БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Язов Ю.К.* Основы методологии количественной оценки эффективности защиты информации в компьютерных системах. – Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. – 274 с.
2. *Fishburn P.* Utility Theory for Decision-Making. N.Y., Wiley, 1970.

УДК 004.056

**В.В. Золотарев**

## МЕТОД ИССЛЕДОВАНИЯ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ КОМПОНЕНТНОЙ МОДЕЛИ ОПЕРАЦИОННОЙ СРЕДЫ*

**Введение**

Представлены результаты, обобщающие процедуру анализа внутренних характеристик средств защиты и их влияния на операционную среду. Основой подхода является выделение внутренних критериев оценки взаимодействий и оценка внутренних структур.

Особенности программного обеспечения и программно-аппаратных комплексов, применяемых для решения задач защиты информации, часто позволяют нарушать безопасность защищаемого объекта или снижать его уровень защищенности. Механизмы такого влияния связаны с реализацией средств защиты информации (СЗИ), а также с взаимным влиянием внутренних параметров СЗИ и операционной среды. Рассматривая практические подходы к такому анализу, можно отметить несколько недостатков, не позволяющих в общем случае провести полный анализ защищенности:

– использование методов анализа, базирующихся на оценке множества известных угроз и уязвимостей, не позволяющих сделать корректный прогноз существования неизвестных;

– неформализованный подход к решению большинства задач, и, как следствие, математически не доказанные факты взаимного влияния внутренних параметров СЗИ и операционной среды;

– неполные или некорректные методы извлечения информации о взаимодействии СЗИ и операционной среды, приводящие к неполным или искаженным выводам по результатам исследования.

Таким образом, постановка задачи в работе следующая: требуется сформулировать, алгоритмизировать и предварительно оценить метод исследования взаимного влияния внутренних параметров СЗИ и операционной среды.

Можно рассмотреть как единый метод исследования, так и частные методы. Далее в статье рассмотрен единый метод, который, в свою очередь, имеет дальнейшее развитие в область частных оценок.

**Общая характеристика области исследования**

Внутренние параметры средства защиты информации и операционной среды представляют собой в рамках исследования строго не определенную область, которая может быть расширена и/или детализирована. Безусловно, к параметрам средств защиты информации необходимо вне зависимости от поставленной задачи относить следующий набор характеристик:

* Работа выполнена при поддержке гранта Президента МК-3625.2007.9.

- настройки СЗИ, особенно прямо либо косвенно влияющие на функционирование;

- характеристики взаимодействия различных модулей СЗИ, в частности, доступность или недоступность определенных модулей, некорректные или неполные запросы или ответы, особенности функционирования.

В каждом случае данные параметры рекомендуется определять отдельно, с учетом условий и цели исследования.

Далее приведем пример расширения области исследования для решения конкретных задач. В табл. 1 и 2 показаны исследуемые классы внутренних параметров для задач защиты программного кода от модификации при условии использования программы в виде закрытого дистрибутива и реконфигурации виртуальной среды-носителя программного средства защиты информации, применяемой для создания виртуального лабораторного комплекса.

Таблица 1

Классы внутренних параметров при решении задачи защиты программ от модификации*

| Класс параметров | Характеристика класса | Примечания |
|---|---|---|
| Взаимодействие модулей программы | Критично в данном случае определить недоступность отдельного модуля | Свидетельствует о нарушении структуры программного кода |
| Взаимодействие с функциями API | Критично изменение или отсутствие корректного вызова функции | Свидетельствует о модификации или разрушении элемента операционной среды |
| Выполнение стандартных функций | Критично изменение или некорректный формат выходных или входных параметров | Проверяется в соответствии с документацией |
| Выполнение дополнительных защитных функций | Критично изменение или некорректный формат выходных или входных параметров | Проверяется в соответствии с документацией |
| Внутреннее взаимодействие функций программного кода | Критично изменение или недоступность функции или связей между функциями | Требуется предварительное изучение программного кода специальными средствами |

Как видно, основной задачей данной классификации внутренних параметров является детализация предметной области. В следующем случае потребовалось расширить набор внутренних параметров, как показано в табл. 2.

