Библиографические ссылки

1. Хилл Р. Математическая теория пластичности. М. : Гостехиздат, 1954.

2. Киряков П. П., Сенашов С. И., Яхно А. И. Приложение симметрии и законов сохранения к решению дифференциальных уравнений. Новосибирск : Изд-во Сиб. отд-ния Рос. акад. наук, 2001.

3. Полянин А. Д. Справочник по линейным уравнениям математической физики. М. : Физматлит, 2001.

4. Сенашов С. И., Филюшина Е. В., Попов Е. А. Преобразование точных решений уравнений пластичности высшими симметриями // Вестник СибГАУ. 2011. Вып. 5 (38). С. 90–92.

S. I. Senashov, E. V. Filyushina

ABOUT NEW SOLUTIONS OF EQUATIONS OF PLASTICITY OBTAINED WITH THE HELP OF HIGHER SYMMETRIES

In the article the authors show how higher symmetries of plane ideal plasticity operate on exact solutions of two-dimensional ideal plasticity. New solutions are obtained.

Keywords: two-dimensional plasticity, exact solutions, higher symmetry.

УДК 004.056

А. А. Ступина, А. В. Золотарев

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ РЕШЕНИЯ ЗАДАЧИ ОЦЕНКИ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ*

Проведен сравнительный анализ методов решения задачи оценки защищенности автоматизированных систем. Рассмотрены их свойства, преимущества, недостатки, а также продукты, созданные на их основе.

Ключевые слова: формальный подход, классификационный подход, оценка защищенности.

Стремительное развитие компьютерной сферы и высоких технологий в последние два десятилетия привело к тому, что информация приобрела конкретные финансовые, репутационные, временные и другие выражения. В связи с этим для все большего числа организаций защита информации становится одной из приоритетных задач. Государство принимает активное участие в процессе становления информационной безопасности в Российской Федерации, о чем говорит усиление и ужесточение требований к защите конфиденциальной информации (коммерческой тайны, персональных данных, банковской тайны и т. д.), принятие новых законов и подзаконных актов в этой области, а также руководящих документов по классификации средств защиты информации исходя из требований безопасности. Одним из первых и основных этапов построения защищенной инфраструктуры организации является анализ оценки защищенности автоматизированной системы (АС).

В настоящее время анализ оценки защищенности АС проводится с помощью двух подходов: формального и классификационного.

Основой для *формального подхода* традиционно считается модель системы защиты с полным перекрытием, в которой рассматривается взаимодействие области угроз, защищаемой области и системы защиты [1]. Таким образом, имеется три множества:

– $T = \{t_i\}$ – множество угроз безопасности;

– $O = \{o_j\}$ – множество объектов (ресурсов) защищенной системы;

– $M = \{m_k\}$ – множество механизмов безопасности АС.

Элементы этих множеств находятся между собой в определенных отношениях, характеризующих систему защиты. Для описания системы защиты обычно используется графовая модель [1].

Множество отношений «угроза–объект» образует двухдольный граф $\{<T, O>\}$. Цель защиты состоит в том, чтобы перекрыть все возможные ребра в графе. Это достигается введением третьего набора M, в результате чего получается трехдольный граф $\{<T, M, O>\}$ (рис. 1).

Развитие модели системы защиты с полным перекрытием предполагает введение еще двух элементов:

– V – набора уязвимых мест, определяемого подмножеством декартова произведения $T*O$: $v_r = <t_i, o_j>$. Под уязвимостью системы защиты понимается возможность осуществления угрозы t в отношении объекта o;

– B – набора барьеров, определяемого декартовым произведением $V*M$: $b_l = <t_i, o_j, m_k>$. Барьеры представляют собой пути осуществления угроз безопасности, перекрытые средствами защиты.

*Работа выполнена при поддержке Министерства образования и науки Российской Федерации (соглашение 14.B37.21.0625).

