Таким образом, если порядок нелинейного энергетического объекта равен трем, его уравнения удовлетворяют указанным выше условиям, а переменные состояния доступны прямому измерению с помощью датчиков, то, как показано выше, уравнения объекта можно привести к управляемой форме Жордана и сформировать стабилизирующее управление по состоянию с требуемыми свойствами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Лупкин В.М.* Анализ режимов синхронной машины методами Ляпунова. – Л.: Энергоатомиздат, 1991.
2. *Нейдорф Р.А., Соловей Н.С.* Инженерные методы синтеза автоматических систем управления: Учебное пособие / Под ред. Р.А. Нейдорфа. – Ухта: УГТУ; Ростов-на-Дону: РГАСХМ, 2004.
3. *Уткин В.А., Краснова С.А.* 20 лет блочному принципу управления // Материалы конференции «Управление в технических системах» (УТС-2010). – СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2010. – С. 74-77.
4. *Åström K.J., Wittenmark B.* Adaptive control. N.Y.: Addison-Wesley Publishing Company, 1995.
5. *Гайдук А.Р.* Синтез нелинейных систем на основе управляемой формы Жордана // Автоматика и телемеханика. – 2006. – № 7. – С. 3-13.
6. *Лукьянов А.Г., Уткин В.И.* Методы сведения уравнений динамических систем к регулярной форме // Автоматика и телемеханика. – 1981. – № 4. – С. 5-13.

Статью рекомендовал к опубликованию д.т.н., профессор А.Р. Гайдук.

Плаксиенко Елена Алексеевна
Таганрогский институт управления и экономики.
E-mail: pumkad@mail.ru.
г. Таганрог, ул. Петровская, 45.
Тел.: 88634362582.
Доцент.

Plaksienko Elena Alexeevna
Taganrog Institute of Control and Economic.
E-mail: pumkad@mail.ru.
45, Petrovskaya Street, Taganrog, Russia.
Phone: +78634362582.
Associate Professor.

УДК 004.021

В.В. Борисов

УГРОЗЫ И ИНФОРМАЦИОННЫЕ РИСКИ ВИРТУАЛЬНЫХ СООБЩЕСТВ И ИХ КОММУНИКАЦИЙ

Представлен алгоритм определения степени уязвимости виртуальных сообществ. Для этого используется методика анализа информационных рисков, впервые примененная для сайтов виртуальных сообществ. Предложенный алгоритм позволяет дать экспертную оценку степени уязвимости анализируемого веб-ресурса на базе информации о количестве и типах найденных уязвимостей. Приведены средства защиты информации, методика их использования.

Защита информации; криминалистика; веб-ресурс; угрозы; риски; информационная безопасность.

V.V. Borisov

THREATS AND INFORMATION RISKS FOR VIRTUAL SOCIETIES

The paper presents an algorithm for determining the vulnerability of virtual co-societies. For this purpose the method of analysis of information risks, first used for sites of virtual communities. The proposed algorithm allows us to give an expert assessment of the vulnerability of the analyzed web-based resource of information about the number and types of detected vulnerabilities. Shows the protection of information, methods of their use.

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

Постановка задачи исследования. 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.

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

- административной 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 (то есть, 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):

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

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".

Заключение. В работе исследуется феномен возникновения "виртуальных сообществ" с позиции оценки информационной безопасности. Для этого оценивается возможность применения методов оценки информационных рисков к понятий-

ям "виртуального сообщества" и коммуникаций, связанных с ними. Предложен алгоритм определения степени уязвимости виртуального сообщества на базе информации о количестве и типах найденных уязвимостей. Показана возможность оценки уязвимости "виртуального сообщества" на базе знаний об уязвимостях веб-ресурсов.

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 А.В. Аграновский.

Борисов Владимир Владимирович
Федеральное государственное научное учреждение научно-исследовательский институт «Спецвузавтоматика».
E-mail: borisovjojoba@gmail.com.
344007, г. Ростов-на-Дону, Газетный пер., 51.
Тел.: 88632411228.
Младший научный сотрудник.

Borisov Vladimir Vladimirovich
FGNU NII "Spetsvuzatomatika" of Ministry of Education and Science of Russian Federation.
E-mail: borisovjojoba@gmail.com.
51, Gazetny'j, Rostov-on-Don, 344007, Russia.
Phone: +78632411228.
Research Engineer.

УДК 004.021

Р.Н. Селин, С.А. Чурилов

МЕТОД ПРОГНОЗИРОВАНИЯ ВАРИАНТОВ РАЗВИТИЯ КОМПЬЮТЕРНЫХ АТАК

Представлена модель сетевых процессов и алгоритм обнаружения угроз в компьютерной сети, предназначенные для прогнозирования изменения уровня информационной безопасности в зависимости от происходящих сетевых событий. Приведена типовая структура компьютерной атаки, показана ее сложность, даны основные определения, необходимые для моделирования процесса мониторинга компьютерной сети.

Авторы предлагают новый способ моделирования механизма угроз информационной безопасности, который позволяет предугадывать различные варианты развития компьютерных атак.

Информационная безопасность; модель; сетевой процесс; уязвимость; обнаружение угроз.