· защита от копирования и нелегального распространения ПО;

· защита от реверс-инжиниринга ПО.

Планы на дальнейшее развитие:

· добавление в систему модуля профилирования выделенных в результате дизассемблирования функций;

· упрощение процесса создания новых подключаемых модулей (создание модулей на языках высокого уровня, добавление скриптового движка);

· увеличение задаваемых пользователем параметров, влияющих на процесс защиты ПО;

· добавление модулей для защиты других форматов исполняемых файлов (PE, Mach-O);

· создание удобного графического интерфейса.

СПИСОК ЛИТЕРАТУРЫ:

1. *Стивенс У. Р., Рago С. А.* UNIX. Профессиональное программирование. 2-е изд. СПб.: Символ-Плюс, 2007.
2. *Лав Р.* Разработка ядра Linux. 2-е изд. М.: ООО «И.Д. Вильямс», 2006.
3. *Щелкунов Д. А.* Разработка методик защиты программ от анализа на основе запутывания кода и данных. М.: МГТУ им. Н. Э. Баумана, 2009 (рукопись).
4. *Лившиц Ю.* Запутывание (обфускация) программ. Обзор. 2004. URL: http://logic.pdmi.ras.ru/~yura/of/survey1.pdf.
5. *Тимовский Д.* Исследование механизмов защиты от динамического анализа для ОС Linux. М.: МИФИ, 2008 (рукопись).
6. Tool Interface Standart (TIS) Executable and Linking Format (ELF) Specification Version 1.2. URL: http://www.x86.org/ftp/manuals/tools/elf.pdf.
7. *Barak B., Goldreich O., Impagliazzo R., Rudich S., Sahai A., Vadhan S., Yang K.* On the (Im)possibility of Obfuscating Programs. LNCS, 2001, 2139. P. 1–18.
8. *Collberg, Thomborson C., Townsend G. M.* Dynamic graph-based software watermarking. Technical Report TR04-08, April 2004.
9. *Lynn B., Prabhakaran M., Sahai A.* Positive Results and Techniques for Obfuscation // Eurocrypt, 2004.
10. *Varnovsky N. P. and Zakharov V. A.* On the Possibility of Provably Secure Obfuscating Programs // In Andrei Ershov Fifth International Conference. July, 2003. P. 91–102. Springer LNCS 2890, 2003.
11. *Chow S., Gu Y., Johnson H., Zakharov V.* An approach to the obfuscation of control-flow of sequential computer programs // LNCS, 2001, 2200. P. 144–155.
12. Ilo. Process Dump and Binary Reconstruction. URL: http://www.phrack.org/issues.html?issue=63&id=12#article.
13. ELFsh crew. Embedded ELF Debugging. URL: http://www.phrack.org/issues.html?issue=63&id=9#article.
14. *Vanegue J., Garnier T., Auto J., Roy S., Lesniak R.* Next generation debuggers for reverse engineering. URL: http://www.blackhat.com/presentations/bh-europe-07/ERSI/Whitepaper/bh-eu-07-ersi-WP-apr19.pdf.

М. В. Тимонин

ОПТИМИЗАЦИЯ СТРАТЕГИИ ИНВЕСТИРОВАНИЯ В СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ В МОДЕЛЯХ, ОСНОВАННЫХ НА ТЕОРИИ НЕЧЕТКОЙ МЕРЫ

Риск, связанный с информационной безопасностью (ИБ) организации, является многомерным сложным понятием, включающим множество связанных друг с другом переменных. Основой построения модели риска является его декомпозиция на логические составляющие, их оценка и агрегация информации снизу вверх для расчета величины риска. В качестве математического аппарата, позволяющего моделировать взаимосвязь между компонентами, возможно использовать

механизмы теории нечеткой меры, имеющие ряд преимуществ перед традиционно используемым вероятностным подходом [1]. В таких моделях уровень надежности той или иной части системы информационной безопасности рассчитывается с помощью интеграла Шоке на основе значений атомарных компонентов защиты, входящих в данную часть, их относительных весов и характера взаимодействия между ними.

$C_м(a_1, \ldots, a_n) = \sum^{n} (a_{(i)} - a_{(i-1)}) м(A_{(i)})$,

где $A_{(i)} = \{a_{(i)}, \ldots, a_{(n)}\}$, а $a_{(1)}, \ldots, a_{(n)}$ перестановка элементов $a_1 \ldots, a_n$, такая, что $a_{(1)} \le a_{(2)} \le \ldots \le a_{(n)}$ и $a_{(0)} = 0$.

В условиях ограниченного бюджета безопасности рациональной является стратегия инвестиции, максимизирующая значение защищенности $C_м$ при постоянном объеме вложений.