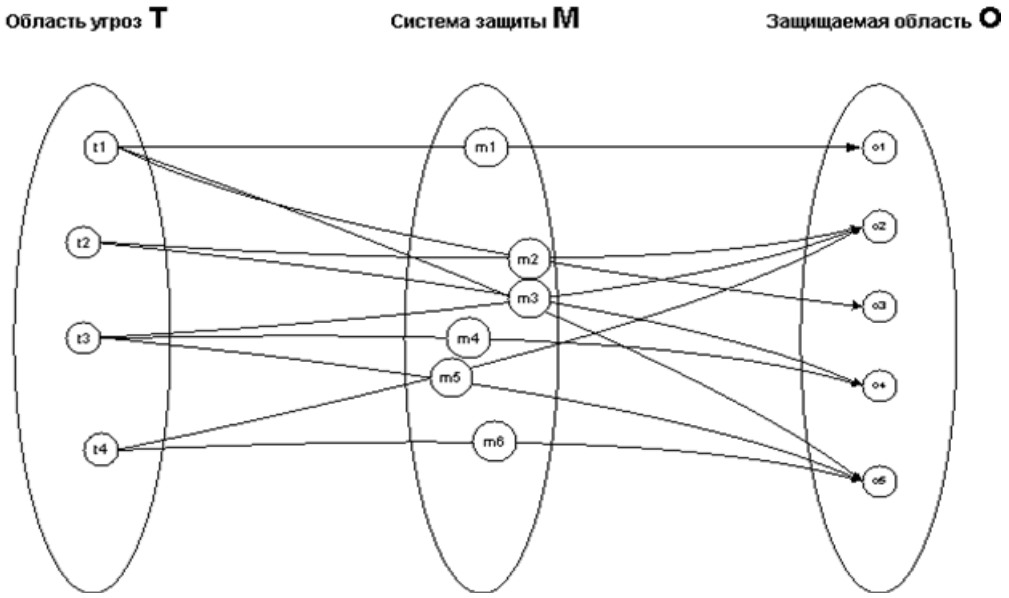

Рис. 1. Графовая модель описания системы защиты информации

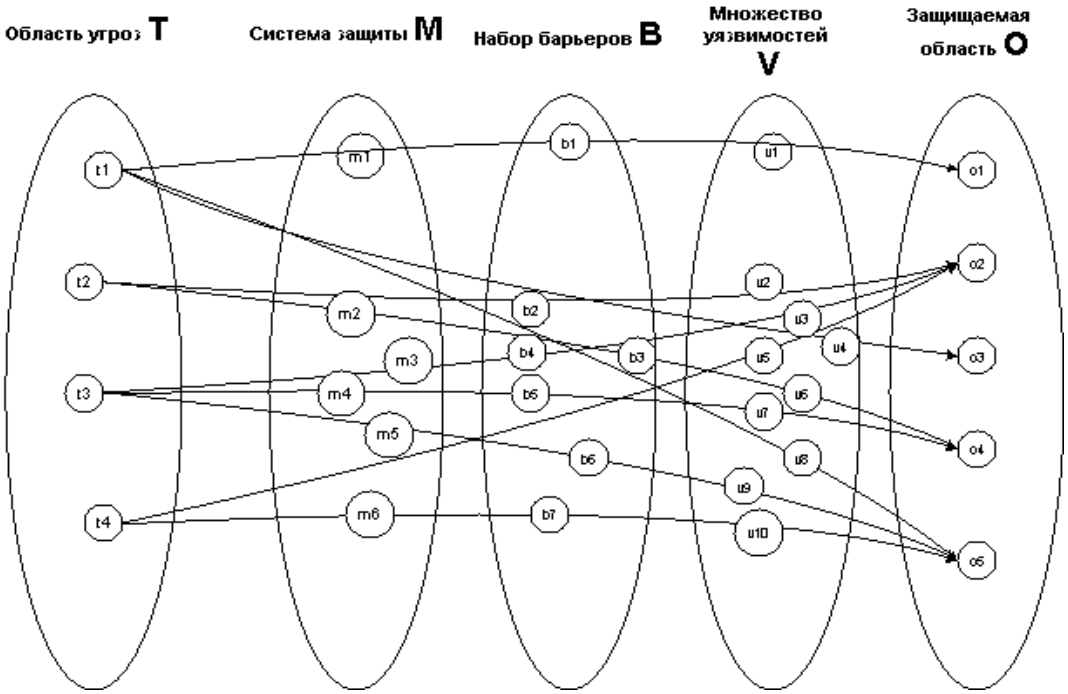

Рис. 2. Модель системы защиты, содержащей уязвимости

В результате будет получена система, состоящая из пяти элементов: $<T, O, M, V, B>$, описывающая систему защиты с учетом наличия в ней уязвимостей [1] (рис. 2).

