Использование современных программно-аппаратных средств разработки и проектирования, таких, как LabView позволяет автоматизировать данный процесс, а также выборочно заменять математические модели реальными элементами. Применение интегральные методов анализа элементов измерительного канала температуры на базе NTC терморезисторов при проектировании ИС позволяет ускорить процесс разработки, улучшить метрологические характеристики, а также находить наиболее эффективные, с точки зрения соотношения точность/сложность решения задачи проектирования измерительного канала температуры ИС.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Шишмарев В.Ю.* Электрорадиоизмерения: Учебник для сред. проф. образования / В.Ю. Шишмарев, В.И. Шанин. – М.: Издательский центр «Академия», 2004. – 336 с.
2. Прецизионные интеллектуальные тензометрические датчики давления. Методы, модели, алгоритмы и архитектуры / Пьявченко О.Н. [и др.] / Под ред. д.т.н. профессора О.Н. Пьявченко. – Таганрог: Изд-во ЮФУ, 2009. – 152 с.
3. *Мэклин Э.Д.* Терморезисторы: Пер. с англ. / Под общей ред. К.И. Мартюшова. – М.: Радио и связь, 1983. – 208 с.
4. *Беляев А.О.* Схемотехнические методы линеаризации температурных характеристик NTC терморезисторов. Пассивные корректирующие цепи // Известия ЮФУ. Технические науки. – 2009. – № 2 (91). – С. 112-119.

Статью рекомендовал к опубликованию д.т.н., профессор А.Е. Панич.

Беляев Алексей Олегович
Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: alexys@pisem.net.
347900, г. Таганрог, ул. Петровская, 81.
Тел.: 88634328052.

Belyaev Alexey Olegovich
Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: alexys@pisem.net.
81, Petrovskaya Street, Taganrog, 347900, Russia.
Тел.: +78634328052.

УДК 004.021

В.В. Борисов

АНАЛИЗ СТЕПЕНИ УЯЗВИМОСТИ ВИРТУАЛЬНЫХ СООБЩЕСТВ НА БАЗЕ ИНФОРМАЦИИ О КОЛИЧЕСТВЕ И ТИПАХ НАЙДЕННЫХ УЯЗВИМОСТЕЙ

Представлен алгоритм определения степени уязвимости виртуальных сообществ. Синтез алгоритма защиты информации в веб-ресурсе реализуется на базе методики анализа информационных рисков, которая впервые примененная для сайтов виртуальных сообществ. Разрабатываемый алгоритм определения степени уязвимости веб-ресурсов предоставляет возможность незамедлительного практического руководства по устранению выявленных недостатков. Предложенный алгоритм позволяет дать экспертную оценку степени уязвимости анализируемого веб-ресурса на базе информации о количестве и типах найденных уязвимостей.

Виртуальное сообщество; информационная безопасность; алгоритм; экспертная оценка; уязвимость; веб-ресурс.

V.V. Borisov

ANALYSIS OF INFORMATION SECURITY LEVEL FOR VIRTUAL SOCIETIES BASED ON TYPE AND NUMBER OF VULNERABILITIES FOUND

The paper presented an algorithm for determining the level of vulnerability for virtual communities. Synthesis of algorithm of a guard of the information in a web- resource is realized on the basis of a technique of the analysis of informational risks, which for the first time applied to sites of virtual communities. The developed algorithm of definition of extent of vulnerability of web-resources gives possibility of the immediate code of practice on elimination of the revealed lacks. The proposed algorithm can give an expert assessment of the vulnerability of the analyzed web-resource-based information on the number and types of vulnerabilities found.

Virtual society; security; algorithm; expert assessment; vulnerability; web-site.

В современной научной лексике фигурируют такие термины, как "virtual community" (виртуальное сообщество), указывающий на виртуальный характер агрегации людей в киберпространстве; "on-line community" (онлайновое сообщество, сообщество "на связи") указывает на интерактивность общения и взаимодействия людей в киберпространстве в реальном времени. Основным понятием здесь является понятие "community", означающее "сообщество".

Понятие "коммьюнити" (community) до массового использования сети Интернет рассматривалось в первую очередь как "территориальная общность". Однако слово "общность" имеет много оттенков значений и поэтому почти невозможно дать точное определение этого понятия. Таким образом, можно сделать вывод о том, что "коммьюнити" – один из наиболее расплывчатых гуманитарных терминов, который, по сути, до сегодняшнего дня так и не приобрел точного значения.

Очень часто в научных работах термин "коммьюнити" пересекается с термином "коммуникация". Сам термин "коммуникация" в первую очередь рассматривается как организация с помощью информационных средств социально-культурного и экономического взаимодействия людей, групп, организации, предприятии, государств и регионов. Таким образом, понятие коммуникация тесно связано с понятием коммьюнити – вида общности людей, выражающееся в объединении их в группах, сообществах для совместной жизни и деятельности.