Формально задача определяется следующим образом:

максимизировать $C_м(S_1, \ldots, S_n)$

со следующими условиями, $\begin{cases} м \\ S_i = F_i(z_i) \\ \sum z_i = B \end{cases}$

где $м$ — значения нечеткой меры, B — общий бюджет вложений, S_i — значения оцениваемых критериев в зависимости от вложения z_i, F_i — функции полезности вложений, демонстрирующие, как уровень защиты, предоставляемый тем или иным компонентом, изменяется в результате вложения определенной суммы z_i, функции, очевидно, носят ступенчатый характер.

Считаем, что структура дерева риска и значения нечеткой меры $м$ известны, так же как и функции $F_i(z_i)$, а исследование фокусируется на нахождении оптимальной стратегии инвестирования $Z_{opt} = \{z_1', \ldots, z_n'\}$, максимизирующей уровень защиты $C_м$.

Для решения данной оптимизационной задачи возможно применение двух подходов — аппроксимация ступенчатых функций непрерывными и нахождение ответа средствами анализа или решение путем рассмотрения всех возможных стратегий инвестирования.

Первый подход широко применяется в экономической литературе, в том числе в статьях по экономическим факторам информационной безопасности [2]. В качестве функции полезности инвестиции возможно использовать монотонно возрастающую функцию, дважды дифференцируемую на всей области определения, что позволит проводить поиск экстремума базовыми средствами анализа. Подход, однако, не лишен недостатков, основными из которых являются сложность, погрешность, которая появляется при замене ступенчатой функции на непрерывную, и в некотором смысле отсутствие гибкости, поскольку решение зависит от конкретного вида функций, выбранных для аппроксимации.

Второй подход лишен данных недостатков, однако обладает другими, в первую очередь вычислительного характера. Обозначим через $Щ$ множество всех возможных инвестиций в атомарный компонент системы защиты, $|Щ| = k$. Множество всех наборов инвестиций в атомарные компоненты (т. е. стратегий инвестирования) мы определим как $2^{Щ} = \{Z = \{z_1, \ldots, z_n\}: z_1, \ldots, z_n \in Щ\}$. При этом число возможных стратегий равняется k^n, что представляет существенные проблемы уже при малых размерах k и n. Это число, впрочем, возможно существенно снизить, если принять во внимание условие $\sum z_i = B$, а также используя древовидную структуру разложения риска.

В докладе подробно рассматриваются оба предложенных варианта решения и предлагается алгоритм по поиску оптимальной стратегии инвестиций.

СПИСОК ЛИТЕРАТУРЫ:

1. *Тимонин М. В., Лаврентьев В. С.* Использование теории нечеткой меры для агрегации составляющих риска информационной безопасности (в печати).
2. *Gordon L. A., Loeb M. P.* The Economics of Information Security Investment // ACM Trans. Inf. Syst. Secur., 5(4): 438–457, November 2002.

К. С. Титков

О МЕТОДАХ ОБЕСПЕЧЕНИЯ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ В КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

При построении системы информационной безопасности (ИБ) в организации необходимо предпринять ряд мер по охране конфиденциальности информации (КИ), продиктованных требованиями бизнес-процессов организации и федерального законодательства. В числе прочего эти меры могут включать в себя введение режима коммерческой тайны (КТ), а значит, определение перечня и порядка обращения с информацией, составляющей эту тайну [1]. Однако, в отличие от КТ, порядок защиты профессиональной и других видов тайн не определяется законодательством столь же подробно. Разумным видится применение к прочим видам тайн требований по защите, схожих с требованиями к КТ. Решение данной задачи обеспечивается системой организационных и технических мер, основанной на внутренних нормативных документах организации. Представляется целесообразным дать обзор перечня, взаимосвязи, структуры и состава этих документов.

Для описания системы защиты требуется ввести некоторые уточнения. Во-первых, необходимо определить виды внутренних нормативных документов и упорядочить их по уровню от верхнего к нижнему. Для построения предлагаемой системы внутренних документов зачастую достаточно четырехуровневой модели, состоящей из политик, положений, регламентов и инструкций по защите информации. Во-вторых, введем более общее понятие режима конфиденциальности информации, путем включения в состав конфиденциальной информации не только КТ, но и других видов тайн в соответствии с законодательством [2]. Для целей настоящего исследования будем полагать, что конфиденциальная информация — это информация, в отношении которой организацией установлен режим конфиденциальности. При этом режим конфиденциальности — это режим, позволяющий обладателю конфиденциальной информации при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду, а режим КТ — это вид режима конфиденциальности, реализующий определенные законом [1] меры по охране конфиденциальности информации.

Таким образом, далее будет рассматриваться единая система внутренних нормативных документов коммерческой организации, поддерживающая защиту коммерческой тайны и других видов тайн.

Предлагаемые меры по поддержанию режима конфиденциальности должны вписываться в действующую политику ИБ организации, содержащую совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности [3]. На основе указанной политики, издаваемой в виде документа верхнего уровня, разрабатывается положение, определяющее режим конфиденциальности в организации.