В системе защиты с полным перекрытием для любой уязвимости имеется устраняющий ее барьер. Иными словами, в подобной системе для всех возможных угроз безопасности существуют специальные механизмы защиты, препятствующие осуществлению этих угроз. Это один из факторов, определяющих защищенность АС. Другим фактором является прочность механизмов защиты [1].

В качестве характеристик элемента набора барьеров $b_l = <t_i, o_j, m_k>$, $b_l \in B$, может рассматриваться набор $<P_l, L_l, R_l>$, где P_l – вероятность появления угрозы; L_l – величина ущерба при удачном осуществлении угрозы в отношении защищаемых объектов (уровень серьезности угрозы); R_l – степень сопротивляемости механизма защиты m_k, характеризующаяся вероятностью его преодоления.

Прочность барьера $b_l = <t_i, o_j, m_k>$ зависит от величины остаточного риска Risk_l, связанного с возможностью осуществления угрозы t_i в отношении объекта

автоматизированной системы o_j при использовании механизма защиты m_k:

$$\text{Risk}_l = P_k L_k (1 - R_k).$$

Для определения величины защищенности S можно использовать следующую формулу:

$$S = \frac{1}{(\sum_{\forall bk \in B} (P_k L_k (1 - R_k)))},$$

где P_k, $L_k \in (0, 1)$; $R_k \in [0, 1)$. Знаменатель этой формулы определяет суммарную величину остаточных рисков, связанных с возможностью осуществления угроз T в отношении объектов АС O при использовании механизмов защиты M. Эта величина характеризует общую уязвимость системы защиты, а защищенность определяется как величина, обратная уязвимости. При отсутствии в системе барьеров b_k, перекрывающих определенные уязвимости, степень сопротивляемости механизма защиты R_k принимается равной нулю.

На практике получение точных значений указанных характеристик затруднено, поскольку понятия угрозы, ущерба и сопротивляемости механизма защиты трудно формализовать. Так, оценку ущерба в результате несанкционированного доступа к информации политического и военного характера точно определить вообще невозможно, а нахождение вероятности осуществления угрозы не может базироваться на статистическом анализе [1].

В *классификационном подходе* вместо стоимостных оценок, применяемых в неформальных классификационных подходах, используют категорирование:

–нарушителей (по целям, квалификации и доступным вычислительным ресурсам);

– информации (по уровням критичности и конфиденциальности);

– средств защиты (по функциональности и гарантированности реализуемых возможностей) и т. п.

Такой подход не дает точных значений показателей защищенности, однако позволяет классифицировать АС по уровню защищенности и сравнивать их между собой [1]. Примерами классификационных методик, получивших широкое распространение, могут служить разнообразные критерии оценки безопасности информационных технологий, принятые во многих странах в качестве национальных стандартов, которые устанавливают классы и уровни защищенности.

Наиболее значимыми нормативными документами, определяющими критерии оценки защищенности и требования, предъявляемые к механизмам защиты, являются:

– Общие критерии оценки безопасности информационных технологий (The Common Criteria for Information Technology Security Evaluation) (ISO 15408);

– Практические правила управления информационной безопасностью (Code of Practice for Information Security Management) (ISO 17799);

– стандарт ИСО/МЭК 27001 «Информационные технологии. Методы защиты. Система менеджмента защиты информации. Требования»;

– руководящие документы Государственной технической комиссии (Гостехкомиссии) России и др.

Главное достоинство формального подхода состоит в том, что он позволяет получить точные количественные оценки различных показателей защищенности АС, однако его практическая реализация представляется делом весьма затруднительным и малоэффективным. Поэтому более предпочтительным в этом плане является классификационный подход.

Анализ защищенности АС – это один из основных пунктов создания комплексной системы защиты информации. Однако в последнее время в области информационной безопасности возник целый ряд новых проблем.

