УДК 004.056.5(045) **Луцкий М.Г., Иванченко Е.В., Казмирчук С.В. (НАУ)**

БАЗОВЫЕ ПОНЯТИЯ УПРАВЛЕНИЯ РИСКОМ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проведен анализ базовых понятий связанных с управлением риска в сфере информационной безопасности. Относительно этого построена схема зависимости процессов связанных с управлением риска и его интегрированными параметрами. Это даст возможность унифицировать процесс исследования существующих методов и методик анализа и оценки риска, повысит эффективность осуществления их выбора. Также приведен пример анализа и оценки наиболее известных методик с использованием интегрированных параметров.

Ключевые слова: риск, анализ риска, информационная безопасность, оценка риска, управление риском, угроза, уязвимость, методика.

В работе [18] был проведен анализ понятия риска в различных предметных областях для последующей его интерпретации в сфере информационной безопасности (ИБ). В результате этого было выделено множество базовых признаков риска (присущих соответствующей предметной сфере), через которые и определяются его параметры. Используя полученные результаты, в работе [19] предложено интегрированное представление этих параметров в виде кортежа и выделены идентифицирующие и оценочные компоненты. На их основе можно сформировать критерии, позволяющие унифицировать и упростить оценку и выбор соответствующих методик оценки и анализа риска, которые представлены в достаточно широком спектре средств, начинающихся нормативными документами (стандартами) и заканчивающихся конкретными программными продуктами. Для эффективного осуществления указанных оценок, актуальным является определение таких базовых понятий, связанных с управлением риска, как анализ и оценка риска, угроза и уязвимость.

В этой связи **целью данной работы** является анализ и раскрытие понятий связанных с управлением риском, с последующей интерпретацией в области ИБ и их использованием для анализа существующих методик с целью дальнейшего упрощения их выбора.

Понятия анализа и оценки риска в научной литературе и нормативно-правовых документах имеют достаточно широкий спектр трактований и практически часто пересекаются, что видно из нижеследующего анализа понятий. **Оценка риска** (risk assessment) в некоторых источниках, рассматривается как **процесс**: идентификации информационных ресурсов (ИР) системы и угроз этим ресурсам, а также возможных потерь (то есть потенциал потери), основанный на оценке частоты возникновения событий и размере ущерба; включающий идентификацию и анализ риска [5, 8, 15, 16, 23]; выявления риска и определения его влияния [7, 24]; определения степени потенциальной угрозы и риска, связанного с системой информационных технологий (ИТ) всюду по ее циклу жизни и развития, включающего в себя 9 шагов (характеристика системы, идентификация угрозы, идентификация уязвимости, анализ контроля, определение вероятности, анализ воздействия, определение риска, рекомендации контроля, документирование результатов) [5]; составления списка рисков, ранжированных по цене и критичности; изучения уязвимостей, угроз, вероятности возможных потерь и теоретической эффективности контрмер; оценки угроз, воздействия на уязвимости ИР и процессов, а также вероятности их возникновения [17, 23]; определения количественными или качественными параметрами величины (степени) рисков [12]. Встречаются и другие определения: (risk evaluation) оценка на постоянной основе вероятности и последствия всех выявленных рисков, с использованием методов, основанных на качественных и количественных оценках [3]; натурально-вещественный и стоимостный анализ всех рисковых обстоятельств, характеризующих параметры риска [14]; оценка последствий нежелательных событий [6]. **Анализ риска** (risk analysis) так же как и оценка, в некоторых источниках, раскрывается **как процесс**: идентификации рисков, определение их

величины и выделение областей, требующих защиты (часть управления рисками); оценки величины рисков [23]; систематического использования информации для выявления источников оценки степени риска [7]; определения источников и количественной оценки риска [7, 16]; подробного расследования с целью выявления нежелательных событий [6]; охватывающий определение относительной стоимости риска (основанной на последствии) и эффективности системы защиты [10, 11]; определения угроз безопасности информации и их характеристик, слабых сторон комплексной системы защиты информации (известных и допустимых); оценки потенциального ущерба от реализации угроз и степени их приемлемости для эксплуатации автоматизированной системы [22].

