УДК 004.056:65.012.8

Н. В. Медведев, П. М. Квасов,
В. Л. Цирлов

СТАНДАРТЫ И ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Рассмотрены вопросы обеспечения информационной безопасности в автоматизированной системе, предотвращения несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации и других форм незаконного вмешательства в информационные ресурсы.

E-mail: medved@mx.bmstu.ru

Ключевые слова: *политика информационной безопасности, автоматизированная система, угрозы безопасности, модель информационной безопасности, информационные риски, модели рисков.*

Цель и задачи политики информационной безопасности. Цель обеспечения информационной безопасности (ИБ) в автоматизированной системе (АС) — это предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации и других форм незаконного вмешательства в информационные ресурсы и системы.

Задача любой подсистемы обеспечения ИБ заключается в обеспечении устойчивого функционирования объекта: предотвращении угроз его безопасности, защите законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний, обеспечении нормальной производственной деятельности всех подразделений АС. Вместе с тем необходимо стремиться к повышению качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов, обслуживаемых системой. Для решения поставленной задачи необходимо:

— отнести соответствующую информацию к категории ограниченного доступа;

— провести прогноз и своевременно выявить угрозы безопасности информационных ресурсов АС, причины и условия, способствующие нанесению финансового, материального и морального ущерба, нарушению нормального функционирования и развития системы;

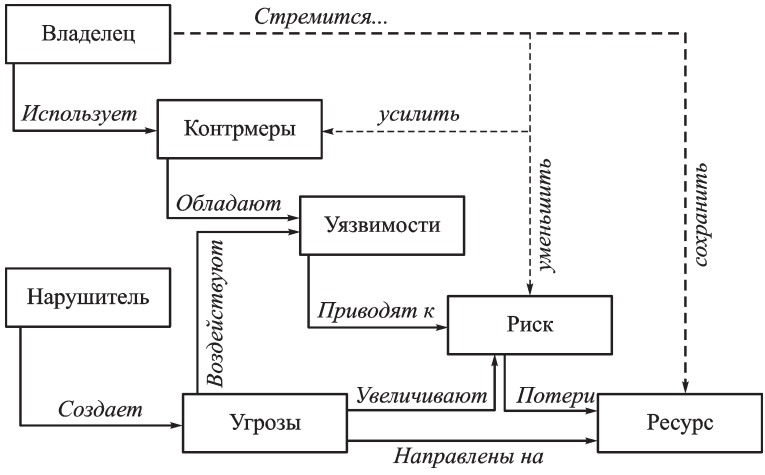

Рис. 1. Модель выработки политики ИБ

— создать условия функционирования, обеспечивающие наименьшую вероятность реализации угроз и нанесения различных видов ущерба информационным ресурсам АС;

— создать механизм и условия для оперативного реагирования на угрозы ИБ и проявление негативных тенденций в функционировании, для эффективного пресечения посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;

— создать условия для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, и тем самым ослабить возможное негативное влияние последствий нарушения ИБ.

Сформулированную задачу решает политика ИБ АС.

Требования к модели ИБ. При разработке политики ИБ целесообразно использовать модель (рис. 1), основанную на адаптации общих критериев (ISO 15408) и проведении анализа риска (ISO 17799). Эта модель соответствует специальным нормативным документам [1–4] по обеспечению ИБ, принятым в РФ, международному стандарту ISO/IEC 15408 “Информационная технология — методы защиты — критерии оценки информационной безопасности”, стандарту ISO/IEC 17799 “Управление информационной безопасностью”.

Представленная модель — это совокупность объективных внешних и внутренних факторов с учетом их влияния на состояние ИБ на объекте и на сохранность материальных или информационных ресурсов.

Рассматриваются следующие объективные факторы:

— угрозы ИБ, характеризующиеся вероятностями возникновения и реализации;

— уязвимость информационной системы или системы контрмер (подсистемы ИБ), что влияет на вероятность реализации угрозы;

— риск, т.е. фактор, отражающий возможный ущерб организации в результате реализации угрозы ИБ, т.е. утечки информации и ее неправомерного использования (риск отражает вероятные финансовые потери, прямые или косвенные).

Для создания эффективной политики ИБ предполагается первоначально проанализировать риски в области ИБ, затем определить оптимальный уровень риска для предприятия на основе заданного критерия. Политику ИБ и соответствующую подсистему защиты информации необходимо построить так, чтобы не превысить заданного уровня риска.