Как видно из приведенных таблиц, необходимо не только подробное изучение особенностей операционной среды, но и корректный выбор уровня детализации, что не всегда возможно на начальном уровне исследования. В связи с этим может потребоваться дополнительная детализация некоторых классов внутренних параметров, что потребует дополнительных временных и технических ресурсов на проведение исследования.

* Табл. 1 может быть дополнена.

Таблица 2

Классы внутренних параметров при решении задачи реконфигурации виртуальной среды-носителя**

| Класс параметров | Характеристика класса | Примечания |
|---|---|---|
| Настройки СЗИ | Критично некорректное или неполное соответствие требованиям | Проверяется в соответствии с документацией |
| Взаимодействие с функциями API | Критично изменение или отсутствие корректного вызова функции | Свидетельствует о модификации или разрушении элемента операционной среды |
| Выполнение стандартных функций | Критично изменение или некорректный формат выходных или входных параметров | Проверяется в соответствии с документацией |
| Настройка параметров конфигурации операционной системы | Критична некорректная настройка правил доступа на изменение | Применено для блокирования возможности косвенного влияния на СЗИ |
| Настройка сервисов операционной системы | Критично изменение или некорректный формат выходных данных или входных запросов | Исследуются сервисы, функционирующие в замкнутой программной среде |

**Описание метода исследования**

Для описания системы и метода исследования рассмотрим:

– множества $U_+$ известных угроз безопасности, блокированных СЗИ, $U_-$ прогнозируемых угроз безопасности, $U_?$ неизвестных угроз. Очевидно, в этом случае, что множества угроз $U_?$, $U_-$ не могут быть гарантированно блокированы СЗИ;

– множество прямых влияний $A_{пр}$, представляющих собой способы воздействия на внутренние параметры СЗИ непосредственным изменением параметров операционной среды;

– множество косвенных влияний $A_{косв}$, представляющих собой способы воздействия на внутренние параметры СЗИ через изменение параметров операционной среды косвенными методами, к примеру, нарушением внутренних связей компонентов среды;

– вектор состояния компонента множества угроз $u(f_1, f_2, ..., f_n)$, здесь $f$ – фактор состояния: 0 – параметр, влияющий на возможность угрозы, неизменяем (заблокирован), 1 – параметр, влияющий на возможность угрозы, изменяем;

– операция изменения вектора состояния компонента множества угроз $\alpha \in (A_{пр} \cup A_{косв})$ с характеристиками: расстояние до начального состояния вектора $\mathrm{R}(\alpha) = \sum_{i=1}^{n} (f_i^{\alpha} - f_i)$, вероятность осуществления операции $p(\alpha)$.

Кроме того, учтем ряд показателей, применимых для формирования элементов алгоритма оценки взаимного влияния внутренних параметров СЗИ и операционной среды, которые будут описаны ниже.

** Табл. 2 может быть дополнена.

**Модели решения задачи оценки**

Оценка защищенности в данном случае может производиться с учетом условия взаимной независимости внутренних параметров средства защиты. В случае операционной среды таких ограничений не накладывается, поскольку внутренние связи компонентов операционной среды, с учетом недокументированных возможностей, заранее неизвестны. Таким образом, выделим два пути решения задачи, согласно [6]:

Задача 1. В первом случае, с учетом взаимной независимости внутренних параметров, устанавливаются следующие ограничения:

- взаимная независимость угроз безопасности, зависящих от некорректной настройки и/или функционирования компонентов средства защиты;
- постоянство и неизменность во времени угроз безопасности указанного выше типа.

Очевидно, что при введении подобных ограничений снимается технически трудноразрешимая задача оценки взаимных внутренних влияний в средстве защиты информации. Сложность такой задачи обусловлена неполной, но чаще закрытой информацией о таких влияниях в документации производителя, наличием недокументированных возможностей в средствах защиты информации, появлением новых угроз безопасности, входящим в множества угроз $U_?$, $U_-$.

При решении задачи 1 может быть учтена следующая гипотеза.

Гипотеза 1. Если система соответствует модели 1, являющейся решением задачи 1, то можно сформулировать следующие ее свойства:

- существует конкретный набор угроз, составляющий множество U, являющееся объединением множеств $U_+$, $U_-$, $U_?$, который однозначно определен, причем вероятности их реализации независимы;
- оценка вероятностей может быть проведена в том числе с использованием экспертной оценки, причем при проведении первичного анализа защищенности с учетом взаимодействия средства защиты информации и операционной среды, в случае невозможности или нецелесообразности нахождения объективных вероятностей.