После проведения анализа вышеизложенных понятий просматривается некоторая неопределенность относительно точного определения того, что представляет собой анализ и оценка риска и чем эти понятия друг от друга отличаются. Из определений видно, что как оценка, так и анализ связанны процессом идентификации риска.

В ИБ, оценку риска можно определить как процесс установления значимости риска, после проведения его анализа. В свою очередь для определения анализа риска ИБ наиболее удачным будет использование понятия анализа как процесс идентификации риска в сфере ИБ.

И так определив, что анализ и оценка риска является последовательными взаимосвязанными процедурами, рассмотрим понятие управления риском в сфере ИБ. В научной литературе и нормативных документах касающихся рассматриваемых вопросов встречаются определения понятия менеджмента или управления риском (risk management), как скоординированные действия или деятельность: по руководству и управлению организацией в отношении рисков (обычно менеджмент риска включает его оценку, обработку, принятие и коммуникацию) [5, 16, 28]; по сокращению возможных потерь, связанных с риском (в том числе: диверсификация риска, маркетинговые исследования, страхование риска) [25].

Так же, как и понятия оценки и анализа риска в отдельных источниках, под его управлением понимают **процесс**: идентификации, управления, устранения или уменьшения вероятности событий, способных негативно воздействовать на ресурсы информационной системы (ИС), уменьшения рисков безопасности, потенциально имеющих возможность воздействовать на ИС, при условии приемлемой стоимости средств защиты (этот процесс содержит анализ риска, анализ параметра “стоимость-эффективность”, выбор, построение и испытание подсистемы безопасности, а также исследование всех аспектов безопасности. Цель процедуры управления риском состоит в том, чтобы уменьшить риски до уровней, одобренных DAA (Designated Approving Authority – лицо, уполномоченное выбрать уровни рисков) [1, 23]); выявления рисков, оценки рисков и предпринятия шагов по его снижению до приемлемого уровня (включает три этапа – оценка риска, его снижение и анализ) [7]; определения приемлемого уровня риска, оценки его текущего уровня, а также выполнения операций по снижению до приемлемого значения и поддержанию последнего [24]; взвешивания политики альтернатив, с учетом оценки риска и других факторов, выбора соответствующих профилактик и контроля параметров [8]; осознания рисков руководством предприятия, определение рисков предприятия и возложения ответственности за управление ими в организации [3]; включающий в себя набор решений для управления рисками (передача риска, например, через страхование, принятие или уменьшение его посредством выбора соответствующих гарантий) [6]; осознание причин и границ нежелательных событий, определение приемлемого уровня риска, а также снижение его текущего значения до уровня приемлемого [17].

Базовая цель управления рисками заключается в обеспечении экономического баланса между уровнем рисков на предприятии и стоимостью защитных мер [4].

Риски, связанные с ИБ в компании, есть составной частью рисков общих. Поэтому компания, заинтересована в том, чтобы ИТ-риски, которые возникают при нарушении ИБ,

уменьшились, а общий процесс управления всеми рисками должен быть завязан на риск-менеджменте.

На основе проведенного анализа указанных определений наиболее оптимальным для отражения понятия управление риском в сфере ИБ будет следующее – согласованные виды деятельности по руководству и управлению организацией в отношении рисков. При этом управление рисками включает в себя все операции, которые можно проводить над риском ИБ: минимизация (risk reduction) – выбор и внедрение контрмер по закрытию нарушений базовых характеристик безопасности ресурсов (процесс минимизации риска происходит после его оценки); нейтрализация – смягчение риска путем выполнения операций, направленных на противостояние угрозам [7, 24]; при работе с ИБ нельзя полностью исключить риски из-за того, что некоторые из них находятся в недосягаемости компании, например, стихийные бедствия, поэтому их принимают (risk retention) – проводиться, например, с рисками, которые имеют малую вероятность или значимость и приведут к низким затратам; остаточный риск или тот который нельзя полностью перекрыть, обычно ответственность за него передают третьему лицу, передача риска или страхование (risk transfer) – это система мер по защите интересов физических и юридических лиц за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов [13]. По анализу операций, которые можно производить над рисками, можно сделать вывод, что все они объединяются таким понятием как управление риском.