Оценка информационных рисков. Разработка политики ИБ АС позволяет проанализировать и документально оформить требования, связанные с обеспечением защиты информации, избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков, правильно планировать и осуществлять защиту на всех стадиях жизненного цикла АС, обеспечить проведение работ в сжатые сроки, представить обоснование для выбора мер противодействия информационным атакам, оценить эффективность контрмер и сравнить различные их варианты.

В ходе разработки политики должны быть установлены границы исследования. Для этого необходимо выделить ресурсы АС, для которых в дальнейшем будут получены оценки рисков. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные, а также отдельные документы и отдельные массивы документов — информационные ресурсы, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и др.) Примерами внешних элементов являются сети связи, внешние сервисы и т.п.

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

Эта модель в соответствии с методикой, предлагаемой стандартами ISO/IEC 15408 и ISO/IEC 17799, строится следующим образом: для выделенных ресурсов определяется их ценность как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т.д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью.

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий проводится по завершению этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

Политика ИБ АС включает в себя требования в адрес персонала, менеджеров и технических служб. Основные направления разработки политики безопасности следующие:

— определить, какие данные и насколько серьезно необходимо защищать;

— определить, кто (что) и какой ущерб может нанести АС в информационном аспекте;

— определить информационные риски и определить схемы уменьшения их до приемлемой величины.

Методика анализа информационных рисков. Существуют две методики оценки текущей ситуации в области ИБ на предприятии. Они получили образные названия “исследование снизу вверх” и “исследование сверху вниз”. Первая методика достаточно проста, требует намного меньших затрат, но и имеет меньшие возможности. Она основана на известной схеме: “Вы — злоумышленник. Ваши действия?”, т.е. служба ИБ, основываясь на данных обо всех известных видах атак, пытается применить их на практике с целью проверить, возможна ли такая атака со стороны реального злоумышленника.

Методика “сверху вниз” представляет собой, наоборот, детальный анализ всей существующей схемы хранения и обработки информации. Первым этапом этой методики является определение, какие информационные объекты и потоки необходимо защищать. Далее следует изучить текущее состояние подсистемы ИБ в целях определения, какие из классических способов защиты информации уже реализованы. На третьем этапе проводится классификация всех информационных объектов в соответствии с уровнем их конфиденциальности, требованиями к доступности и целостности.

Далее следует выяснить, насколько серьезный ущерб может нанести АС раскрытие или иная атака на каждый конкретный информационный объект. Этот этап состоит в определении рисков. Следует отметить, что классификацию ущерба, наносимого атакой, должен

оценивать владелец информации или работающий с нею персонал. Оценку вероятности появления атаки должны выполнять специалисты по обеспечению ИБ.

Инструментарий для анализа информационных рисков. В соответствии с представленной методикой авторами разработана программная система (ПС) анализа информационных рисков — анализатор рисков BRA, предназначенный для применения в составе АРМ администратора ИБ сложных информационных систем. Анализатор рисков рассматривает основные категории угроз и соответствующие меры защиты программно-аппаратных средств и информационных ресурсов. Программная система позволяет оценить вероятные финансовые потери, связанные с возможной реализацией угроз ИБ.

Порядок проведения анализа рисков с использованием ПС следующий.

1. *Сбор исходных данных в соответствии с таблицей потенциальных рисков*: исходными данными для проведения анализа рисков являются сведения об активах — аппаратуре и программном обеспечении (ПО) информационной системы.

2. *Формализация активов*: каждый из активов системы заносится в единую базу данных в виде, представленном на рис. 2.

3. *Оценка критических факторов, влияющих на реализацию угрозы*: в зависимости от типа активов задаются параметры факторов, способствующих реализации угрозы (рис. 3).

4. *Тонкая настройка параметров модели рисков*: весовые коэффициенты используемой модели рисков задаются и корректируются с учетом специфики предприятия (рис. 4).

5. *Вычисление рисков*: на основе полученных данных вычисляются вероятный и максимально возможный ущербы для каждого из активов; процесс вычисления показан на рис. 5.

