Выводы

В работе был предложен подход, который позволяет обосновать величину приемлемого значения риска в организации. Знание такой величины в дальнейшем позволит сформировать модель расчета допустимых значений риска r_j активов или группы активов организации. В свою очередь, знание допустимых значений риска r_j позволит принимать обоснованное управленческое решение о необходимости внедрения защитных мер для информационных активов организации.

1. ISO/IEC 27001:2005. Information technology -- Security techniques -- Information security management systems – Requirements.
2. ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management.
3. *В.В.Мохор, А.М.Богданов*, Изложение руководства «ISO GUIDE 73:2009. RISK MANAGEMENT – VOCABULARY» на руском языке», №2/04-06/2011 Das Management.
4. *В.И.Завгородний* /Парадигма информационных рисков // http://fa-kit.ru.
5. *Иванов А.А., Олейников С.Я., Бочаров С.А.* /Риск-менеджмент. Учебно-методический комплекс. Международный консорциум «Электронный университет».// Московский государственный университет экономики, статистики и информатики. Евразийский открытый институт. Москва - 2008.
6. *Лобанов А.Е. Чугунов А.В.* /Энциклопедия финансового риск–менеджмента,// Москва, Альпина Паблишер , 2003 .
7. *Е. Д. Соложенцев,* / Сценарное логико-вероятносное управление риском в бизнесе и технике,// Издательский дом «Бизнес-пресса», Санкт-Петербург -2006.
8. *И.А. Рябин* / Надежность и безопасность структурно-сложных систем.//Политехника 2000- 248с.

Поступила 18.02.2013р.

УДК 519.711

А.Е. Макаревич, И.В. Коцюба, г.Киев

ВОПРОСЫ ПРИМЕНЕНИЕ АППАРАТА ЛОГИКО-ВЕРОЯТНОСТНОГО МОДЕЛИРОВАНИЯ К РЕШЕНИЮ ЗАДАЧ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Abstract. We propose an approach for information security risk assessment with application of logical-and-probabilistic method.

Актуальность

Не секрет, что в наше время в повседневной деятельности организаций всех видов и форм собственности, все большую важность приобретает

защита информационных ресурсов. Многие уже убедились на собственном горьком опыте, что пренебрегание вопросами информационной безопасности может обернуться большими материальными потерями, уходом ключевого персонала, закрытием важных проектов или даже целого бизнеса. Построение и поддержание оптимальной работы системы информационной безопасности организации становится актуальной задачей, в связи, с чем предъявляются повышенные требования к методам и средствам анализа рисков информационной безопасности. В частности все более актуальным становится разработка и внедрения новых методов количественного анализа рисков. В данной статье рассматриваются возможные подходы к решению данной задачи с использованием методов логико-вероятностного моделирования.

Постановка задачи

Рассмотрим модель менеджмента рисков, принятую в международном стандарте серии ISO 31000. Процесс работы с риском в предложенном стандартном подходе разбивается на следующие основные этапы:

- Обмен информацией и консультирование
- Установление контекста
- Оценку риска (включающую идентификацию, анализ и оценивание риска)
- Обработку риска
- Мониторинг и анализ

Рассмотрим один из основных этапов – Оценка риска, который в данном контексте подразумевает идентификацию, анализ и оценивание риска.

Этап идентификации состоит из выявления уязвимостей и сценариев угроз по отношению к информационному активу.