Составим схему зависимости процессов связанных с управлением риска (рис. 1). Для организации процесса управления риском определяют его параметры (“параметры риска”). После определения параметров необходимо провести его анализ – идентификацию. После прохождения этапа “анализа”, переходим к этапу “оценки риска”. Для реализации соответствующих процессов анализа и оценки применяются различные методы, методики и методологии. После этапа оценки переходим к операциям над риском – принятия решения, что делать с полученным результатом. Все описанные этапы можно объединить в одно понятие “управление риском”. В работе [19] были определенны идентифицирующие и оценочные параметры риска, которые, в свою очередь, используются в одноимённых этапах управления риском.

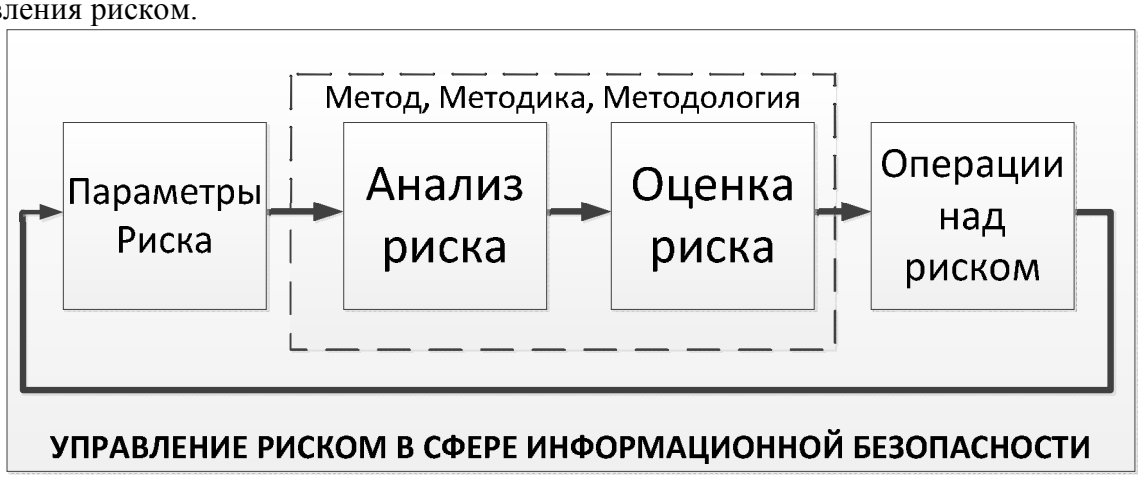

Рис. 1. Схема зависимости процессов связанных с управлением риском в сфере ИБ.

В определениях оценки и анализа риска встречаются понятия угроза и уязвимость. Под угрозой будем понимать потенциальную возможность нарушения безопасности [20], а под уязвимостью – дефект (или слабое место) в процедурах безопасности системы, проекте, выполнении или внутреннем контроле, который может возникнуть случайно или намеренно и приведет к нарушению безопасности или нарушению политики системы безопасности [2].

Определив базовые понятия и схему зависимости процессов, связанных с управлением рисков в сфере ИБ, а также основываясь на интегрированных параметрах [19] можно перейти

к анализу и оценке отдельных методик с целью упрощения их выбора. Приведем пример такого анализа и оценки с использованием наиболее известных методик.

Методика COBRA (Consultative Objective and Bi-Functional Risk Analysis, разработчик – C & A Systems Security Ltd**,** Великобритания) ориентирована на поддержку требований стандарта ISO 17799 посредством тематических вопросников (check list's), используемых в ходе оценки рисков информационных активов и электронных бизнестранзакций компании [9]. Продукт расширен инструментарием для консалтинга и проведения обзоров безопасности, который разработан на основании принципов построения экспертных систем. В комплект ПО входят модули COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant, а также менеджер модуля COBRA, используемый для настройки и изменения снабжаемой базы знаний.