Первая из них – это нехватка кадров. Информационная безопасность – относительно новое направление в нашей стране, им занимаются всего несколько десятилетий, а дипломированных специалистов по данному направлению готовят только последние 10 лет. И даже если учесть, что в Российской Федерации специалистов по информационной безопасности выпускают уже 47 вузов (данные 2011 г. [2]), они все равно не могут покрыть дефицит кадров.

Вторая проблема – необходимость придерживаться принципа законности, который предполагает осуществление защитных мероприятий и разработку системы безопасности информации АС в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также с другими нормативными актами по безопасности, утвержденными органами государственной власти в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией [3].

Обычная организация ориентируется на множество стандартов и нормативных и правовых актов в зависимости от вида конфиденциальной информации, циркулирующей в АС. К примеру, для персональных данных такими документами являются Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и подзаконные ему акты. А вот российские банки могут подпадать под действие целого ряда законов и стандартов, однако наибольшее влияние на них оказывают рекомендации Центрального банка (ЦБ) России (здесь следует отметить, что несмотря на рекомендательный характер этих стандартов обеспечение информационной безопасности и получение лицензии от ЦБ России банком без их использования практически невозможно).

Третья проблема – постоянно меняющаяся статистика инцидентов информационной безопасности. Организации должны защищать инфраструктуру, обеспечивая безопасность конечных точек, системы передачи сообщений, веб-трафика и др. Другими приоритетными задачами должны быть защита критических внутренних серверов и обеспечение резервного копирования и восстановления данных. Для быстрого

реагирования на угрозы также необходимо обладать информацией о динамично меняющихся угрозах и методах борьбы с ними [4].

В связи с этим в настоящее время на рынке очень популярны специализированные программные средства оценки защищенности АС, использующие классификационный подход к анализу защищенности, который основан на нормативных документах, определяющих критерии оценки защищенности и требования, предъявляемые к механизмам защиты, такие как программные комплексы Risk Watch (США), CRAMM, COBRA (Великобритания), «АванГард», ГРИФ, КОНДОР+ (Россия) [5].

Сравнение данных программных комплексов (см. таблицу) показывает, что они охватывают большое количество критериев оценки информационной безопасности, что, безусловно, является положительным моментом. Однако их серьезным недостатком является ориентация только на один-два стандарта информационной безопасности (COBRA – на ISO 17799, CRAMM – на BS 7799:1995, RiskWatch – на LAFE (Local Annual Frequency Estimate) и SAFE (Standard Annual Frequency Estimate), являющихся документами NIST, ГРИФ – на ISO 17799, ISO 15408), и не учитывают руководящие документы Гостехкомиссии и Федеральной службы по техническому и экспортному контролю России, а также нормативные и правовые документы в области информационной безопасности, что делает эти программные продукты фактически непригодными для использования в России.

Сравнение программ анализа оценки защищенности АС

Сравниваемый критерий	ГРИФ	COBRA	CRAMM	Risk Watch	«АванГард»
Риски					
Использование категорий рисков	+	+	+	+	+
Использование понятия максимально допустимого риска	+	+	+	+	+
Подготовка плана мероприятий по снижению риска	+	+	+	+	+
Управление					
Использование понятия «владелец риска»	+	*	+	+	+
План работ по снижению риска:	+	+	*	+	+
проведение тренингов	*	*	*	*	*
проведение семинаров, собраний	*	*	*	*	*
Оценка бизнес-рисков/операционных рисков/ИТ-рисков	+	*	*	+	*
Оценка рисков на техническом уровне	*	*	+	+	+
Оценка рисков на организационном уровне	+	+	+	+	+
Информирование руководителя	+	+	+	+	+
Предлагаемые способы снижения риска					
Обход (исключение) риска		*	*	*	
Снижение риска	+	+	+	+	+
Принятие риска	*	*	*	*	
Процессы					
Использование элементов риска					
Материальные активы	+	+	+	+	+
Нематериальные активы	+	+	+	+	+
Угрозы	+	+	+	+	+
Ценность активов	+		+	+	+
Уязвимости	*	+	+	+	+
Меры безопасности	+	+	+	+	+
Потенциальный ущерб	+	+	+	+	+
Вероятность реализации угроз	+	*	+	+	+
Рассматриваемые типы рисков					
Бизнес-риски	+	*			
Риски, связанные с нарушением законодательных правил		+		+	+
Риски, связанные с использованием технологий	+	+		+	+
Коммерческие риски		*			
Риски, связанные с привлечением третьих лиц					
Риски, связанные с привлечением персонала	+				+
Повторные оценки риска	+	*	*	+	+