Корректная оценка защищенности виртуальных сообществ необходима для сравнения аналогичных по назначению и уровню сложности систем и для мониторинга динамики уровня защищенности конкретной информационной системы во времени. Кроме того, разрабатываемый алгоритм определения степени уязвимости веб-ресурсов предоставляет возможность незамедлительного практического руководства по устранению выявленных недостатков.

Поскольку исходная информация для алгоритма представляет собой многопараметрические данные, полученные инструментальным путем, алгоритм определения степени уязвимости имеет нелинейный характер. Можно ли, например, оценить как не слишком опасную уязвимость, которая потенциально может помочь запустить чрезвычайно опасную вредоносную программу?

По этой причине в алгоритме должны быть учтены зависимости механизмов реализации уязвимостей друг от друга. С другой стороны, результирующая функция является одномерной – это степень уязвимости веб-ресурса. Таким образом, необходимо преобразование множества не всегда четко определенных данных в некоторую одномерную шкалу, понятную обычному пользователю.

Такое преобразование возможно определить, например, если каждая найденная уязвимость будет иметь стоимостную характеристику. Однако полученный показатель будет характеризовать лишь опасность уязвимых звеньев. Необходимо

также учитывать степень противодействия существующим уязвимостям с помощью эксплуатируемых систем защиты информации. Данный показатель будет определять степень влияния уязвимостей на веб-ресурс.

Третьим направлением оценки является сам ресурс – точнее, степень критичности потерь от его взлома и совершения с ним несанкционированных действий. Веб-ресурс можно разделить на несколько существенных частей, которые будут оцениваться самим пользователем по принципу "насколько важно, чтобы это работало всегда". При таком подходе, алгоритм определения степени уязвимости является интерактивным, но при этом пользователь не вовлекается в технологические особенности сканирования.

Определим все составляющие алгоритма. Так, для анализа веб-ресурса, представим его в виде следующих частей:

- администраторской веб-консоли (значение критичности раздела обозначим как $U_{console}$);
- система удаленного управления (в нее входит SSH, Telnet, FTP и прочие службы, которые отвечают за удаленное управление процессами и файлами, значение критичности обозначим как U_{remote});
- база данных, в которой хранится информация веб-ресурса (значение критичности обозначим как U_{db});
- система вывода информации веб-браузеру пользователя (значение критичности обозначим как U_{cms});
- система приема он-лайн платежей (в случае, если это Интернет-магазин, значение критичности – $U_{payment}$);
- модуль журналирования запросов и действий операторов и пользователей (критичность U_{log});
- система резервного копирования данных (U_{backup}).

Значение критичности каждого раздела (например, $U_{console}$) задается с помощью баллов – числами от 1 до 10 самим пользователем. Таким образом, эта оценка носит экспертный характер и определяет наиболее важные, с точки зрения пользователя (т.е. с точки зрения функционирования самого веб-ресурса), места.

Средства защиты информации, которые эксплуатируются на веб-ресурсе, аналогично разделам веб-ресурса можно разделить на несколько типов и дать им соответствующие обозначения:

- межсетевой экран (обозначим через $P_{firewall}$);
- штатные системы защиты операционной системы (система разграничения доступа к файлам, процессам и памяти – обозначим через P_{access});
- система разграничения доступа по сети (включая консоль администрирования – обозначим через P_{remote});
- антивирусная защита (обозначим через $P_{antivirus}$);
- система обнаружения компьютерных атак и защиты сетевых портов (обозначим через P_{ids});
- система анализа контрольных сумм файлов и контроля резервного копирования (обозначим через P_{tamper});
- система журналирования и анализа действий пользователей и операторов (обозначим через $P_{log\ ging}$);

- система распределения нагрузки и защиты от атак на отказ в обслуживании (обозначим через P_{ddos});
- система контроля работоспособности служб и оповещения администратора (обозначим через P_{sentry}).

На основе существующих материалов и исследований [1-2] разработана оценка критичности (важности) для веб-ресурса систем защиты информации. Для оценки использовались баллы в пределах от 1 до 10. Дополнительно оценивалась роль взаимной работы (например, межсетевого экрана и система распределения нагрузки и защиты от атак на отказ в обслуживании).

После того, как будет собрана информация о количестве и типах найденных на веб-сервере уязвимостей, следует оценить уязвимость веб-ресурса и для этого в разработанном алгоритме также используются баллы. Обозначим начисленные баллы к уязвимости с номером k из некоторого перечня через E_k.