На основе инициализации тематического вопросника осуществляется оценка и анализ риска по следующим категориям: высокоуровневая; ИТ безопасности; оперативная ИТ и бизнеса; инфраструктуры электронной коммерции. Модули тематического вопросника информационно поддерживают отдельные приложения, например: APP-MAN (Application level security management) – управления безопасностью; APPAUDIT (Application level Auditing) – аудит; APPCNTRL (Application Staff control) – контроль штата; APPDEPND (Application Staff dependency) – зависимость штата; AUDIT (System Audit) – проверка системы и т.д. Примером инициализации данных для APPCNTRL, посредством запроса – "Сколько инцидентов воровства произошло за последние 2 года?", может быть ввод числа "10" при количестве таких инцидентов больше десяти.

Как видно из запроса, здесь нет конкретизации по украденному, что не позволяет четко определить степень урона и на какие характеристики безопасности ресурсов информационных систем (РИС) повлиял тот или иной инцидент. Такой подход дает возможность реализовать лишь достаточно грубое оценивание риска. Воровство (с учетом [20]) есть субъективной активной угрозой КЦД-типа, конфиденциальность, целостность и доступность в этом случае нарушается, например, с исчезновением единственного экземпляра определенных информационных ресурсов, кража также может быть связана с подменной данных перед их вводом или в процессе вывода [20] и т.д. Касательно степени урона для компании при краже конфиденциальной информации, например, личной информации сотрудников или базы данных клиентов, то он будет значительно отличаться при наступлении этих событий.

Относительно интегрированного представления параметров риска [19] для методики COBRA можно получить отображения его идентифицирующих составляющих: **E, A, M** и **C**. Так, компоненту **A** (исходя из указанного примера) соответствует, например, значение A_1="Кража". Это действие приводит к нарушению определённых характеристик безопасности атакованных ресурсов и может быть связано со значением E_7="НКЦД". Инициализация данных осуществляется в числовой форме, что отображается количественной мерой посредством идентифицирующего параметра $M_{кл}$. Очевидно, что определение **C** в этом запросе можно осуществить через параметр C_o поскольку задается точное количество инцидентов. С учетом [19], здесь анализ (идентификация) риска осуществляется посредством идентифицирующих параметров во время обработки запросов, а оценка – посредством результатов анализа с использованием оценочных компонентов.

После обработки инициализированых данных система генерирует отчет, в котором описана детальная оценка (Detailed Risk Assessment (continued)) по следующим характеристикам риска: категория (RISK CATEGORY); уровень (RISK LEVEL); оценка (RISK ASSESSMENT). Например: КАТЕГОРИЯ РИСКА – "Непредвиденная ситуация в бизнесе"; УРОВЕНЬ РИСКА – 96,61%; ОЦЕНКА РИСКА – "Персонал плохо подготовлен к непредвиденным ситуациям, нет планирования действий в непредвиденных ситуациях и не выполняются требования к ним". Отметим, что в анализируемой методике риск отображается тремя характеристиками, первая и последняя из которых несут в себе

идентифицирующую составляющую (название категории и комментарии к ней), а оставшаяся – оценочную составляющую, которой соответствует "УРОВЕНЬ РИСКА", представленный в процентах (вероятность наступления риска), в связи с этим (учитывая [19]) уровень риска можно отобразить через оценочный компонент **P**.

Анализ и оценка риска происходит во время обработки данных инициируемых через тематический вопросник. Все рассматриваемые действия **(A)**, которые отображаются в запросах, собраны в категории риска, например, действие рассмотренное в примере запроса A_1 входит в категорию риска "Непредвиденная ситуация в бизнесе (НСБ)", следовательно идентифицирующий параметр в данной категории риска можно представить как $A_{ÍÑÁ} \in \{A_{ÍÑÁ1}, A_{ÍÑÁ2}, ..., A_{ÍÑÁà}\}$, где $A_{НСБ1}$= "Кража" (а – количество идентификаторов угроз для категории НСБ) [19].

После описания всех категорий и ранжирования уровней риска (с самого высокого до нулевого) в методике приводятся рекомендуемые меры по их снижению. Так, в приведенном примере для указанной категории риска дается рекомендация – "Пользователи должны формально определить свои минимальные требования обслуживания и быть готовыми к непредвиденным ситуациям". Также в методике имеется возможность просмотра инициируемых данных для тематического вопросника (Question & Response Listing (continued)).

После проведенного анализа с учетом интегрированного представления параметров риска [19] кортеж для этой методики можем представить в виде **<E, A, C, M, P>**, а например, относительно запроса про инциденты воровства его идентифицирующие параметры принимают конкретные значения – $E_{нкцд}$, $A_{НСБ1}$, $C_о$, $M_{кл}$.

Метод CRAMM (CCTA Risk Analysis and Management Method, разработчик – Центральное агентство по компьютерам и телекоммуникациям (CCTA – Central Computer and Telecommunications Agency), Великобритания**)** реализован фирмой Insight Consulting Limited в одноимённом программном продукте, в котором предусматривается поэтапный и строгий подход к анализу и оценке риска, охватывающий аспекты безопасности как технического (например, ИТ-оборудование и программное обеспечение), так и нетехнического характера (например, физического и человеческого) [26]. В дальнейшем будем рассматривать программное инструментальное средство CRAMM, в котором процесс оценивания реализуется в три этапа. На первом – проводится идентификация физических, программных и информационных ресурсов, содержащихся внутри границ системы. Ценность физических ресурсов в CRAMM определяется стоимостью их восстановления в случае разрушения. Для данных и ПО выбираются применимые к данной ИС критерии, дается оценка ущерба по шкале со значениями от 1 до 10. Например, шкала оценки по критерию "Финансовые потери, связанные с восстановлением ресурсов" отображается через следующие значения [21, 27]: 2 балла – менее $1000; 6 баллов – от $1000 до $10 000; 10 баллов – свыше $100 000 и т.д.

На втором этапе рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. Оценивается зависимость пользовательских сервисов от определенных групп ресурсов и существующий уровень угроз и уязвимостей, а также вычисляются уровни рисков и анализируются результаты. Ресурсы группируются по типам угроз и уязвимостей. Например, в случае существования угрозы пожара или кражи в качестве группы ресурсов разумно рассмотреть все ресурсы, находящиеся в одном месте (серверный зал, помещение средств связи и т. д.).

Программное средство CRAMM для каждой группы ресурсов (и каждого из 36 типов угроз) генерирует список запросов, для которых после инициализации данных оценка уровней осуществляется, например, как очень высокий, высокий, средний, низкий, очень низкий (для угрозы), и как высокий, средний и низкий (для уязвимости). Рассмотрим пример запроса для "**оценки угрозы"**: "Сколько раз за последние три года сотрудники организации пытались получить несанкционированный доступ к хранящейся в ИС информации с

использованием прав других пользователей?" Также, для дальнейшей обработки, предлагаются варианты инициализации данных запросу посредством присваивания определённого количества балов: a) ни разу (0 балов); … d) в среднем чаще одного раза в год (30 балов) и т.д. Пример запроса для **"оценка уязвимости"**: "Сколько людей имеют право пользоваться ИС?" a) от 1 до 10 (0 балов); b) от 11 до 50 (4 бала) и т.д. На основе этой информации рассчитываются уровни рисков (риск определяется как возможность потерь в результате какого-либо действия или события, способного нанести ущерб [27]) в дискретной шкале с градациями от 1 до 7. Программное средство CRAMM объединяет угрозы и уязвимости в матрице риска, а для создания шкал, например, используются данные из табл. 1 (для уровней угроз и уязвимостей).

Анализ риска проводится на первом и втором этапах, после чего осуществляется его оценка. Во время анализа предлагается проставить коэффициенты для каждого ресурса с точки зрения частоты возникновения угрозы и вероятности реализации угрозы, в связи с этим с учетом [19] здесь можно выделить оценочные компоненты **F** и **P**.

Исходя из оценок стоимости ресурсов защищаемой ИС, угроз и уязвимостей, определяются "ожидаемые годовые потери". На рис. 2 приведен пример матрицы оценки ожидаемых потерь [27], где второй столбец слева содержит значения стоимости ресурса, верхняя строка заголовка таблицы – оценку частоты возникновения угрозы в течение года (уровня угрозы), нижняя строка заголовка – оценку вероятности успеха реализации угрозы (уровня уязвимости).

Значения ожидаемых годовых потерь (Annual Loss of Expectancy) переводятся в баллы, показывающие уровень риска, согласно шкалы, представленной на рис. 3 (в этом примере размер потерь приводится в фунтах стерлингах) и далее в соответствии с матрицей (рис. 4) выводится оценка риска. Здесь, с учетом [19], годовые потери можно отразить через компонент **L**.

Шкалы для уровней угроз и уязвимостей Таблица 1

Шкалы	**Описание**	**Значение**
Шкала оценки уровней угрозы (частота возникновения)	Инцидент происходит в среднем, не чаще, чем каждые 10 лет	очень низкий
	Инцидент происходит в среднем один раз в 3 года	низкий
	Инцидент происходит в среднем раз в год	средний
	Инцидент происходит в среднем один раз в четыре месяца	высокий
	Инцидент происходит в среднем раз в месяц	очень высокий
Шкала оценки уровня уязвимости (вероятность успешной реализации угрозы)	В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию меньше 0,33	низкий
	В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию от 0,33 до 0,66	средний
	В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию выше 0,66	высокий
	В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию меньше 0,33	низкий

	0.1	0.1	0.1	0.34	0.34	0.34	1	1	1	3.33	3.33	3.33	10	10	10
	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1
1	1000	1.0E+01	5.0E+01	1.0E+02	3.4E+01	1.7E+02	3.4E+02	1.0E+02	5.0E+02	1.0E+03	3.3E+02	1.7E+03	3.3E+03	5.0E+03	5.0E+03	1.0E+04
2	10000	1.0E+02	5.0E+02	1.0E+03	3.4E+02	1.7E+03	3.4E+03	1.0E+03	5.0E+03	1.0E+04	3.3E+03	1.7E+04	3.3E+04	5.0E+04	5.0E+04	1.0E+05
3	30000	3.0E+02	1.5E+03	3.0E+03	1.0E+03	5.1E+03	1.0E+04	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.0E+04	1.0E+05	1.5E+05	1.5E+05	3.0E+05
4	100000	1.0E+03	5.0E+03	1.0E+04	3.4E+03	1.7E+04	3.4E+04	1.0E+04	5.0E+04	1.0E+05	3.3E+04	1.7E+05	3.3E+05	5.0E+05	5.0E+05	1.0E+06
5	300000	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.1E+04	1.0E+05	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.0E+05	1.0E+06	1.5E+06	1.5E+06	3.0E+06
6	1000000	1.0E+04	5.0E+04	1.0E+05	3.4E+04	1.7E+05	3.4E+05	1.0E+05	5.0E+05	1.0E+06	3.3E+05	1.7E+06	3.3E+06	5.0E+06	5.0E+06	1.0E+07
7	3000000	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.1E+05	1.0E+06	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.0E+06	1.0E+07	1.5E+07	1.5E+07	3.0E+07
8	1E+07	1.0E+05	5.0E+05	1.0E+06	3.4E+05	1.7E+06	3.4E+06	1.0E+06	5.0E+06	1.0E+07	3.3E+06	1.7E+07	3.3E+07	5.0E+07	5.0E+07	1.0E+08
9	3E+07	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.1E+06	1.0E+07	3.0E+06	1.5E+07	3.0E+07	1.0E+07	5.0E+07	1.0E+08	1.5E+08	1.5E+08	3.0E+08
10	1E+08	1.0E+06	5.0E+06	1.0E+07	3.4E+06	1.7E+07	3.4E+07	1.0E+07	5.0E+07	1.0E+08	3.3E+07	1.7E+08	3.3E+08	5.0E+08	5.0E+08	1.0E+09

Рис. 2. Матрица ожидаемых годовых потерь

CRAMM Measure of Risk	"Annual Loss of Expectancy"
1	<£1,000
2	<£10,000
3	<£100,000
4	<£1,000,000
5	<£10,000,000
6	<£100,000,000
7	<£1,000,000,000

Рис. 3. Шкала оценки

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln.	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Рис. 4. Матрица оценки риска

Третий этап исследования заключается в поиске адекватных контрмер. Здесь CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням.

Относительно интегрированного представления параметров риска для CRAMM (аналогично методике COBRA) можно определить значения: **E, A, C, M**. Компонент **A** отображается действием которое привело к нарушению характеристик ИБ, что можно показать на примере "оценки угрозы", а именно A_2="Несанкционированный доступ" может привести к E_1="Нарушение конфиденциальности (НК)". Характеристика ситуация в приведенных запросах соответствует C_o, а для инициализации данных используется качественная и количественная шкалы, что в свою очередь соответствует идентифицирующему параметру $M_{кч}$ и $M_{кл}$.

После прохождения всех этапов в результате имеем полное описание ИС. Оценка угроз и уязвимостей осуществляется на основе оценки риска по двум факторам – риск рассматривается как комбинация вероятности реализации угрозы и уязвимости, а также ущерба [21, 27]. В процессе оценивания угрозы и уязвимости все балы суммируются и полученное значение относительно определенного диапазона, отображает их степень. Например, если сумма балов для угрозы равна 25, то она определяется как средняя, при этом используемая шкала для степени угрозы следующая: до 9 балов – очень низкая; от 20 до 29 – средняя; 40 и более – очень высокая. Аналогично для уязвимости, например, если сумма балов равна 53, то она оценивается как высокая, а шкала для степени уязвимости следущая: до 9 балов – низкая; 20 и более – высокая. Эта методика подходит для уже существующих систем и малопригодна на стадиях их разработки, поскольку для качественной оценки риска требуется полное описание ИС компании.

После проведенного анализа с учетом [19] составим кортеж для данного метода: **<E, A, C, M, F, P, L>**, а, например, относительно запроса с A_2="Несанкционированный доступ" его идентифицирующие параметры принимают конкретные значения: $E_{нк}$, A_2, $C_н$, $M_{кл}$.

И так, проведенный анализ базовых понятий управления риском дал возможность конкретизировать их для сферы ИБ, относительно этого построить схему зависимости

процессов связанных с управлением рисков и интегрированными параметрами, что даст возможность унифицировать процесс исследования существующих методов, методик анализа и оценки риска, а также повысит эффективность осуществления их выбора.

Литература

1. Caelli W. Information Security for Managers. / Caelli W. D. Longley & M. Shain. // Stockton Press. – UK. – 1989.
2. CCSDS (Consultative Committee for Space Data Systems) Guide for secure system interconnection informational report CCSDS 350.4-G-1 Green book November 2007 // [Электронный ресурс] – Режим доступа: http://public.ccsds.org/publications/archive/350x4g1.pdf.
3. Control Objectives for IT and reated Technology COBIT 4.1 Framework Control Objectives Management Guidelines Maturity Models.
4. Hill, Scott & Martin Smith. Computers & Security. Risk Management & Corporate Security – 1995 – P. 199 – 204.
5. ISO/IEC Guide 73:2002. Risk management – Vocabulary – Guidelines for use in standards.
6. Lichtensteir S. Factors in the Selection of a Risk Assessment Method / Lichtensteir S. // Department of Information Systems – Monash University. Australia.
7. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology / NIST, Special Publication 800-30 [Электронный ресурс] – Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
8. Securing Europe's Information Society Regulation 2004/460 Inventory of risk assessment and risk management methods.
9. Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance: COBRA. [Электронный ресурс] – Режим доступу: http://www.riskworld.net/.
10. Security Risk Assessment Methodology for Communities (RAM-C) Cal Jaeger, PhD Security Systems and Technology Center Sandia National Laboratories Albuquerque, New Mexico.
11. Smith M. Commonsense Computer Security, your practical guide to information security / Smith M // McGraw – Hill. London. 1993 – 105 p.
12. Анализ и оценка рисков. [Электронный ресурс] – Режим доступа: http://www.risk24.ru/analiz.htm
13. Бартон Т.Л. Риск-менеджмент / Бартон Т.Л., Шенкир У.Г., Уокер П.Л. // Практика ведущих компаний: пер. с англ.– М. : Издательский дом “Вильямс”, 2008. – 208 с.
14. Глоссарий [Электронный ресурс] – Режим доступа: http://www.glossary.ru
15. ГОСТ Р 51897-2002 Менеджмент риска. [Электронный ресурс] / Термины и определения (принят постановлением Госстандарта РФ от 30 мая 2002 г. N 223-ст) Risk management. Terms and definitions – Режим доступа: http://sklad-zakonov.narod.ru/gost/Gr51897-2002.htm
16. ГОСТ Р 51901-2002 Управление надежностью. Анализ риска технологических систем [Электронный ресурс] – Режим доступа: http://zodchii.ws/normdocs/info-2065.html
17. Захаров А.И. Информационные системы: оценка рисков [Электронный ресурс] / Захаров А.И., ведущий специалист по информационной безопасности Securance Technologies, к.т.н. // Опубликовано: Журнал “Information Security/ Информационная безопасность” – 2005. №6 – С. 18 – 19 – Режим доступа: http://www.itsec.ru/articles2/actual/inform_sist_ocenka_riskov.
18. Корченко А.Г. Анализ и определение понятия риска для его интерпретации в области информационной безопасности / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Научно-технический журнал “Защита информации” – 2010. – №3. – С. 5-10.
19. Корченко А.Г. Интегрированное представление параметров риска / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Научно-технический журнал “Защита информации” – 2011. – №1. – С. 96-101.
20. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А.Г. – К. : “МК-Пресс”, 2006. – 320с. (ил. Монография).
21. Медведовский И. Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ [Электронный ресурс] / Медведовский И. – Режим доступа: http://www.ixbt.com/cm/informationsystem-risks012004.shtml
22. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
23. Петренко С. А Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. - М.: Компания АйТи ; ДМК Пресс, 2004. - 384 с.: ил.
24. Руководство по управлению рисками безопасности. [Электронный ресурс] / Группа разработки решений Майкрософт по безопасности и соответствию, регулятивным нормам и Центр Microsoft security center of excellence. – Режим доступа: http://www.microsoft.com/rus/technet/security/guidance/complianceandpolicies/secrisk/

25. Словарь бизнес-терминов [Электронный ресурс] – Режим доступа: http://dic.academic.ru/dic.nsf/business/13134.

26. Современные методы и средства анализа и контроля рисков информационных систем компаний [Электронный ресурс] / Илья Медведовский // (Опубликовано на "SecurityLab") – 2004. – Режим доступа: http://www.securitylab.ru/analytics/216326.php

27. Управление рисками. Метод CRAMM [Электронный ресурс] / Алексеев А. // ЗАО «ИТ Эксперт». – 2010. – С. 1 – 5. – Режим доступа: http://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf

28. Широков К. П. “Большой советской энциклопедии” [Электронный ресурс] / “Советская энциклопедия” в 1969 — 1978 годах в 30 томах. – Режим доступа: http://slovari.yandex.ru

Надійшла: 08.06.2011 р.

Рецензент: д.т.н., проф. Корченко О.Г.