Такой метод принят в качестве способа решения общей задачи анализа защищенности, описанной в данной работе. Вместе с тем, для решения частных задач такие ограничения могут привести к неучтенным угрозам безопасности, особенно из множеств прогнозируемых или неизвестных угроз. В этом случае рекомендуется усложнить постановку задачи как показано ниже.

Задача 2. Усложнение задачи оценки защищенности происходит следующим образом – снимается ограничение на взаимную независимость угроз. На практике существуют угрозы несанкционированного доступа, которые зависят друг от друга (см., к примеру, [1]). Может существовать два пути решения задачи 2:

- декомпозиция и упрощение угроз, сведение их к взаимно независимым классам;
- введение в задачу условных вероятностей реализации различных угроз.

В обоих случаях используемых исходных данных о взаимных влияниях компонентов средств защиты информации и операционной среды может оказаться недостаточно. Вместе с тем, на практике возможен и дополнительный сбор данных.

**Алгоритм оценки взаимного влияния внутренних параметров**

Для оценки взаимного влияния внутренних параметров СЗИ и операционной среды введем характеристики операции $\alpha$ и множеств $U_+$,$U_-$,$U_?$. Для операции изменения вектора состояния компонентов:

– сложность, определяемая параметром $p(\alpha)$;

– уровень воздействия на систему (определяемый количеством изменений в системе $\mathrm{R}_{\text{сист}} = \sum_{i=1}^{M} R(\alpha_i)$, где $M$ – общее количество известных угроз, обратимостью воздействия и работоспособностью системы после воздействия);

– устойчивость к блокированию.

Для множеств в алгоритме предполагается конечное количество элементов.

Алгоритм оценки воздействия можно представить в виде следующей последовательности шагов:

– определение базового множества известных угроз $U_+$;

– определение универсального набора факторов состояния угроз; возможно существование нескольких выделенных подмножеств $U_+$ и, следовательно, нескольких наборов факторов, анализируемых отдельно. В этом случае необходима детализация задачи:

– определение векторов состояния компонента множества угроз $U_+$;

– предварительное определение компонентов множеств $A_{пр}$, $A_{косв}$;

– расчет первой целевой функции СЗИ $\mathrm{R}^{(1)}{}_{\text{сист}} = \sum_{i=1}^{M} R(\alpha_i)$, $\alpha \in A_{пр}$, здесь $M$ – общее количество известных угроз, определяющей возможность перевода системы в небезопасное состояние;

– моделирование вероятных транзакций;

– расчет второй целевой функции СЗИ $\mathrm{R}^{(2)}{}_{\text{сист}} = \sum_{i=1}^{M+N} R(\alpha_i)$, $\alpha \in (A_{пр} \cup A_{косв})$, здесь $N$ – прогнозируемое количество угроз в множестве $U_-$.

Расчет первой целевой функции позволяет оптимизировать процесс выбора блокирующих механизмов СЗИ, а также оценить качество прогноза по множеству $U_-$. Расчет второй целевой функции позволяет оценить устойчивость системы к неучтенным, а также косвенным воздействиям и пригоден для анализа множества $U_?$.

**Итеративный метод реализации мер защиты**

С учетом применяемого метода оценки защищенности можно предложить способ нейтрализации угроз безопасности, предлагающий итеративное наложение дополнительных блокирующих элементов (или настройку дополнительных параметров) в зависимости от результатов анализа защищенности.

В случае применения итеративного метода нейтрализации угроз безопасности, используемого в случае невозможности ограничения всех элементов множества угроз безопасности, выявленных по результатам анализа защищенности предлагаемым или любым иным методом, составляется матрица дополнительных мер обеспечения безопасности.

Матрица мер обеспечения безопасности $R_0$ имеет вид

$$R_0 = \begin{pmatrix} r_1^{(1)} & \dots & r_1^{(n)} \\ r_2^{(1)} & \dots & r_2^{(n)} \\ \dots & \dots & \dots \\ r_m^{(1)} & \dots & r_m^{(n)} \end{pmatrix}.$$

Здесь $n$ – количество итераций каждой меры обеспечения информационной безопасности, $m$ – количество выделяемых классов угроз (в зависимости от детализации и выбранного уровня абстракции количество может быть изменено), $r$ – вероятности реализации заданных мер и их итераций. Правила заполнения матрицы таковы:

- в матрице $R_0$ не должно быть нулевых (пустых) строк, существование которых показывает неучтенные (незаблокированные), но при этом известные или прогнозируемые воздействия;

- меры обеспечения надежности должны гарантировать снижение вероятности хотя бы одного класса угроз безопасности, выявленного в результате проведенного анализа защищенности.