Обобщая все определения, перед собственно выполнением алгоритма определения степени уязвимости, необходимо собрать и оценить следующую информацию:

- информацию о самом веб-ресурсе (баллы критичности разделов ресурса);
- оценка системы защиты (баллы критичности для веб-ресурса систем защиты информации);
- перечень действительных уязвимостей программных средств и конфигураций веб-ресурса (баллы уязвимостей).

Баллы критичности разделов ресурса и баллы, начисленные за найденные уязвимости в каждом из разделов, составляют вместе "баллы уязвимости" ресурса (для каждого раздела баллы уязвимости подсчитываются отдельно и умножаются на "важность" раздела):

$$S_{exploit} = U_{console} \sum_{k \in K(console)} E_k + U_{remote} \sum_{k \in K(remote)} E_k + U_{db} \sum_{k \in K(db)} E_k + U_{cms} \sum_{k \in K(cms)} E_k +$$
$$+ U_{payment} \sum_{k \in K(payment)} E_k + U_{\log} \sum_{k \in K(\log)} E_k + U_{backup} \sum_{k \in K(backup)} E_k .$$

Используя обозначенные выше определения и таблицы значений можно представить алгоритм определения степени уязвимости на базе информации о количестве и типах найденных уязвимостей как последовательность следующих шагов:

1. Получить от пользователя описание тестируемого веб-ресурса. На основе этого описания и экспертного решения пользователя составить таблицу "значимости разделов" для ресурса.
2. На основе информации пользователя осуществить оценку критичности систем защиты информации для веб-ресурса (уточнить количество и тип эксплуатируемых систем защиты информации), составить перечень применяемых средств защиты информации.
3. Вычислить "баллы защиты".
4. Провести автоматическое сканирование веб-ресурса с целью выявления уязвимостей.
5. Оценить найденные уязвимости по 10 бальной шкале. Вычислить максимальное значение баллов. Вычислить сумму баллов по всем уязвимостям.
6. Ранжировать результат "баллов уязвимости".

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Карпычев В.Ю., Минаев В.А.* Цена информационной безопасности // Системы безопасности. – 2003. – № 5. – С. 128-130.
2. *Климовский А.А.* К анализу подходов классификации компьютерных атак // Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. – М.: МЦНМО, 2006. – 480 с.
3. *Жижелев А.В., Панфилов А.П., Язов Ю.К., Батищев Р.В.* К оценке эффективности защиты информации в телекоммуникационных системах посредством нечетких множеств // Изв. вузов. Приборостроение. – 2003. – Т. 46, № 7. – С. 22-29.
4. *Никифоров С.В.* Введение в сетевые технологии. – М.: Финансы и статистика, 2003. – 224 с.
5. *Девянин П. Н. и др.* Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000.

Статью рекомендовал к опубликованию д.т.н., профессор Е.А. Башков.

Борисов Владимир Владимирович
Научно-исследовательский институт «Спецвузавтоматика».
E-mail: author@nosecure.info.
344002, г. Ростов-на-Дону, пер. Газетный, 51.
Тел.: 88632411228.

Borisov Vladimir Vladimirovich
Scientific Research Institute «Spetsvuzavtomatika».
E-mail: author@nosecure.info.
51, Gazetniy, Rostov-on-Don, 344002, Russia.
Phone: +78632411228.

УДК 519.688:[519.17+681.518]

С.Л. Беляков, Я.А. Коломийцев, И.Н.Розенберг, М.Н. Савельева

МОДЕЛЬ РЕШЕНИЯ ЗАДАЧИ МАРШРУТИЗАЦИИ В ИНТЕЛЛЕКТУАЛЬНОЙ ГЕОИНФОРМАЦИОННОЙ СИСТЕМЕ*

Статья посвящена анализу особенностей решения задачи маршрутизации с использованием интеллектуальных механизмов геоинформационных систем. В качестве базы интеллектуализации рассматривается использование оценок информационных ресурсов сообществами социальных сетей Интернет. Предлагается новая методология построения картографической основы посредством накопления опыта. Приведён алгоритм поиска кратчайшего пути, адаптированный для применения на динамических графах. Предложенный алгоритм обеспечивает получение результата для задачи маршрутизации с учетом изменений временных параметров и активности дуг, обеспечивая актуальность решения в каждый момент времени.

ГИС; пространственные данные; интеллектуальные системы; маршрутизация; алгоритм Дейкстры; динамический граф.

S.L. Beliacov Y.A. Kolomiytsev, I.N. Rozenberg, M.N. Savelyeva

MODEL FOR SOLVING ROUTING PROBLEM IN THE INTELLECTUAL GEOINFORMATION SYSTEM

Article is devoted the analysis of features of the decision of a problem of routing with use of intellectual mechanisms of geoinformation systems. As base of intellectualization use of estimations of information resources by communities of social networks the Internet is considered. The

* Работа поддержана грантом РФФИ, проект № 11-01-00011а.