Этап анализа риска представляет собой выявление последствий от реализации риска и определение вероятностей их наступления. Знание этих ключевых параметров в совокупности позволяет снизить неопределенность в отношении защищенности данного информационного актива, то есть оценить риск. Этапы процесса анализа приведены на рис.1

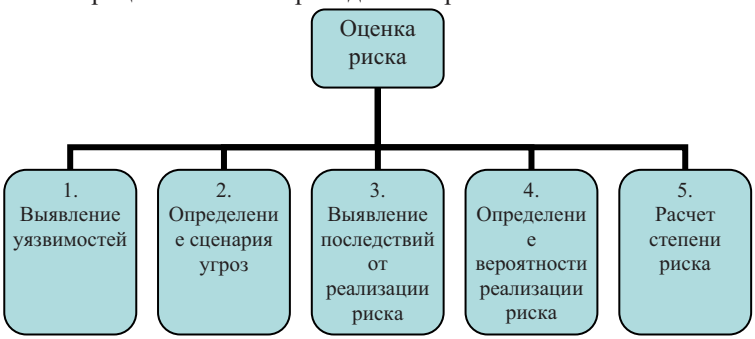

Рис. 1

Логическая структура процесса анализа выглядит следующим образом. Имеется некий информационный актив, существуют определенные предпосылки или условия (уязвимости) при использовании которых (сценарий угрозы) может наступить факт потери данным активом его целостности, доступности или конфиденциальности (ЦДК). Наша задача определить эти уязвимости, т.е. слабые места организации по отношению к сохранности (безопасности) выбранного актива. Далее мы должны выявить возможные варианты развития событий по отношению к нашему активу, то есть, определить сценарии угроз. Определив уязвимости и угрозы, мы можем спрогнозировать последствия от потери свойств ЦДК, вероятность их наступления и рассчитать степень риска. На данном этапе актуальным становится вопрос количественной оценки вероятности реализации риска. Если мы располагаем статистическим материалом, позволяющим определить закон распределения вероятности наступления инцидентов, то возможно использование множества уже предложенных и стандартизованных методов и подходов. Таких как методы с использованием цепей Маркова, метода Байеса, анализа дерева событий, анализа причин и следствий, имитационного моделирование методом Монте-Карло, NAZOP, HACCP и др. Если же такой статистики нет, то использование выше упомянутых методов серьезно затруднено. Нельзя не учитывать, тот факт, что во многих организациях инциденты информационной безопасности происходят достаточно редко, их наличие может тщательно скрываться или просто не учитываться, а для вновь созданных систем или систем, находящихся только на этапе проектирования, данную статистику получить просто невозможно. Кроме того, при стандартизованном подходе к анализу рисков, каждый риск для каждого информационного актива рассматривается отдельно без учета связей его с другими активами и особенностей функционирования информационной системы организации как единого целого. Последний факт приводит к тому, что из рассмотрения выпадает ценная информация, заключенная в самой логике функционирования информационной системы.

Решение задачи

Решение задачи анализа рисков ИБ с использованием логики функционирования информационной системы с последующим переходом к оценке вероятностей представляется очень перспективным на базе метода логико-вероятностного моделирования, разработанного и предложенного для оценки надежности и безопасности структурно-сложных систем профессором И.А Рябининым еще в середине 60-х годов.

Суть метода логико-вероятностного моделирования (ЛВМ) состоит в построении логической модели опасности системы, функции алгебры логики (ФАЛ) по правилам булевой алгебры, и последующего перехода к вероятностной модели с использованием теоремы разложения и других алгоритмов. Основным отличием ЛВМ от традиционного подхода к анализу рисков является проведение анализа «сверху вниз», то есть определение

некоего опасного состояния системы и затем выявление структуры и связей ее составляющих, вплоть до выявления инициирующих условий (ИУ) и инициирующих событий (ИС), составляющих причинную базу наступления опасного состояния. Понятия ИУ и ИС могут полностью соответствовать понятиям уязвимостей и угроз в традиционной методологии анализа рисков. Однако применение метода ЛВМ для решения задач оценки рисков в системах ИБ потребует некоторого пересмотра последовательности работ по анализу рисков.

