УДК 510.6:681.3

Хорев П.Б., Ларионов И.П.

ОСОБЕННОСТИ РАЗРАБОТКИ МЕТОДИКИ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ДЛЯ ЭКСПЕРТНЫХ СИСТЕМ

Аннотация. *Определяются проблемы и особенности разработки методики оценки информационной безопасности предприятия для использования в экспертной системе поддержки проектирования комплексных систем защиты информации, рассматриваются требования законодательства по обеспечению информационной безопасности и способы их представления и оценки соответствия им в экспертных системах.*

Ключевые слова: *Экспертные системы, комплексные системы защиты информации, информационная безопасность, методика оценки информационной безопасности.*

Larionov I.P., Khorev P.B.

Design peculiarities of information security assessment methodology for expert systems

Abstract. *There described problems and peculiarities of information security assessment methodology design for expert systems for development of complex information security system for enterprise, the overview is given for the legal requirements for information security and their methods of presentation and conformity assessment them in expert systems.*

Keywords: *expert systems, complex information security systems, information security, information security assessment methodology.*

Комплексные системы защиты информации (КСЗИ) для предприятий России стали обязательной частью в составе информационных систем (ИС) для обеспечения информационной безопасности (ИБ) в соответствие с требованиями законных и подзаконных актов РФ [4]. Для многих предприятий после вступления в силу федерального закона №152-ФЗ «О персональных данных» от 27.07.2006 возникла необходимость по проектированию и внедрению КСЗИ на своем предприятии для защиты персональных данных сотрудников и клиентов. Однако создание КСЗИ не является тривиальной и однозначной задачей, которая ложится на плечи руководителей организации и отделов, не имеющих достаточной компетенции по данному вопросу. Возникает необходимость в формировании штата специалистов по защите информации (ЗИ), которые будут заниматься данным вопросом в сотрудничестве с компаниями-интеграторами, специализирующиеся на внедрении КСЗИ. Но даже эти шаги недостаточно упрощают работу над разработкой и внедрением КСЗИ на предприятии, поэтому предлагается автоматизировать процесс решения таких задач, как разработка

организационно-распорядительных документов (ОРД), разработка технического проекта внедрения или модернизации существующей КСЗИ, соблюдение дополнительных требований заказчика и государственных органов по регулированию защиты персональных данных (ПД). Автоматизация данных задач требует подходов к проблеме на основе экспертной системы (ЭС) [6] или системы поддержки принятия решений (СППР) [2,3].

Прежде чем приступить к разработке КСЗИ, необходимо определить текущий уровень ЗИ на предприятии, составить и оценить модель угроз ИБ, проверить текущие меры и средства защиты на соответствие требованиям законодательства РФ. Особого рассмотрения требует задача оценки ИБ предприятия с помощью ЭС. ЭС проектирования КСЗИ должны «владеть» такой методикой оценки ИБ. Затруднение вызывает тот факт, что на данный момент нет общепринятой государственной методики оценки соответствия ИБ предприятия нормативно-правовым актам РФ, поэтому приходится пользоваться требованиями текущих документов по ЗИ и международных стандартов и практик [4].

Такая методика должна подходить как для предприятий малого и среднего бизнеса, так и больших компаний. Методика должна позволять определять численные показатели риска ИБ с целью идентификации текущего уровня защищенности для дальнейшего совершенствования КСЗИ предприятия до допустимого уровня риска ИБ [1,5].

Обобщенная последовательность действий любой методики оценки рисков ИБ представлен на рис.1.

Рис.1. Обобщенная последовательность действий методики оценки рисков ИБ

Для ЭС дополнительной задачей также является формализация методики оценки рисков ИБ и поддержка возможности создания дополнительных (пользовательских) методик с возможностью редактирования. ЭС может осуществить такую формализацию на основе базы знаний, фактов и правил, при этом для поддержки разработки собственных методик по оценки рисков ИБ необходимо создать некий шаблон правил и фреймов знаний для каждого из этапов.

