УДК - 004.056 + 005. 334:004.056 Вестник УрФО № 1(23) / 2017, с. 28–35

Зырянова Т. Ю.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ОЦЕНКИ И ПРОГНОЗИРОВАНИЯ РИСКОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Понятия оценки рисков и управления рисками появились относительно недавно и сегодня вызывают постоянный интерес специалистов как в области обеспечения непрерывности бизнеса, так и в области информационной безопасности.

Использование информационных технологий всегда связано с определенной совокупностью рисков, под которыми обычно понимается количественная оценка событий, ведущих к финансовым потерям.

В наиболее распространенном понимании этой проблемы процесс управления информационными рисками представляет собой действия по идентификации угрозы, оценке вероятности появления угрозы, количественной оценке ущерба в случае осуществления угрозы, выработке контрмер и оценке их эффективности.

В статье приводится постановка задачи анализа информационных рисков; анализ международной концепции информационной безопасности и особенностей ее применения; анализ теоретических и практических подходов к оценке и прогнозированию информационных рисков.

Ключевые слова: *система менеджмента информационной безопасности, риск информационной безопасности, анализ риска, оценка риска, прогнозирование риска, количественная оценка риска.*

Zyryanova T. Yu.

COMPARATIVE ANALYSIS OF METHODS FOR RISK ASSESSMENT AND RISK FORECASTING FOR INFORMATION SYSTEMS

The concept of risk evaluation and risk management have emerged relatively recently and today cause a constant interest of specialists both in the business continuity and in the information security.

The use of information technology is always associated with a certain set of risks, which are usually understood as the estimation of events leading to financial losses.

In the most common understanding of this problem, the process of information risk management is the actions for identifying a threat, evaluation the probability of a threat, quantifying the damage in the event of a threat, developing countermeasures and assessing their effectiveness.

The article presents the task of analyzing information risks; the analysis of the international concept of information security and features of its application; the analysis of theoretical and practical approaches to the assessment and forecasting of information risk.

Keywords: *information security management system, information security risk, risk assessment, risk forecasting, risk evaluation.*

Современный уровень развития информационных технологий выдвигает на передний план новые требования к построению систем защиты информации и обеспечению информационной безопасности.

На протяжении длительного времени понятие информационной безопасности отождествлялось с обеспечением конфиденциальности информации, а наибольшее распространение получило применение технических средств защиты. Сегодня информация, будучи нематериальной по своей природе, становится предметом товарно-денежных отношений и объектом нормативно-правового регулирования. Перед государственными и коммерческими предприятиями и организациями все острее встает проблема не только обеспечения надежной защиты информации от несанкционированного ознакомления и распространения, но и поддержки стабильного доступа к информации и возможности эффективной работы с ней.

Актуальность исследований в данной области обусловлена высокими темпами развития и расширения сферы применения информационных технологий, которые значительно опережают формирование теоретической и методологической базы построения систем управления информационной безопасностью.

Потери от нарушения информационной безопасности зачастую превышают затраты на создание и эксплуатацию систем защиты.

Создаваемые системы менеджмента информационной безопасностью должны быть основаны на анализе рисков информационных систем (а именно на оценке текущего уровня риска и прогнозировании этого уровня в будущем).

Эффективные методики оценки и прогнозирования информационных рисков на сегодняшний день отсутствуют, но именно они должны помочь ответить на вопросы:

– какая информация подлежит защите и по каким причинам;

– к чему может привести отсутствие эффективной системы защиты информации;

– как организовать наиболее эффективную систему защиты информации;

– какова ее стоимость.

Под системой менеджмента информационной безопасности (СМИБ) понимается часть общей системы менеджмента, базирующаяся на анализе рисков и предназначенная для проектирования, реализации, контроля, сопровождения и совершенствования мер в области информационной безопасности.

Под термином «риск» будем понимать отрицательное следствие наличия уязвимости, характеризующееся вероятностью возникновения негативного события и последствиями возникновения этого события.

В основу исследования положено предположение о том, что СМИБ должна базироваться на анализе рисков с целью наибольшей ее эффективности.

Для достижения этой цели необходимо решить следующие задачи.

Первая задача связана с тем, что формирование модели угроз должно носить динамический характер. Какое бы множество угроз не было сформировано, всегда есть возможность появления новой, неизвестной ранее угрозы в неопределенный заранее момент времени. Предпосылки таких событий в модели угроз необходимо учитывать.

Вторая задача состоит в разработке методики оценки и прогнозирования информационного риска, что в сумме и составляет процесс анализа информационного риска.

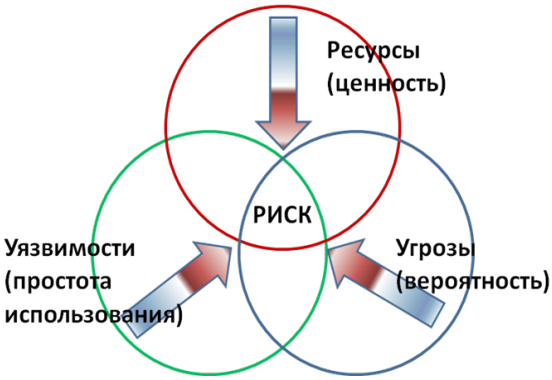
При решении третьей задачи необходимо оценить эффективность построенной методики на конкретных моделях или примерах информационных систем.