Таким образом, при реализации итеративного метода реализации мер защиты информации в рамках метода можно производить оценку качества применяемых мер с использованием предлагаемых расчетных целевых функций R, причем вторая целевая функция в теории может показать и влияние применяемых защитных механизмов на множество неизвестных угроз.

**Характеристика методов доказательства защищенности**

Очевидным методом доказательства защищенности в данном случае может являться основная теорема безопасности (анализ и коррекция векторов состояния компонентов множества с целью минимизации первой целевой функции системы, то есть приведения системы к неизменному либо контролируемому состоянию) [4].

Необходимо отметить, что обязательным условием работоспособности этого метода доказательства защищенности является формальное (математическое или логическое) доказательство безопасности исходного состояния операционной среды. Эта задача также имеет определенную сложность. Практические подходы в этой области [1-3] не дают окончательных оценок, более того, такие оценки могут быть получены только для некоторых состояний системы и простых структур операционных сред.

Кроме того, возможны методы оценки защищенности на основе анализа взаимного влияния внутренних параметров СЗИ и операционной среды:

– метод внутренних блокировок;

– метод управления структурой.

Далее рассмотрим подробнее два последних метода, основанных на принятом в работе методе анализа.

Метод внутренних блокировок предполагает анализ множества $A_{пр}$ с целью выявления операций $\alpha \in A_{пр}$ с характеристиками: расстояние до начального состояния вектора $\mathrm{R}(\alpha) = \max_{i-1}^{M} R(\alpha_i)$ по известным угрозам, количество которых принято за $M$, вероятность осуществления операции $\mathrm{p}(\alpha) = \min_{i=1}^{M} p(\alpha_i)$. После выявления операций с такими характеристиками требуется принимать меры блокировки и отслеживания функций операционной среды, которые так взаимосвязаны с внутренними параметрами средства защиты информации.

Метод управления структурой, предлагаемый в данной работе, имеет целью минимизацию второй целевой функции системы. В таком случае, при невозможности косвенного воздействия на систему, упрощаются анализируемые связи между внутренними параметрами средства защиты информации и операционной среды. При этом происходит минимизация количества элементов множества $U_?$.

Следует избегать минимизации второй целевой функции без введения дополнительных условий. В данном случае безусловная оптимизация указанной функции может привести к полной статичности операционной среды, что повлечет за собой неэффективное использование операционной среды в иных задачах. Это допустимо только в том случае, если программно-аппаратный комплекс в целом, включая операционную систему, операционную среду, интегрированные средства защиты информации и иные компоненты используются только для решения задач обеспечения информационной безопасности. Такая ситуация имеет место, к примеру, в программно-аппаратных межсетевых экранах на собственной аппаратной платформе и с модифицированными операционными системами.

**Апробация метода**

Для апробации метода были выбраны две задачи, требующие предварительного анализа внутренних взаимодействий средств защиты информации и операционной среды.

Задача защиты программного кода от модификации при условии распространения программного продукта в виде дистрибутива без открытых кодов, описанная в серии публикаций, например в [7]. Результатом применения метода в данном случае стал сформированный метод защиты программного кода, предполагающий использование четырехуровневого защитного механизма с различной стойкостью. При этом выбирается нужный уровень в зависимости от предполагаемого нарушителя.

Задача формирования виртуальной среды для выполнения специальных лабораторных работ, выполняемых в рамках дисциплин: безопасность операционных систем – при анализе внутренних настроек и их взаимного влияния, программно-аппаратные методы защиты информации – при изучении вирусных технологий и развертывании в виртуальной среде специальных программных средств защиты информации. Результатом применения стала методика реконфигурации виртуальной среды, предлагающая универсальные решения для поставленной задачи.

Развитие связано с оптимизацией метода, созданием базы знаний с учетом известной информации о взаимном влиянии компонентов средств защиты информации и операционной среды, развитием и совершенствованием теоретической основы метода. Кроме того, метод возможно развивать и в область частных решений.