На первом этапе методики должно производиться выявление информационных активов предприятия, подлежащих защите согласно

требованию законодательства (ПД) или компании (коммерческая тайна). Это можно сделать методом анкетирования, причем такая анкета уже содержит предопределенные типы информационных активов таких как:

1. Собственно сведения, хранимые в виде отдельных файлов в ИС.
2. Аппаратные обеспечение (компьютеры, принтеры, другие устройства).
3. Программное обеспечение (прикладные программы, информационные системы и т.д.).
4. Телекоммуникационное обеспечение (линии связи, оборудование по обеспечению связи).
5. Программно-аппаратные средства (внешние носители информации).
6. Документы (контракты, стратегии развития и планирования).
7. Продукция и услуги предприятия («ноу-хау», рецептура, интеллектуальная продукция, обеспечение конфиденциальности услуг).

Также должно быть предусмотрена возможность создания пользовательского типа информационных активов. Каждый тип активов должен характеризоваться в ЭС определенным набором свойств, которые позволят методике более точно рассчитывать риски ИБ предприятия. Такими свойствами могут выступать:

1. Стоимость актива (количественная оценка).
2. Критичность актива (насколько он важен для компании – качественная оценка).
3. Категория конфиденциальности (ПД, коммерческая тайна, служебная тайна, государственная тайна).
4. Гриф конфиденциальности (для коммерческой тайны используются грифы, утвержденные предприятием).
5. Описание актива.
6. Название актива.
7. Тип актива.

Ряд свойств носят чисто информационный характер и используются для категорирования и описания самих активов (5-7), другие позволяют провести оценку рисков ИБ и построить модель угроз (1-4). Данный набор свойств можно считать минимально необходимым.

На втором этапе для анализа несоответствий требованиям законодательства текущей КСЗИ нужно предварительно выявить текущие меры и средства ЗИ, степень осведомленности персонала о ЗИ, наличие всех необходимых ОРД в области ИБ. Здесь тоже подойдет метод анкетирования. Анкета должна быть составлена группой специалистов по ЗИ и содержать полный перечень требований законодательства по ЗИ в зависимости от типа существующих активов и классов ИС в соответствии с принятой в государстве классификацией ИС по обработке ПД и по обработке информации ограниченного доступа, разрабатываемыми ФСТЭК России. На сегодняшний момент это два основных документа РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г. и Постановление Правительства РФ от 01.11.2012 №1119 «Об

утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также требования некоторых других федеральных законов, руководящих документов и приказов ФСТЭК, ФСБ и Роскомнадзора. Отсюда также возникает необходимость в обновлении данных такой методики, которая должна всегда основываться на актуальных нормативно-правовых актах РФ. Требования, зафиксированные в законе, должны быть описаны понятно для пользователя, не обладающего юридическим образованием. Оценка соответствия производится численно: за каждое выполненное требование ставится единица, за не выполненное – ноль. Вводится показатель – риск несоответствия требованиям законодательства – R_L, обратно пропорциональный объему выполненных обязательных требований:

$$R_L = 1 - \frac{\sum_{i=1}^{N} r_i}{N} \quad (1)$$

где N – общее число требований (учитываемых методикой), r_i – значение выполнения требования (1 – выполнено, 0 – не выполнено).

Третий этап заключается в создании модели угроз. В ЭС модель угроз сначала определяет перечень объектов защиты – информационных активов компании, полученных на этапе 1, – и перечень типовых угроз, которые хранятся в базе знаний и связаны с конкретными типами активов. На основе второго этапа можно сформировать предварительный перечень контрмер на основе анализа выполнения требований законодательства. Отношения между активами и угрозами можно отобразить в виде двудольного графа (рис.2а), а с учетом контрмер – в виде трехдольного графа (рис.2б). Такой способ наглядно изображает уже защищенные и подверженные угрозам объекты. Диаграмма должна быть редактируемой, чтобы пользователь мог исключить лишние, по его мнению, угрозы, объединять активы, средства ЗИ и угрозы в группы и добавлять новые элементы в перечни средств ЗИ, угроз и активов.