1. Базовая терминология и основные положения теории управления информационными рисками

Базовая терминология теории управления информационными рисками на сегодняшний день сформирована в системе международных стандартов ISO/IEC 27000, которые гармонизированы в Российской Федерации в серии ГОСТ Р ИСО/МЭК 27000, например [1 – 4].

Понятие информационного риска наглядно иллюстрирует схема, приведенная на рис. 1.

Рис. 1. Составляющие информационного риска



Угрозой называется потенциальная причина нежелательного инцидента, который может причинить ущерб информационному ресурсу.

Уязвимость – слабость в системе защиты, дающая возможность реализации угрозы.

Стрелки на рис. 1 указывают направление роста следующих показателей:

– для ресурса – его ценность;

– для угрозы – вероятность ее реализации;

– для уязвимости – простота, с которой уязвимость используется.

Существует ряд общепринятых подходов к измерению рисков. Наиболее распространенные из них – оценка по двум факторам и оценка по трем факторам. Формула (1) иллюстрирует подход вычислению риска по трем факторам (здесь не указаны единицы измерения ущерба, так как зачастую невозможно оценить ущерб в его материальном выражении. Он может быть обусловлен, например, потерей репутации компании, причинением вреда жизни и здоровью людей, террористической угрозой).

$$R = P \cdot P_y \cdot V, \quad (1)$$

где R – риск, P – вероятность реализации угрозы, P_y – вероятность того, что уязвимость будет использована; V – размер возможного ущерба или ценность ресурса.

Если переменные в (1) являются количественными величинами (выраженные, например, в денежных единицах), то риск – это математическое ожидания размера ущерба.

Если переменные являются качественными величинами (оценка производится относительно *низкого, среднего, высокого* уровней некоторой шкалы измерения), то метрическая операция умножения не определена. Таким образом, в явном виде эта формула использоваться не может, а рассматривается лишь как формулировка общей идеи. В этом случае применяются разного рода табличные методы оценки риска.

Пример табличного метода приведен на рис. 2. Здесь вероятность возникновения угрозы и вероятность использования уязви-

Вероятность возникновения угрозы		**Низкая**			**Средняя**			**Высокая**		
Вероятность использования уязвимости		**Н**	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Низкий риск: *0 – 2*
Средний риск: *3 – 5*
Высокий риск: *6 – 8*

Рис. 2. Табличный метод оценки ценности ресурса, характеристик угроз и уязвимостей

мости оцениваются по трехуровневой шкале, ущерб – по пятиуровневой и итоговый риск – по 9-уровневой [4].

После того как оценки риска получены для каждой известной угрозы, они должны быть интегрированы в итоговый показатель.

В соответствии с приведенным подходом информация, подлежащая защите на конкретном предприятии или в организации классифицируется на основе утвержденной системы классификации, например:

– информация, составляющая коммерческую тайну предприятия (организации);

– персональные данные;

– информация, составляющая служебную тайну и т. д.

Для каждого класса защищаемой информации формируется модель угроз, определяется их актуальность, размер возможного ущерба.

Например, к угрозам несанкционированного доступа могут быть отнесены:

– угрозы, реализуемые с применением программных средств операционной системы;

– угрозы, реализуемые с применением специального программного обеспечения;

– угрозы, реализуемые с применением вредоносных программ.

Аналогично определяются и оцениваются уязвимости по различным направлениям безопасности (табл. 1).

Для выявления угроз и уязвимостей используются следующие методы:

– автоматизированные инструментальные средства поиска уязвимостей;

– тестирование на проникновение;

– проверка кодов;

– опрос сотрудников и пользователей;

– физический осмотр;

– анализ документов.

После всех проведенных классификаций и оценок полученные результаты сводятся в таблицу, аналогичную приведенной на рис. 2, по которой определяется итоговый уровень риска.

Очевидно, что такие методики не всегда могут быть эффективны.

Таблица 1

Примеры уязвимостей информационных систем

Класс уязвимостей	Примеры уязвимостей
Аппаратные средства	Недостаточное техническое обслуживание Отсутствие эффективного контроля изменений конфигурации Незащищенное хранение
Программные средства	Отсутствующее или недостаточное тестирование программных средств Неверное распределение прав доступа Незащищенные таблицы паролей
Сеть	Незащищенные линии связи Ненадежная сетевая архитектура Передача паролей в незашифрованном виде
Персонал	Неадекватные процедуры набора персонала Недостаточное осознание требований безопасности Безнадзорная работа внешнего персонала

2. Постановка задачи оценки и прогнозирования информационного риска

Исходя из вышеизложенных фактов, будем рассматривать задачу оценки и прогнозирования информационного риска в следующих предположениях.

1. Невозможно сформировать полные множества угроз и уязвимостей.

2. Множества угроз и уязвимостей формируются динамически.

3. Элементы множества угроз и множества уязвимостей могут быть взаимосвязаны.

4. Суммарный риск в информационной системе зависит от множества параметров (2).

$$R = F\left(f_1, f_2, \ldots, f_N\right). \qquad (2)$$

Параметров, формирующих риск, может быть сколь угодно много, и выявить функциональную зависимость не представляется возможным.

Итак, для решения задачи оценки и прогнозирования информационного риска требуется:

– получить оценку текущего значения риска;

– построить прогноз значения риска на