Окончание таблицы

Сравниваемый критерий	ГРИФ	COBRA	CRAMM	Risk Watch	«АванГард»
Определение правил принятия риска	*	*	*	*	+
Качественное ранжирование рисков	+	+	+	+	+
Количественное ранжирование рисков	+	*	+	+	+
Использование независимой оценки	+	*	*	+	*
Расчет возврата на инвестиции	+	*		+	
Расчет оптимального соотношения между мерами безопасности					
Меры предотвращения	+	+	+	+	+
Меры выявления	+	*	+	+	+
Меры по исправлению	+	*	+	+	+
Меры по восстановлению	+	+	+	+	+
Интеграция способов управления инцидентами	*	*	*	*	*
Описание назначения способов управления инцидентами	*	*	*	*	*
Процедура принятия остаточных рисков	+	*	+	+	+
Управление остаточными рисками	*	*	*	*	+
Мониторинг рисков					
Применение мониторинга эффективности мер безопасности	*	*	*	*	*
Использование процесса реагирования на инциденты в области информационной безопасности	*	*	*	*	
Проведение мероприятий по снижению риска	+	+	+	+	+
Структурированное документирование результатов оценки риска	+	+	+	+	+

Примечание. В таблице использованы следующие обозначения: + – отвечает критерию; * – не отвечает критерию; без отметки – соответствие критерию зависит от других факторов.

В связи с этим встает проблема создания программного комплекса, который учитывал бы не только зарубежные стандарты по защите информации, но и отечественные разработки в этой области. Такой комплекс мог бы облегчить организациям реализацию защиты информации ограниченного доступа в соответствии с законодательством РФ в условиях недостатка кадров по информационной безопасности. При этом организации придется затратить минимум усилий для аудита информационной безопасности и определения мер по устранению имеющихся недостатков: для этого будет необходимо лишь установить программный комплекс, ответить на контрольные вопросы и получить рекомендации по защите информации в соответствии с законодательством РФ.

Библиографические ссылки

1. Астахов А. Анализ защищенности корпоративных автоматизированных систем [Электронный ресурс]. URL: http://iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti/analiz-zaschischennosti-korporativnyh-avtomatizirovannyh-sistem (дата обращения: 02.05.2012).

2. Российское образование [Электронный ресурс] : федер. портал. URL: http://www.edu.ru/abitur/act.2/index.php?spe_=090105&sort=0&show_results=0&page=3 (дата обращения: 02.05.2012).

3. Виды мер и основные принципы обеспечения информационной безопасности [Электронный ресурс]. URL: http://asher.ru/security/book/its/06 (дата обращения: 02.05.2012).

4. Золотарев В. В. Введение в информационную безопасность : учеб. пособие / Сиб. гос. аэрокосмич. ун-т. Красноярск, 2007.

5. Жукова М. Н., Золотарев А. В. Применение нечеткой логики при решении задачи комплексной оценки защищенности автоматизированных систем // В мире науч. открытий. 2011. Вып. 12 (24). С. 205–213.

6. Золотарев В. В., Данилова Е. А. Управление информационной безопасностью : учеб. пособие. В 3 ч. Ч. 1. Анализ информационных рисков / Сиб. гос. аэрокосмич. ун-т. Красноярск, 2010.

A. A. Stupina, A. V. Zolotarev

COMPARATIVE ANALYSIS OF METHODS FOR SOLUTION OF AUTOMATISED SYSTEMS PROTECTION ESTIMATION PROBLEM

In the article the authors present comparative analysis of methods for solution of problem of estimation of protection of automated systems, their features, advantages, disadvantages and products developed on their basis.

Keywords: formal approach, classified approach, protection estimation.