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

СОВРЕМЕННЫЕ СРЕДСТВА УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

В работе проведено исследование широкого спектра существующих методик и программного обеспечения управления информационными рисками относительно набора параметров, характеризующих риск. К этим параметрам принадлежат: событие, действие, характеристика ситуации, мера, вероятность, опасность, затраты и потери. Для этих средств с учетом интегрированных параметров риска составлен кортеж, который даст возможность унифицировать процесс сравнительного анализа соответствующего инструментального программного обеспечения, что повысит эффективность осуществления его выбора.

Ключевые слова: информационная безопасность, риск, анализ риска, оценка риска, управление риском, угроза, уязвимость, интегрированное представление параметров риска.

На сегодняшний день существует достаточно широкое множество инструментальных средств и методик управления информационными рисками, под которыми подразумевается определение параметров риска, анализ и оценка риска (АОР), а также определение операций над рисками [19]. Часто перед специалистами компании для повышения эффективности решения задач защиты информации (ЗИ) возникает вопрос о выборе соответствующего средства, удовлетворяющего текущим требованиям информационной безопасности (ИБ). В работе [19] осуществлен анализ и раскрытие понятий связанных с управлением риском и последующей его интерпретацией в области ИБ. На этой основе, с учетом интегрированного представления параметров риска (ИППР) [17], проанализированы такие инструментальные средства как COBRA и CRAMM. Предложенный подход, в отличие от известных исследований [14, 18, 20, 21, 24], позволяет относительно ИППР унифицировать процесс анализа соответствующих инструментальных средств, что даст возможность повысить эффективность осуществления их выбора.

В связи с этим, целью данной работы является проведение анализа широкого спектра существующих методик и программного обеспечения (ПО) АОР (с использованием предложенного в [16, 17, 19] подхода) для определения набора параметров, по которым можно осуществить сравнительный анализ таких средств оценивания с возможностью дифференциации этих параметров на те, которые требуются на входе (входные данные) и те, которые необходимо получить в результате АОР (выходные данные).

В работе [17] для интегрированного представления параметров риска с отображением на сферу ИБ, предлагается представить его в виде десятикомпонентного кортежа <E, A, M, C, P, D, S, F, L, V>, где E – событие, A – действие, M – мера риска, C – характеристика ситуации, P – вероятность, D – опасность, S – ситуация выбора, F – частота, L – затраты и потери (расходы), V – отклонение от цели. Относительно этого представления осуществляется анализ современных средств управления информационными рисками.

Методика RiskWatch (США). Методика отображает требования стандартов ISO 27001 и 27002, NIST а также COBIT IV. Входные данные. Анализ и оценка риска происходит в 4 фазы [20]: 1) *Описание ИС организации с точки зрения ИБ* – определение предмета исследования; 2) *Ввод данных*. Для выявления возможных уязвимостей используется тематический вопросник, база которого содержит более 600 запросов; 3) *Оценка риска*. На этом этапе рассчитывается профиль рисков, и выбираются меры обеспечения безопасности; 4) Генерация отчета.

Выходные данные. После прохождения всех фаз, для аналитиков в отчете предоставляется следующая информация: диаграмма соответствия требованиям стандарта, диаграмма каким именно требованиям не соответствует данные ответы на запросы, таблица детального представления соответствия и несоответствия требованиям стандарта, диаграмма потерь.

В вопросах отражается все события, которые могут привести к нарушению ИБ (E) и действия (A), которые привели к этим событиям. Касательно идентифицирующего параметра M, в ПО используется $M_{кл}$, $M_{и}$. Во время ответов на вопросы присутствуют нечеткие ситуаций $C_{н}$ при выборе варианта “не знаю” и определённых $C_{о}$ при выборе точного значения

выдается на экран компьютера пользователя в виде диаграммы или на печать в виде отчета. После ввода данных высчитывается ущерб от риска, например. В отчете представлен общий риск организации с её филиалами (если таковы присутствуют) в денежном эквиваленте.

Риск в КЭС представлен как общий ущерб от всех событий риска L. Мера риска используется при оценки только $M_{кл.}$ Кортеж для этой методики <E, A, M, D, P, L>.

Методика Enterprise Risk Assessor (Risk Advisor – Новая Зеландия). Методика анализа, оценки и управления рисками, разработана компанией Methodware, соответствует требованиям австралийского стандарта Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999) и стандарта ISO17799.

Входные данные. Анализ и оценка происходит в три шага прохождения разных приложений данной методике, что позволяет структурировать оценку, сделать её более точной: 1) The Builder Tool; 2) The Assessor; 3) The Consolidation Tool.

На этапе "описания риска" задается матрица рисков, в результате риски будут описаны в соответствии с определенным шаблоном и заданы связи их с другими элементами модели. Оценка происходит с использованием качественной шкалы. На этапе "описание угроз" вначале формируется список угроз. Описание также делается на качественном уровне и позволяет зафиксировать их взаимосвязи. Во время этапа "описание потерь" описываются события (последствия), связанные с нарушением режима ИБ. Потери оцениваются в выбранной системе критериев. Для упрощения сбора данных экспертами может быть использован тематический вопросник, который составляется вручную.

Выходные данные. Последний из этапов "анализ результатов". В результате построения модели можно сформировать подробный отчет (около 100 разделов) и посмотреть на экране агрегированные описания в виде графа рисков [21, 24].

В отчете с вероятностной лингвистической шкалой, риск представлен в виде матрицы по шкале: почти наверняка, вероятно, возможно, маловероятно, редко.

Для данного ПО можно отметить присутствие идентифицирующих E, A, M, C и оценочных компонент – таких как P, L, D. В Enterprise Risk Assessor в качестве риска рассматриваются действия, которые могут привести к нарушению ИБ. Для отображения компонент риска используются качественные $M_{кч}$ и количественные $M_{кл}$ шкалы. В процессе описания риска дополнительно используются оценочные компоненты P и L (consequence – следствие, которое можно представить в виде L) при этом используются лингвистические шкалы. Во время оценки риску проставляется коэффициент значимости и уровень опасности D. Кортеж для Enterprise Risk Assessor <E, A, C, M, P, L, D>.

vsRisk, Risk Assessment Tool (Великобритания). Программное обеспечение для оценки рисков ИБ в соответствии с требованиями стандартов ISO 27001 и BS 7799-3, разработано компанией Vigilant Software Ltd.

Входные данные. Первым этапом анализа и оценки риска является выбор шкалы для вероятности и воздействия. Потом для каждого действия, например, «отказ в обслуживание» выбирается вероятность по выбранной шкале [6].

В качестве идентифицирующих параметров в ПО на этапе анализа риска используется A. Для провидения подобных оценок характеристика ситуации всегда должна быть C_o. В методике используется качественные $M_{кч}$ и количественные $M_{кл}$ шкалы. Для оценки изначально задается P и воздействие, отобразим его как D.

Выходные данные. После провидения анализа риска, выдается оценка в виде выбранного бала для вероятности. В дальнейшем эта информация используется при выводе рекомендации на соответствие стандарту ISO 27001. В ПО нет детальной оценки риска с описаниями рекомендуемых действий [6]. Кортеж для этой методики: <E, A, C, M, D, P>.

Метод OCTAVE (США). Метод анализа и оценки риска разработан институтом Carnegie Mellon Software Engineering Institute и Центром обучения, исследований и технологий (CERT), реализован в линейке продуктов: метод OCTAVE – для крупных организаций, OCTAVE-S – для небольших организаций, OCTAVE Allegro – для организаций, основное внимание которых уделяется информационным активом и порядочному подходу.

Входные данные. OCTAVE использует трехэтапный подход (фазы) для изучения организационных и технических вопросов: 1) Идентификация активов и уязвимостей. Для удобства прохождения этой фазы предлагается ответить на запросы. Первая фаза состоит из 4 процессов (идентификация ресурсов, идентификация эксплуатационных, идентификация ресурсов штата, создания профили угрозы); 2) Идентификация угроз и уязвимостей инфраструктуры. В неё входят два процесса – идентификация ключевых и оценка отобранных компонентов. В методе предлагается разделять угрозы на следующие категории: с участием человека с использованием технических средств, с участием человека с использованием физического доступа, технические проблемы, другие проблемы; 3) Развитие стратегии и планов безопасности, во время этой части оценки, команда анализа идентифицирует риски к критическим активам организации и решает, что с ними сделать. Состоит из 2 процессов – анализ и оценка риска, развитие стратегии защиты.

Выходные данные. Во время выполнения фазы 3 происходит оценка рисков для критических активов, определение ценности воздействия (высокое, среднее, или низкое) угроз к критическим активам [12].

Относительно идентифицирующих компонент, в методе присутствуют параметры E, A, C, M. Для оценки в методе используется качественные $M_{кч}$ и количественные $M_{кл}$ шкалы. Для проведения корректной оценки “характеристика ситуации” должна быть всегда C_o, для этого в методе предусмотрен детальный анализ риска. Риск в методе рассматривается как “опасность”, например, опасность потери репутации и т.д., это определяет присутствие оценочного компонента D. Кортеж для метода OCTAVE <E, A, C, M, D>.

Callio Secura 17799. Callio Secura 17799 является web-приложением, которое включает все необходимые инструменты для менеджера при разработке, внедрении, управлении и сертификации Information Security Management System (ISMS – Системы Управления Информационной Безопасностью), основанной на стандарте ISO 17799 / BS7799 [14]. С помощью Callio Secura 17799 вы примените практический метод разработки, внедрения, управления и сертификации Information Security Management System.

Входные данные. Необходимо для оценки ответить на вопросы, которые составлены согласно требованиям стандарта. Предварительно необходимо описать все бизнес-процессы и активы, которые важны для организации. В ходе описания необходимо определить критерии (3) –высокий, (2) – средний, (1) – низкий [4].

Выходные данные. После описания определенны уровень риска в виде вероятности, угрозы, уязвимости.

Оценивается вероятность возникновения P для каждого действия A, которое приводит к возникновению события E. Также необходимо выбрать на что эти действия могут повлиять. Мера риска используется $M_{и.}$ Кортеж выглядит так: <E, A, M, L, P>.

Гриф 2006. Основная задача системы ГРИФ — дать возможность ИТ-менеджеру самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе и эффективность существующей практики по обеспечению безопасности компании, а также предоставить возможность доказательно (в цифрах) убедить руководство компании в необходимости инвестиций в сферу ее ИБ.

Входные данные. Для оценки используется разработанная Digital Security классификация угроз, которая описывает все действия, которые рассматриваются во время оценки и приводят к нарушению базовых характеристик, то есть событиям. Заключительная фаза – указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз. На завершающем этапе необходимо ответить на вопросы по политике безопасности, реализованной в системе, что позволит оценить реальный уровень защищенности системы и детализировать оценки рисков. Вопросы подразумевают два вида ответа – «да» или «нет». Анализ рисков ИБ осуществляется с помощью построения модели информационной системы организации. Задается ущерб отдельно по трем угрозам (конфиденциальности, целостности, доступности) [20].

Выходные данные. Риск оценивается отдельно по каждой связке «группа пользователей – информация», то есть модель рассматривает взаимосвязь «субъект – объект», учитывая все их характеристики. Риск реализации угрозы ИБ для каждого вида информации рассчитывается по трем основным угрозам: конфиденциальность, целостность и доступность. Рассчитывается вероятность реализации угрозы. Так же рассчитывается ущерб от реализации угрозы. При работе с алгоритмом используется шкала от 0 до 100%. Максимальное число уровней – 100. Рассчитывается уровень угрозы по уязвимости на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

Анализ риска происходит с помощью идентифицирующих компонент A и E, оценка риска осуществляется с помощью оценочных компонент P, L и D. Для отображения результатов используется $M_{кл.}$ <E, A, M, L, P, D>.

@RISK. ПО @RISK проводит анализ рисков, используя моделирование Монте-Карло, с помощью Microsoft Excel. Это значит, что можно проследить какие риски принимать и каких можно избежать, принимать наилучшие решений в условиях неопределенности. Так же используется метод Value at Risk (VAR) [15].

Входные данные. Создание своей модели, заменяя неопределенными значениями в таблице с @ RISK функций распределения вероятностей, как нормальные, равномерной, или свыше 35. Происходит расчет расходов если ситуация нарушения ИБ произойдёт.

В таблице описаны действия A. Задаются вероятности P, рассчитывается L. В методе используется $M_{кл.}$. Кортеж имеет вид: <E, A, M, P, L>.

Метод на основе байесовских сетей. Метод построение каузальных моделей оценки операционных рисков, в частности, байесовских сетей. Байесовская сеть (или Байесовская сеть доверия) – это вероятностная модель, представляющая собой множество переменных и их вероятностных зависимостей.

Входные данные. Байесовская сеть представляет собой графовую модель, в которой рисковые события и причины этих событий (факторы риска) обозначаются в виде окружностей (называемых концептами графа), а причинно-следственные взаимосвязи между ними – в виде направленных стрелок (рёбер графа), соединяющих концепты [25]. В основе методологии байесовских сетей лежит теорема Байеса, ценность которой применительно к оценке ОР заключается в её способности комбинировать данные о вероятности событий, получаемые экспертным и статистическим путём. Для отдельных факторов риска (угроз), для которых нет статистики потерь, оценки вероятности рисковых событий могут быть основаны с использованием теоремы Байеса, только на экспертных знаниях; а для других — на статистике потерь, если объём собранных данных достаточен для целей моделирования.

Вероятность реализации события может быть указана в байесовской сети в виде непрерывной функции распределения или в виде таблицы вероятностей, то есть в виде дискретных вероятностей.

Выходные данные. Определяется абсолютная вероятность и величина расходов. Рассматриваются три категории последствий: нарушение целостности, доступности, конфиденциальности, а для материальных активов ущерб определяется по шкале – от полной утраты актива до сбоя (остановки, неполадки) на несущественный промежуток времени.

Для оценки используются идентифицирующие компоненты E, A и оценочные компоненты P, L, D и M. Кортеж имеет вид: <E, A, M, L, P, D>.

Методика NIST (National Institute of Standards and Technology). Методология оценки риска охватывает девять первичных шагов [11]: 1) Характеристика системы; 2) Идентификация угрозы; 3) Идентификация уязвимости; 4) Анализ контроля; 5) Определение вероятности; 6) Анализ воздействия; 7) Определения риска; 8) Рекомендации контроля; 9) Документация результатов.

Входные данные. Сбор информации, идентификация угроз: идентификация источника угрозы; причина и действия угрозы. Используются уровни вероятности: высокий, средний,

низкий. При анализе воздействия определяется события: потеря доступности, целостности, конфиденциальности. Величина воздействия определяется как: высокая, средняя, низка.

Выходные данные. Для определения риска используется матрица уровня риска: высокий, средний, низкий. В процессе анализа риска используются идентифицирующие компоненты E и A, а так же оценочные компоненты P и D. Мера риска M_u. Кортеж для данной методики – <E, A, M, P, D>.

Методика Value at Risk. VAR - это статистический подход. Методология VAR обладает рядом несомненных преимуществ: она позволяет измерить риск в терминах возможных потерь, соотнесенных с вероятностями их возникновения [15].

Входные данные. Структура VAR для оценки риска ИБ состоит из четырех стадий: 1) Идентификация угроз; 2) Оценка вероятности этих угроз; 3) Вычисление ценности в опасности; 4) Уменьшение риска. *Идентификация угроз*. Методология классифицирует угрозы как мошенничество, злонамеренные действия, шутки, попытки получить доступ к частной информации, стихийные бедствия, саботаж и ошибки пользователей.

Выходные данные. *Оценка вероятности*: есть много документов, которые описывают частоту нарушения правил безопасности. *Оценка VAR*: Когда различные риски были идентифицированы, вероятность этих рисков (распределение вероятности рисков) оценена и возможные развитые сценариев риска описаны, следующий шаг должен вычислить ценность опасности фирмы. От предполагаемого распределения вероятности худшего случая потери, вычисляют наихудшую потерю для предоставленного уровня доверия. Это значение потери - VAR. Таким образом, VAR суммирует ожидаемую максимальную потерю (или худшую потерю) по целевому горизонту в пределах данного доверительного интервала.

При анализе риска используется идентифицирующий компонент A. Во время этапов оценки используются оценочные компоненты P, D и L. Для отображения результатов оценки используется $M_{кл.}$. Кортеж для данной методики – <E, A, M, L, P, D>.

CSE (Communications Security Establishment, Government of Canada). Методика разработана на основе трех документов: 1) Справочник по управлению риском безопасности для IT систем; 2) Справочник по сертификации и аккредитации IT систем; 3) Справочник по оценки риска и выбору гарантий для IT-систем.

Входные данные. Идентификация угроз, идентификация сценария угрозы, сценарии фильтра угрозы.

Выходные данные. Оценка риска обеспечивает меру риска для каждого сценария угрозы, отражая его воздействие и вероятность. Метод назначения риска должен составлять число случаев области безопасности, или через оценки воздействия или вероятности (или оба). Эта форма оценки риска – среднее предвкушение потери (СПП) за данный период времени [1].

При анализе угроз используется идентифицирующий компонент A. Во время оценки используется оценочные компоненты P, D и M. <E, A, M, P, D>.

RiskPAC (разработчик – компания CSCI, Нидерланды). Программа анализа риска RiskPAC, обнаруживает и помогает устранять уязвимости в информационных системах и данных безопасность.

Входные данные. Необходимо ответить на вопросы. Вопросники представлены в виде реляционных баз данных. Для ответа необходимо выбрать варианты ответов. Каждый вопрос отображает определенное действие, которое приводит к нарушению ИБ. Каждый ответ имеет свой «вес по умолчанию», таким образом, происходит идентификация угроз.

Выходные данные. Подсчитывается вероятность угроз – по шкале: маловероятно, возможно, вероятно и весьма вероятно. Также, подсчитывается воздействие, по шкале: минимальное, значительное, серьёзное и катастрофическое. В состав ПО входит калькулятор ожидаемых среднегодовых потерь [24].

В ходе ответов на вопросы идентифицируется A. Во время оценки определяется P, воздействие, которое можно интерпретировать как опасность D и потери то есть расходы L. <E, A, M, L, P, D>.

Методика Facilitated Risk Analysis Process (FRAP) [14]. В методике, обеспечение ИБ информационной системы предлагается рассматривать в рамках процесса управления рисками.

Входные данные. 1) Определение защищаемых активов производится с использованием опросных листов, изучения документации на систему, использования инструментов автоматизированного анализа (сканирования) сетей. 2) Идентификация угроз. 3) Когда список угроз закончен, каждой из них сопоставляют вероятность возникновения. После чего оценивают ущерб, который может быть нанесен данной угрозой. Исходя из полученных значений, оценивается уровень угрозы. При проведении анализа, как правило, принимают, что на начальном этапе в системе отсутствуют средства и механизмы защиты. Таким образом оценивается уровень риска для незащищенной ИС, что в последствии позволяет показать эффект от внедрения средств защиты информации.

Выходные данные. Подсчитывается: вероятность (Probability): высокая (High); средняя (Medium); низкая (Low); ущерб (Impact), определим его как опасность: высокий (High Impact); средний (Medium Impact); низкий (Low Impact). Оценка определяется в соответствии с правилом, задаваемым матрицей рисков.

Анализ риска происходит с помощью идентифицирующего компонента A. Оценка риска – с использованием оценочных компонентов P и D. Результаты отображаются в $M_{кл}$. Кортеж для этой методики – <E, A, M, P, D>.

Microsoft Security Assessment Tool. Система Microsoft Security Assessment Tool (MSAT) базируется на материалах «Руководства по управлению рисками» [23]) выполняет следующие функции: 1) оценка рисков; 2) поддержка принятия решений; 3) реализация контроля; 4) оценка эффективности программы. Приложение ориентировано на организации с числом сотрудников менее 1000 человек для содействия лучшему пониманию потенциальных проблем в сфере ИБ.

Входные данные. В ходе работы пользователь, выполняющий роль аналитика ответственного за вопросы ИБ, работает с двумя группами запросов. Первая из них посвящена оцениванию риска для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Создается так называемый профиль риска для бизнеса. Запросы этой группы разбиты на 6 этапов: 1) Параметры компании; 2) Безопасность инфраструктуры; 3) Безопасность приложений; 4) Безопасность операций; 5) Безопасность персонала; 6) Среда.

Выходные данные. После реализации этапов этой группы осуществляется обработка (посредством подключения к Интернет) полученной информации и осуществляется переход к второй группе запросов. После инициализации запросов клиентская часть программной системы вновь обращается к удаленному серверу и генерирует отчеты. Наибольший интерес представляет “Полный отчет”, содержащий предлагаемый список приоритетных действий. На этапе анализа риска производится идентификация активов, предлагается их качественная классификация (высокое, среднее и низкое влияние на бизнес), а также определяется перечень угроз и уязвимостей. На этапе оценки риска определяется потенциальный ущерб, по трехуровневой шкале (высокая, средняя и низкая подверженность воздействию). Относительно ИППР в ПО отображены E, A, C, M. При оценивании риска, возможны варианты, когда респондент недостаточно осведомлен о ситуации, которая идентифицируется в запросе, при этом инициируется вариант “не знаю”, что соответствует значению $C_н$, в противном случае – $C_о$. Для оценки используются качественная ($M_{кч}$) и количественная ($M_{кл}$) шкалы, а риск рассматривается как опасность D. Отметим, что кортеж для MSAT следующий: <E, A, C, M, D>.

Методика BSI-Standard 100-3. Методика BSI-Standard 100-3 [3] основывается на процессе АОР IT-безопасности, предложенного в BSI-Standard 100-3, включает семь этапов:

1) Предварительная подготовка; 2) Подготовка описания угрозы; 3) Определение дополнительных угроз. 4) Оценка угрозы (ОУ); 5) Обработка рисков; 6) Консолидация концепции ИБ; 7) Обратная связь.

Входные данные. На первом этапе определяется область ИБ, требования к ней (нормальные, высокие и очень высокие), которые рассматриваются с точки зрения обеспечения К, Ц и Д. Также проводится анализ структуры предприятия, дополнительный анализ ИБ, оценивается её текущий уровень. С помощью предложенного в методике списка угроз осуществляется их анализ для конкретного предприятия. Идентифицируются модули и целевые объекты (ЦО) защиты, которые заносятся в таблицу.

Выходные данные. Каждый модуль ЗИ связан со списком угроз, а номер и их название соответствует конкретному ЦО. Результатом прохождения этапа является список угроз конкретному объекту. Далее в обобщенной таблице угрозы сортируются по каждому ЦО.

Относительно ИППР отметим, что все множество действий (А), представлено как угрозы, приводящие к нарушению ИБ. Относительно компонента Е, следует отметить, что рассмотренные действия приводят к нарушению определенных характеристик. Для инициализации данных, используются лингвистические значения ($M_{кч}$), а характеристика ситуации всегда определена (C_o), поскольку четко фиксируется выполнение или невыполнение требований. С учетом ИППР кортеж для этой методики можем представить в виде: <E, A, C, M>.

Методика РС БР ИББС-2.2-2009. Методика РС БР ИББС-2.2-2009 [22] (Рекомендации в области стандартизации Банка России, обеспечение ИБ организаций банковской системы, Российская Федерация) АОР нарушения ИБ проводится для типов информационных активов (ИА), входящих в предварительно заданную область оценки.

Входные данные. На начальном этапе определяется: полный перечень типов ИА, входящих в область оценки; полный перечень типов объектов среды, соответствующих каждому из типов ИА области оценки; модель угроз ИБ, основанной на всех выделенных типах объектов среды всех уровней иерархии информационной инфраструктуры.

Выходные данные. Оценка риска нарушения ИБ определяется на основании КЧ оценок ($M_{кч}$) вероятности (Р) реализации угрозы (в оригинале СВР – степень возможности реализации угроз ИБ) и потенциального ущерба (D) от ее реализации (в оригинале СТП – степень тяжести последствий от потери свойств ИБ для рассматриваемых типов ИА). Оценка определяется на основе экспертного мнения специалистов службы ИБ с привлечением профессионалов в области IT. Дополнительно, следует привлекать сотрудников профильных подразделений, использующих рассматриваемые типы ИА. Риски нарушения ИБ могут быть оценены в КЛ (денежной) форме на основании оценок СВР угроз ИБ (например, в % (Р)) и СТП (например, в денежном виде (L) от величины капитала компании (ВКК)). Количественные оценки также производятся экспертными методами. При необходимости, могут использоваться шкалы [22] соответствия КЧ и КЛ оценок СВР угроз и СТП.

Отметим, что в данной системе АОР угрозы отображаются как действия (А) приводящие к нарушению ИБ. Параметр Е в методике присутствует косвенно. Относительно компонента С, следует отметить, что при использовании статистических данных характеристика ситуация всегда C_o. Входные данные основываются на КЧ и КЛ шкалах ($M_{кл}$ и $M_{кч}$). Касательно оценочных компонент, то при анализе риска используется степень потенциального ущерба, которую можно в КЧ шкалах косвенно отобразить посредством D (при переводе в КЛ шкалы – L), а также вероятность (Р) и статистические данные о частоте реализации угрозы (F). После проведенного анализа, кортеж для этой методики следующий: <E, A, C, M, D, P, L, F>.

Стандарт ISO/IEC 27005:2008. Стандарт ISO/IEC 27005:2008 [7] предоставляет рекомендации для менеджмента риском ИБ организации, в особенности поддерживая требования “Системы менеджмента информационной безопасности” (ISMS) согласно ISO/IEC 27001.

Входные данные. Осуществляется общий анализ всей информации об организации, относящейся к созданию контекста, а также производится установка основных критериев, необходимых для менеджмента рисков ИБ и определение для него области применения и границ осуществления. Осуществляется идентификация (активов, угроз, существующих

требований, уязвимостей и последствий), оценка и описание (КЛ, КЧ или их комбинация), расположение по приоритетам рисков, относящимся к организации.

Выходные данные. В ISO/IEC 27005:2008 предложена высокоуровневая и детальная ОР ИБ. Для последней может использоваться матрица с предопределёнными значениями. Для каждого актива рассматриваются соответствующие уязвимости и угрозы. Также предложена матрица определения вероятности сценария инцидента (ВСИ) Получаемое в результате значение риска измеряется по шкале от 0 до 8, может быть оценено относительно критериев принятия риска. В приложении стандарта рассмотрен пример ранжирования угроз посредством мер риска [7]. Матрица может использоваться, для связи факторов последствий (ЦА) с ВВУ (принимая в расчет аспекты уязвимости). В стандартах ISO/IEC 27001 и 27002 на этапе оценки риска ИБ дается ссылка на документ ISO/IEC TR 13335-3, который теперь представлен как ISO/IEC 27005. Отметим, что в ISO/IEC 27005:2008 в качестве риска рассматриваются действия, которые могут привести к нарушению ИБ поэтому параметр E в стандарте присутствует косвенно, что можно сказать и относительно характеристики ситуации, где C соответствует C_o. Для отображения M используются КЧ ($M_{кч}$), КЛ ($M_{кл}$) шкалы или их комбинация (M_u). В процессе анализа и оценки риска можно дополнительно идентифицировать компонент P и косвенно – D (величина потенциальных последствий), следовательно, кортеж имеет вид: <E, A, C, M, P, D>.

Методика Risk Matrix. Методика Risk Matrix [13] ориентирована на АОР и впоследствии была реализована приложением для Microsoft Excel. Основной процесс включает: планирование оценки степени риска; идентификацию задач или требований; определения; ранжирование; составление рейтинга рисков; управление планами действий; непрерывную оценку рисков. Оценки риска заключается в планировании деятельности.

Входные данные. Изначально производится идентификация риска с помощью применения экспертами “Мозгового штурма”.

Выходные данные. Далее присваиваются различные атрибуты каждому риску, такие как, например, период времени (даты начала и окончания возможной реализации) и ВВ. С помощью сценария “Если риск …, то последствия …” составляется матрица риска. Для определения воздействия используется шкала: C (критическое); S (серьезное); M_o (средние); M_i (низкое); N (незначительное), а для вероятности – (P): 0-10% (очень низкая); 11-40% (низкая); 41-60% (средняя); 61-90% (выше среднего); 91-100% (высокая). На этапе ранжирования используется метод Borda и далее составляется рейтинг риска с определением его степени – “H”, “C” или “B” [13]. Для определения наиболее приоритетных рисков используется диаграмма частот.

Рассмотрим наличие компонент относительно ИППР, в примере матрицы риска [13]. Здесь действия можно отобразить через параметр A_1=“Не обновляется ПС”, которое имеет логическую связь с E_7= “НКЦД”. В процессе АОР используются КЧ ($M_{кч}$) и КЛ ($M_{кл}$) шкалы, C соответствует C_o, а ОР основывается на F, P и косвенно – D (представлен как воздействие). Общая запись кортежа для Risk Matrix имеет следующий вид: <E, A, C, M, F, P, D>.

Методология Mehari. Методология Mehari [2] предоставляет собой структурированный подход к оценке рисков. Она дает возможность качественно и количественно оценить факторы риска и УР.

Входные данные. Для оценки предлагаются два основные варианта – использовать базы знаний (которые интегрируются в Microsoft Excel, OpenOffice) или ПС (например, Risicare которое обеспечивает более богатый пользовательский интерфейс, а также позволяет моделировать, визуализировать и оптимизировать полученные результаты).

Выходные данные. Для оценки используется структурированная модель риска, которая учитывает “факторы снижения риска” [10]. Процесс АОР реализуется в 9 этапов: 1) Идентификация риска; 2) Оценка воздействия; 3) Оценка сдерживающих факторов; 4) Оценка защитных, паллиативных и рекуперативных факторов; 5) Оценка потенциальности; 6) Оценка влияния; 7) Оценка воздействия после принятия мер по снижению и показателей сокращений воздействия; 8) Глобальная ОР; 9) Принятия решения о приемлемости или неприемлемости риска [2].

Относительно ИППР в методологии отображены идентифицирующие и оценочные параметры. Для оценки используются КЧ ($М_{кч}$) и КЛ ($М_{кл}$) шкалы, а характеристика ситуации всегда определена ($С_о$) поскольку четко фиксируется выполнение или невыполнение требований стандарта. Риск рассматривается как воздействие, которое можно интерпретировать уровнем опасности D. Отметим, что кортеж для Mehari следующий: <E, A, C, M, D>.

Стандарт ISO/FDIS 31000. Стандарт ISO/FDIS 31000 [8] описывает основные принципы АОР. В нем определены 7 основных этапов управления рисками:

1) Описание структуры организации и ее контекста;
2) Определение политики риск-менеджмента;
3) Определение ответственности;
4) Интеграция в организационные процессы;
5) Идентификация ресурсов;
6) Создание внутренних связей и механизмов отчетности;
7) Создание внешних связей и механизмов отчетности организации.

Входные данные. Для проведения АОР определяются критерии риска, которые должны отразить цели и ресурсы организации, быть совместимыми с ее политикой риск-менеджмента, определенны в начале любого процесса риск-менеджмента и постоянно пересматриваться.

Выходные данные. На этапе идентификации организация должна выявить источники риска, области воздействий, события и их причины, а также потенциальные последствия. На этапе анализа определяются последствия, вероятность и другие признаки риска. Цель оценки состоит в оказании помощи при принятии решений, основанном на результатах анализа. Оценка риска подразумевает сравнение УР (найденного во время аналитического процесса) с критериями (установленными, при рассмотрении контекста) [8].

Отметим, что относительно ИППР в стандарте рассматривается событие риска, которые можно отобразить как действие А, приводящее к нарушению ИБ, следовательно параметры А и Е в стандарте присутствуют косвенно. Входные данные основываются на КЧ и КЛ шкалах ($М_{кл}$ и $М_{кч}$), а оценочные компоненты, используемые в процессе анализа риска, представляются воздействием, которое можно отобразить через D и вероятностью риска Р. После проведенного анализа с учетом ИППР кортеж для стандарта будет <E, A, C, M, D, P>.

Методика MAGERIT. Методика MAGERIT [9] предназначена для реализации АОР, которая проводится в 3 этапа.

Входные данные. Этап 0 – Планирование. Этап 1 – Анализ риска. Состоит из 5 шагов: 1. Идентификация и оценка активов, являющихся элементами ИС ценными для организации. После ранжирования активов производится их оценка относительно стоимости.

Выходные данные. 2. Анализ и ОУ ИБ. С помощью категории угроз, которые приведены в данной методике, производится их идентификация, реализуется оценка частоты (F) (используется шкала: 100 – очень часто (ежедневно); 10 – часто (ежемесячно); 1 – обычно (ежегодно); 1/10 – редко (раз в несколько лет)) и ущерба (L); 3. Определение превентивных мер для предотвращения угрозы; 4. Оценка воздействия (D). Измерение повреждения активов связанного с угрозой; 5. Определение риска. Риск отражается вероятностью (Р) повреждения ИС и увеличивается с ростом воздействия и частоты [9]. Этап 2 – Управление рисками. Выбираются и реализуются защитные меры, а также осуществляется интерпретация значения для воздействия и остаточных рисков, проводится анализ прибыли и убытков [9]. Методика реализована в ПО “Techniques Guide”.

Рассмотренные угрозы можно интерпретировать как параметр А. Для оценивания используются КЛ ($М_{кл}$) шкалы, а касательно характеристики ситуации (С) то ей соответствует значение $С_о$ (поскольку применяются статистические данные для определения Р). В процессе оценки используются оценочные компоненты F, L, D и P. Следовательно общая запись кортежа для MAGERIT: <E, A, C, M, F, L, D, P>.

Методика Information Security RA. Методика Information Security RA [5] предоставляет возможность реализации АОР в сфере ИБ.

Входные данные. Методика состоит из 3 фаз:

Фаза 1. Документирование системы. Фаза реализуется в нескольких процессах – идентификация системной документации и активов, а также определение текущего уровня ИБ [5].

Выходные данные.

Фаза 2. Определение риска. Расчет УР для каждой пары угрозы и уязвимости, на основе вероятности (Р) того, что угроза с использованием уязвимости будет осуществлена и степень воздействия (косвенно можно отобразить как D), которую она окажет на ИС (ее данные и бизнес-функции) с точки зрения потери К, Ц и Д. Фаза 2 состоит из 6 шагов: 1. Выявление угрозы; 2. Определение уязвимости; 3. Выявление существующих элементов управления для снижения риска реализации данной угрозы (с использования уязвимости). 4. Определение ее ВВ с учетом существующих элементов управления, для чего используется семиуровневая шкала: НЗ – незначительная (маловероятно); ОН – очень низкая (вероятно два/три раза в пять лет); Н – низкая (произойдет один раз в год или меньше); С – средняя (может произойти один раз в шесть месяцев или менее); В – высокая (произойдет один раз в месяц или меньше); ОВ – очень высокая вероятность (несколько раз в месяц); ЭВ – Экстремально вероятно (несколько раз в день). 5. Оценивание степени воздействия на систему осуществляется по шестиуровневой шкале: НЗ – незначительное, МЛ – малое, ