информационной системе;
- объем информации о системе, которая может быть доступна злоумышленнику (количества внутренних объектов системы, версии установленного программного обеспечения и т.д.);
- цель злоумышленника (остановка работы сервиса, хищение данных, подмена данных и т.д.).

При оценке эксплуатируемости уязвимости может быть использована группа входных параметров, аналогичная вышеперечисленной для модели злоумышленника:

- необходимость воздействия изнутри системы или возможность эксплуатации уязвимости извне;
- требования к профессиональным навыкам и знаниям нарушителя эксплуатирующего уязвимость: определенный класс атак может быть реализован посредством запуска программы-эксплойта, в то время как эксплуатация некоторых уязвимостей требует от нарушителя реакции «на лету» и дополнительных знаний о использующихся протоколах безопасности и связи;
- требования к ресурсам доступным нарушителю: в случае если система уязвима к атакам вызывающим отказ в обслуживании, эксплуатация данной уязвимости требует от злоумышленника определенных технических ресурсов, таких как вычислительная мощность процессора атакующей рабочей станции, объем оперативной памяти или пропускная способность канала связи. Данные ресурсы должны находиться в определенном минимальном соотношении с ресурсами аппаратных узлов информационной системы. В случае распределенной атаки с отказом в обслуживании ресурсом также является количество рабочих станции находящихся под управлением злоумышленника;
- необходимость обладать определенными правами доступа к информационной системе;
- необходимость в обладании определенной информацией о системе: методах взаимодействия объектов системы между собой, адресах отдельных аппаратных узлов сети и т.д.

Особое место в данной модели злоумышленника занимает цель нарушителя. Как таковой, данный параметр не оказывает прямого влияния на эксплуатируемость уязвимости, тем не менее влияет на конечный уровень опасности уязвимости. Это связано с характером воздействия на систему: определенные конечные цели могут быть достигнуты лишь с помощью эксплуатации определенных уязвимостей.

Перечисленные выше параметры напрямую определяются характеристиками уязвимости, т.е. могут быть использованы как входные в процессе оценки уязвимостей информационной системы. В частности, как указано выше, если в модели нарушителя были определены возможные цели, опасность соответствующих уязвимостей, позволяющих их достичь, повышается.

В процессе составления модели нарушителя в некоторых ситуациях разумным представляется допущение о более обеспеченном ресурсами и опытном нарушителе, для повышения уровня безопасности в системе. Данное допущение оказывает также влияние и на процесс оценки.

Исходя из предположения, об обладании злоумышленником всеми необходимыми знаниями и необходимыми ресурсами, можно сделать вывод о равенстве для потенциального нарушителя относительной эксплуатируемости всех выявленных уязвимостей:

$$V_{Exi} = \begin{cases} V_{Ex1} = \ldots = V_{Exi-1} = V_{Exi+1} = \ldots = V_{Exn} = 1/n, \text{ если } M = 1 \\ V_{Exi-\exp}, \text{ если } M = 0, \end{cases} \quad (3)$$

где M – логическая величина принимающая истинное значение при допущении о максимально возможных обеспечении ресурсами и квалификации злоумышленника, и ложное – во всех остальных случаях. Величина $V_{Edi\text{-}exp}$ – относительная эксплуатируемости уязвимости, полученная путем экспертной оценки по методу анализа иерархий.

Составление модели злоумышленника и ее последующее применение в процессе оценки уязвимости позволяет:

- сократить временные затраты на процесс составления иерархической модели критериев оценки уязвимостей;
- получить модель, адекватную ситуации, а также хранимой и обрабатываемой в системе информации, относительно возможной заинтересованности нарушителя;
- значительно уменьшить количество временных и вычислительных ресурсов, необходимых для расчета относительной эксплуатируемости выявленных уязвимостей.

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. *Завгородний В.И.* Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.
3. *Саати Т. Г.* Принятие решений. Метод анализа иерархий / Т.Г. Саати: Пер. с англ. Р.Г. Вачнадзе. – М.: Радио и связь, 1993. – 320 с.

Статью рекомендовал к опубликованию д.т.н., профессор А.В. Боженюк.

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

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