Попытаемся сформулировать последовательность работ при анализе рисков информационной безопасности (ИБ) с использования метода ЛВМ:

1. Поставить в соответствие основные термины и определения традиционной методологии анализа рисков терминам и определениям ЛВМ
2. Определить, что является опасным состоянием для рассматриваемой системы
3. Составить логическую схему опасного состояния исследуемой системы
4. Определить ФАЛ
5. Определить вероятностную функцию (ВФ)
6. Рассчитать вероятность наступления ИУ и ИС
7. Рассчитать весовые коэффициенты ИУ и ИС

Как видно из сформулированной выше последовательности, подход к анализу рисков ИБ с использованием ЛВМ является кардинально противоположным традиционному, например, активо-ориентированному методу анализа, где в качестве отправной точки анализа используются информационные активы организации.

Для устранения вышеуказанного противоречия предлагается метод анализа информационной безопасности имеющий в своей основе построение модели логического функционирования информационной системы организации. При этом информационная система представляется как логическая модель с входными данными в виде перечня информационных активов и выходными данными в виде различных опасных состояний системы.

Предлагаемая модель анализа рисков информационной безопасности представлена на рис.2.

В состав логической модели информационной системы должны входить как структурные составляющие собственно самой системы, так и инициирующие ситуации и условия, соответствующие традиционным понятиям угроз и уязвимостей. При этом состав угроз и уязвимостей может меняться в зависимости от типа поступившего на вход информационного актива. Таким образом, логическая система представляется в виде схемы с

обратными связями и может классифицироваться как структурно сложная система (ССС). Именно такой тип систем предпочтителен для анализа с помощью ЛВ-методов. После построения логической модели, определения перечня опасных состояний и множества информационных активов производится дальнейший анализ путем построения функции алгебраической логики и перехода к вероятностной функции. В результате расчетов мы получаем вероятности рисков по отношению к каждому информационному активу, получаем возможность учета весовых коэффициентов угроз и уязвимостей (что позволяет оценить вклад каждой составляющей в опасное состояние системы), а также вероятности наступления опасного состояния всей информационной системы.

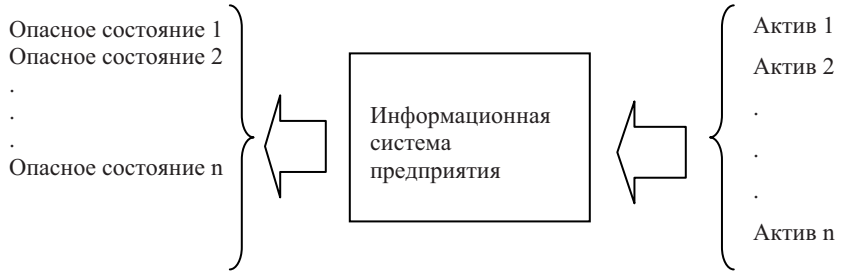

Рис. 2

Выводы

Предложен вариант применения метода логико-вероятностного моделирования для оценки риска информационной безопасности в рамках методологии принятой рядом международных стандартов. Использование предложенного варианта интеграции метода ЛВМ в традиционный подход к оценке риска информационной безопасности может позволить количественно оценить риск информационной системы организации и ранжировать вклады аргументов, составляющих логическую модель системы в ее безопасность даже в случае отсутствия вероятностей истинности инициирующих событий.

1. *Рябинин И.А.* Надежность и безопасность структурно-сложных систем. СПб.: Политехника, 2000.
2. *Соложенцев Е.Д.* Сценарное логико-вероятностное управление риском в бизнесе и технике. СПб.: Издательский дом "Бизнес-пресса", 2004.
3. *Соложенцев Е.Д., Степанова Н.В., Карасев В.В.* Прозрачность методик оценки кредитных рисков и рейтингов. СПб.: Изд-во С.-Петербургского ун-та, 2005.
4. *Можаев А.С., Громов В.Н.* Теоретические основы общего логико-вероятностного метода автоматизированного моделирования систем. СПб.: ВИТУ, 2000.
5.BS 31010 – 2010, ISO IEC 31010-2009.

Поступила 11.02.2013р.