**Выводы**

В статье представлены результаты, на основе теоретико-множественного подхода и теории графов, а также основных положений теории информационной безопасности в предметной области позволяющие:

– с некоторой степенью формализации описать метод исследования влияния внутренних параметров средств защиты информации на операционную среду;

– алгоритмизировать процесс анализа защищенности операционных сред с инсталлированными средствами защиты информации;

– доказать защищенность системы и оценить ее уязвимость в терминах рассматриваемого метода.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

*1. Джонс К.Дж., Шема М., Джонсон Б.С.* Антихакер. Средства защиты компьютерных сетей. Справочник профессионала / Пер. с англ. – М.: СП ЭКОМ, 2003. – 688 с.

*2. Кэрриэ Б.* Криминалистический анализ файловых систем. – СПб.: Питер, 2007. – 480 с.

*3. Касперски К.* Компьютерные вирусы снаружи и изнутри. – СПб.: Питер, 2006. – 527 с.

*4. Девянин П.Н., Михальский О.О., Правиков Д.И. и др.* Теоретические основы компьютерной безопасности: Пособие для вузов. – М.: Радио и связь, 2000. – 192 с.

*5. Золотарев В.В.* Метод исследования взаимного влияния внутренних параметров средств защиты информации и операционной среды / В.В. Золотарев / Проблемы правовой и технической защиты информации: сб. ст. / Под ред. В.В. Полякова, В.А. Мазурова. – Барнаул: Изд-во Алт. ун-та, 2008. – 180 с.

*6. Золотарев В.В.* Анализ информационных рисков при передаче данных по открытому каналу / В.В. Золотарев, О.Н. Жданов / Актуальные проблемы безопасности информационных технологий: Материалы I международной заочной научн.-практ. конф. / Под общ. ред. О.Н. Жданова, В.В. Золотарева; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2007. – С. 32-38.

*7. Лубкин И.А.* Защита программного кода от модификации и исследования методом использования в качестве адресов перехода значений хэш-функций / И.А. Лубкин / Информационная безопасность: Материалы IX Международной научн.-практ. конф. – Ч.1. – Таганрог: Изд-во ТТИ ЮФУ, 2007. – С. 216-220.

УДК 681.3.053:681.32:007.5

**А.М. Цыбулин, А.В. Никишова, М.Ю. Умницын**

## ИССЛЕДОВАНИЕ ПРОТИВОБОРСТВА СЛУЖБЫ БЕЗОПАСНОСТИ И ЗЛОУМЫШЛЕННИКОВ НА МНОГОАГЕНТНОЙ МОДЕЛИ

Пропасть между угрозами информационной безопасности и тем, что делается для защиты от них, становится все шире. Все это обуславливает чрезвычайную актуальность вопросов обеспечения информационной безопасности. Практически любая информационная система (ИС) представляет интерес для злоумышленника.

Специалист по защите информации разрабатывает и реализует ряд стратегий по защите ИС, однако оценка эффективности этих стратегий является насущной и острой проблемой.

Злоумышленник также разрабатывает и реализует ряд стратегий по проведению атак на ИС, используя ее уязвимости, и пытается максимизировать свой успех [1].

Существует множество моделей для исследования эффективности действий службы безопасности и злоумышленников. И, как правило, одна из противоборствующих сторон рассматривается упрощенно.

Исследование противоборства службы безопасности и множества злоумышленников проводится с помощью интеллектуальной многоагентной модели.

Модель включает множество агентов-нарушителей и агентов-системы безопасности, которые являются активными агентами, и агента ИС – пассивный агент. Активные агенты способны выбирать наиболее рациональные стратегии защиты и нападения в зависимости от располагаемых знаний об ИС и обучаться в процессе выполнения своих действий.

Формально агент описывается кортежем:

$$A = (K, B, T, З, И, C, П),$$

где К – класс агента; В – вид агента; Т – время жизни агента; З – совокупность знаний; И – множество инструментальных средств; С – множество стратегий; П – пользовательский идентификатор.

Выделяются следующие классы агентов: агенты службы защиты информации ($А_{сб}$); агенты ИС ($А_{ис}$); агенты злоумышленники ($А_{зл}$).