Рис. 2. База данных активов

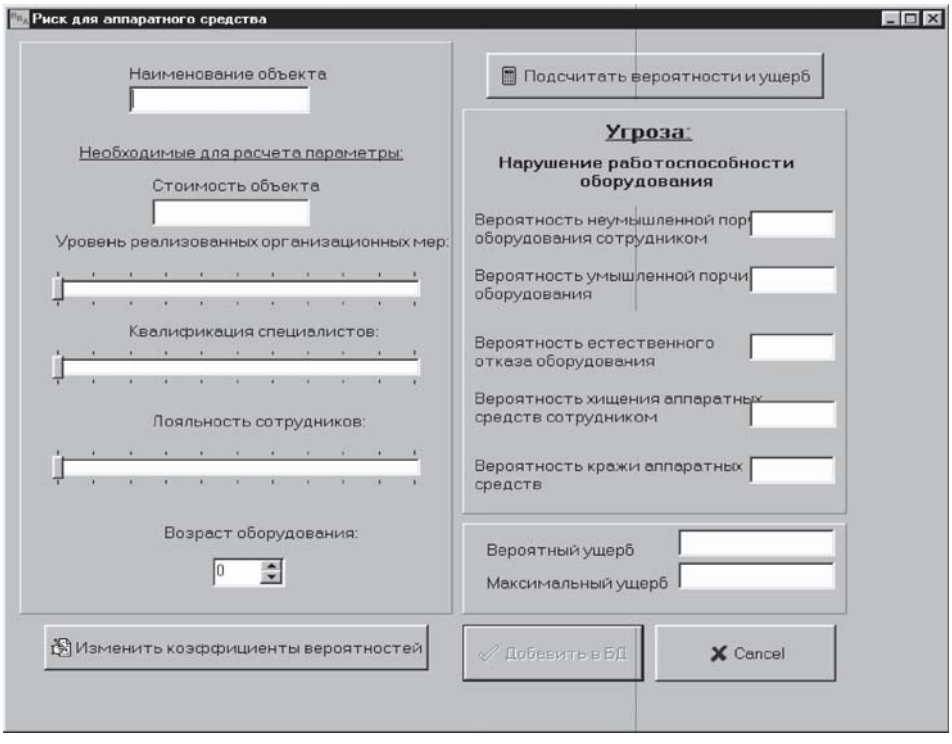

Рис. 3. Параметры факторов реализации информационных угроз

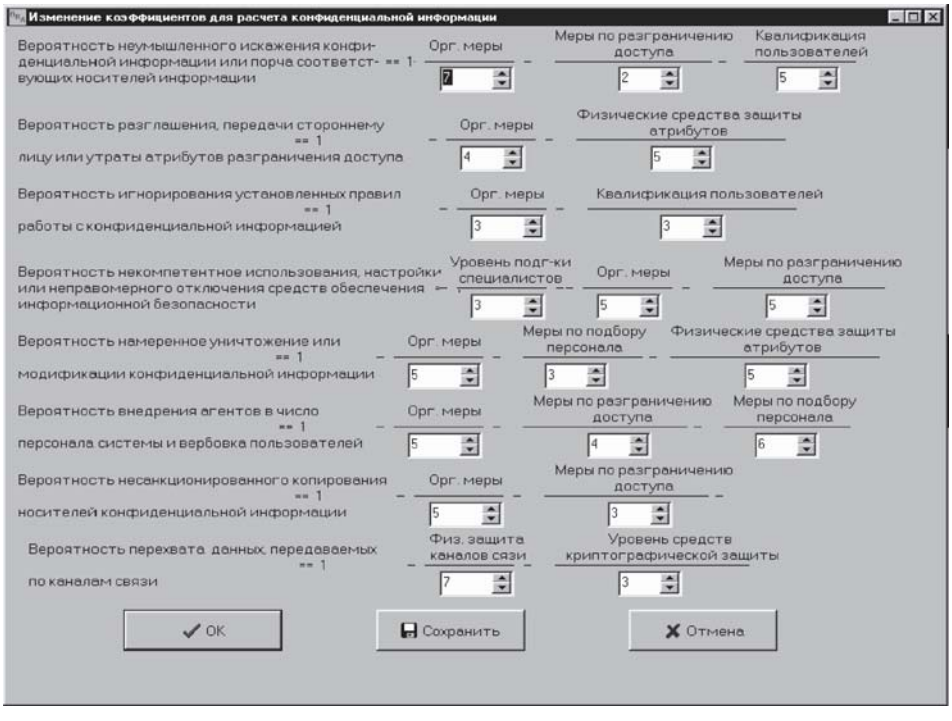

Рис. 4. Ввод и корректировка весовых коэффициентов

6. *Анализ результатов*: сохраненные в единой базе данных результаты, становятся доступными в окне оценки угроз; формат окна оценки угроз показан на рис. 6.

Заключение. Если интегральный риск превышает допустимое значение, то существуют погрешности в системе безопасности, которые в сумме не позволят предприятию эффективно работать. В этом случае из строк выбираются те, содержание которых внесет самый значительный вклад в значение интегрального риска, и выполняется попытка их уменьшить или полностью устранить.

Одним из наиболее важных соображений при выборе методики оценки риска является то, что полученные результаты должны быть эффективны при реализации подсистемы обеспечения ИБ. Использование сложной методики, требующей точных исходных данных и имеющей на выходе неоднозначные результаты, вряд ли поможет создать эффективную защиту.

Процесс оценки риска утечки информации проводится в два этапа. На первом этапе определяют детальную конфигурацию АС для построения ее модели. На втором этапе проводится анализ риска. Анализ риска разбивается на идентификацию ценностей, угроз и уязвимых мест, оценку вероятностей и измерение риска. Показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть найдены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например, учитывающими возможные воздействия внешней среды.

Наибольшее распространение среди методик оценки рисков получила методика “матрицы рисков”. Это достаточно простая методика анализа рисков. В процессе оценки эксперты определяют вероятность возникновения каждого риска и размер связанных с ним потерь (стоимость риска). Причем оценка выполняется по шкале с тремя градациями: высокая, средняя, низкая. На базе оценок для отдельных рисков выставляется оценка системе в целом (в виде клетки в такой же матрице), а сами риски ранжируются. Данная методика позволяет быстро и корректно оценить риски.

Политика ИБ АС должна обеспечить надлежащие уровни как отдельных рисков, так и интегрального. При ее разработке необходимо учитывать объективные проблемы, которые могут возникнуть на пути реализации политики безопасности. Такими проблемами могут стать законы страны и международного сообщества, внутренние требования корпорации, этические нормы общества.

После описания всех технических и административных мер, планируемых к реализации, рассчитывается экономическая стоимость разработки политики. В том случае, когда финансовые вложения в

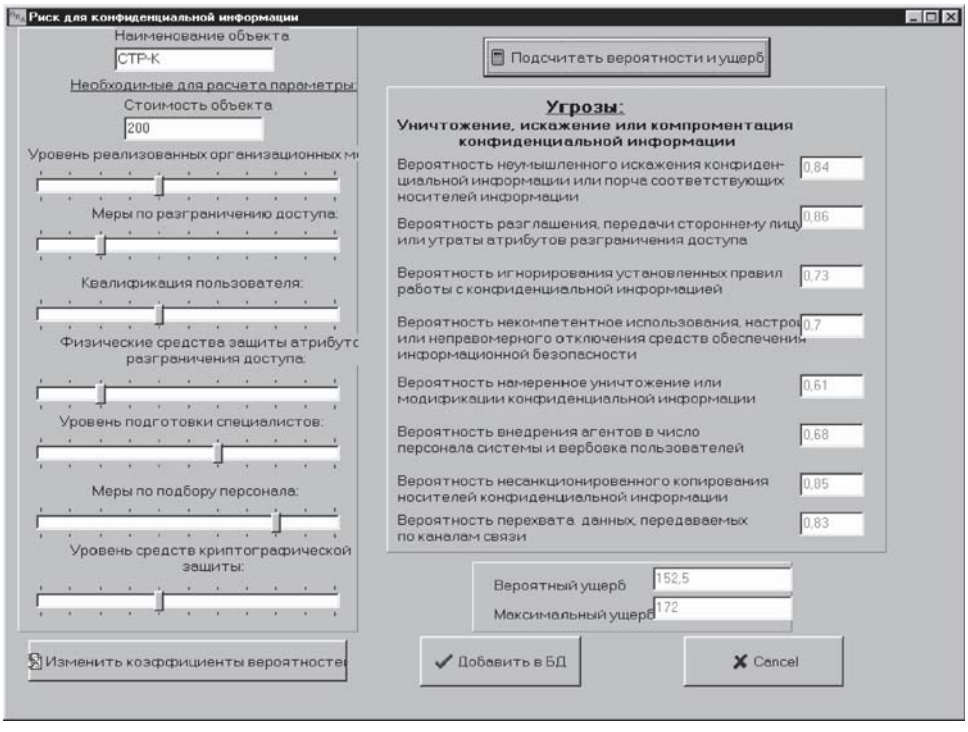

Рис. 5. Форма для вычисления рисков

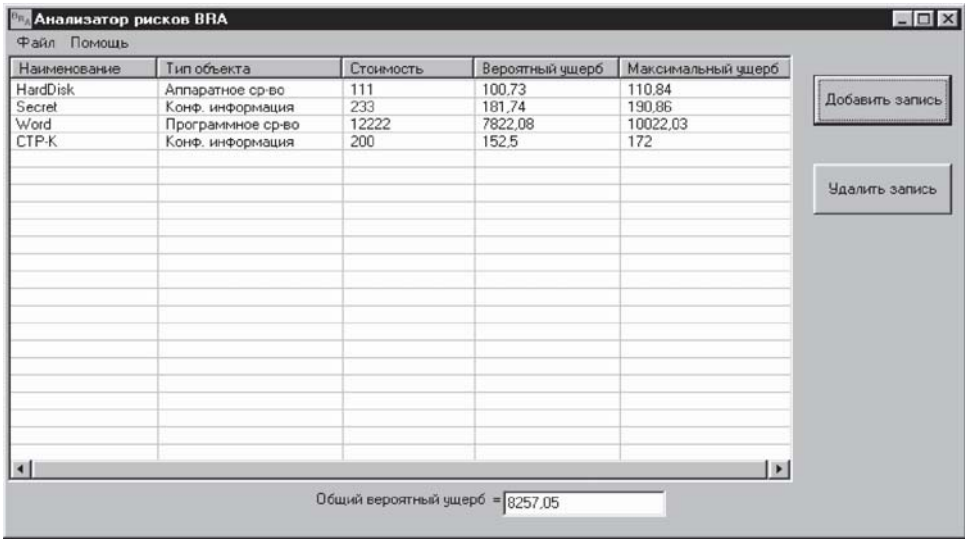

Рис. 6. Окно оценки угроз

программу безопасности являются неприемлемыми или просто экономически невыгодными, по сравнению с потенциальным ущербом от атак, проводится возврат на уровень, где был задан максимально допустимый риск, и его значение увеличивается на один или два пункта.

Разработка политики ИБ завершается ее утверждением у руководства фирмы и детальным документированием. За этим должна следовать активная реализация всех компонентов, указанных в плане. Перерасчет таблицы рисков и, как следствие, модификация политики ИБ АС проводится раз в год.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. – М.: Госстандарт России, 2002.
2. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности. – М.: Госстандарт России, 2002.
3. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Требования доверия к безопасности. – М.: Госстандарт России, 2002.
4. ISO/IEC 17799:2005 Information technology — Security techniques — Information security management systems — Requirements, 2005.

Статья поступила в редакцию 18.06.2009

Николай Викторович Медведев родился в 1954 г., окончил в 1977 г. МГТУ им. Н.Э. Баумана, Канд. техн. наук, зав. кафедрой “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор около 50 научных работ в области исследования и разработки защищенных систем автоматической обработки информации.

N.V. Medvedev (b. 1954) graduated from the Bauman Moscow Higher Technical School in 1977. Ph. D. (Eng.), head of “Information Security” department of the Bauman Moscow State Technical University. Author of about 50 publications in the field of study and development of protected systems of automated data processing.

Павел Михайлович Квасов родился в 1981 г., окончил в 2004 г. МГТУ им. Н.Э. Баумана. Зав. лабораторией кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор ряда научных работ в области информационной безопасности.

P.M. Kvasov (b. 1981) graduated from the Bauman Moscow State Technical University in 2004. Head of laboratory of “Information Security” department of the Bauman Moscow State Technical University. Author of some publications in the field of information security.

Валентин Леонидович Цирлов родился в 1981 г., окончил в 2005 г. МГТУ им. Н.Э. Баумана. Ассистент кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор более 10 научных работ в области информационной безопасности и защиты автоматизированных систем.

V.L. Tsirlov (b. 1981) graduated from the Bauman Moscow State Technical University in 2005. Assistant of lecturer of “Information Security” department of the Bauman Moscow State Technical University. Author of more than 10 publications in the field of information security and protection of automated systems.