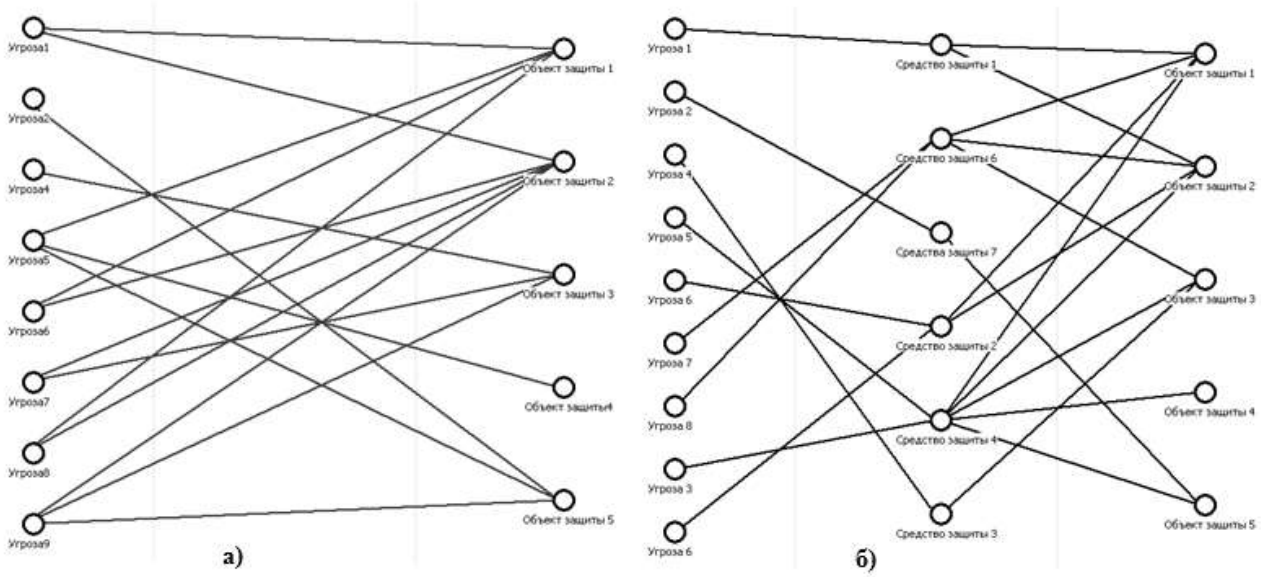

Рис. 2. Слева (а) изображен двудольный граф, где отображены вершины-угрозы от которых направлены дуги к вершинам-активам; справа (б) – модель трехдольного графа, где между активами и угрозами располагаются вершины контрмеры.

Такой способ позволяет автоматически создать предварительную модель угроз (двудольный граф) и модель угроз с контрмерами (трехдольный граф) с возможностью последующей коррекции. Для помощи пользователю данный функционал должен быть подробно описан в руководстве пользователя. Итогом определения модели будет являться перечень актуальных угроз – угроз, от которых нет полноценной защиты на данном предприятии и которые необходимо в дальнейшем снизить до приемлемого уровня.

На четвертом этапе производится количественная оценка риска ИБ на основе перечня актуальных угроз, информационных активов и контрмер. С помощью этих данных (фактов) и правил логического вывода и знаний должен быть определен алгоритм вычисления количественного показателя рисков ИБ. Пошаговый алгоритм количественного определения риска ИБ представлен на рис.3.

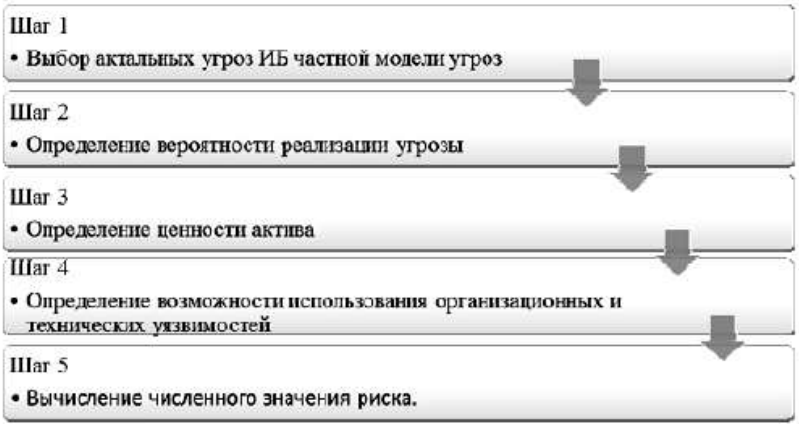

Рис.3. Алгоритм количественного оценивания риска ИБ

На пятом этапе происходит определение допустимого уровня риска. Допустимый риск – это риск, принятый приемлемым при существующих оценках стоимости активов и затрат на ИБ. Данное значение также определяется на основе правил, где главными показателями будут являться:

1) тип предприятия (малого, среднего, крупного бизнеса);
2) категории обрабатываемой информации (класс, гриф конфиденциальности, объем);
3) общая стоимость защищаемых активов.

В зависимости от выбора приемлемое значение может лежать в диапазоне от 3% до 10%. Выполнение всех этапов проведения оценки рисков ИБ на предприятии производится для каждого типа актива и затем складывается в интегральную оценку рисков ИБ. Если итоговое значение риска меньше приемлемого, то делается вывод о том, что на предприятии выполнены требования по ИБ в полной мере, а риск ИБ оцениваемого типа актива допустимый. Но необходимо периодически проводить переоценку рисков ИБ. Если итоговое значение риска больше или равно 5%, то делается вывод о том,

что на предприятии не выполняются требования по ИБ, а риск ИБ оцениваемого типа актива повышенный и требует немедленного принятия решений. Именно на защиту активов с наибольшим риском ИБ и стоимостью должна быть направлена модернизация или внедрение КСЗИ на предприятии [1,4].

Список литературы

1. Кустов Г.А. Управление информационными рисками организации на основе логико-вероятностного метода: автореф. дис. ... канд. тех. наук. – Уфа, 2008. – 18 с.
2. Ларионов И.П. Система поддержки принятия парето-оптимальных решений в области проектирования комплексной системы защиты информации предприятия. // «Современные проблемы информационной безопасности и программной инженерии» 2013, №1 с 85-91.
3. Лотов А.В., Бушенков В.А., Каменев Г.К., Черных О.Л., Компьютер и поиск компромисса, метод достижимых целей, издательство «Наука», М: 1997. – 404 с.
4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов – М.: Горячая линия – Телеком, 2004. – 280 с.
5. Симонов С. Технологии и инструментарий для управления рисками // Jet Info. – 2003. –№ 2 (117). – С. 3–32.
6. Советов Б.Я. Интеллектуальные системы и технологии: учебник для студ. Учреждений высш. проф. образования . – М.: Издательский центр «Академия», 2013. – 320 с.

ДАННЫЕ ОБ АВТОРАХ

***Хорев Павел Борисович**, доцент кафедры ИБиПИ, к.т.н, доцент.*
Российский государственный социальный университет – ул. Вильгельма Пика, д.4 стр.1, Москва, 129226, Россия.
Электронная почта: ***info@rgsu.net***

***Ларионов Игорь Павлович**, ассистент.*
Российский государственный социальный университет – ул. Вильгельма Пика, д.4 стр.1, Москва, 129226, Россия.
Электронная почта: ***info@rgsu.net***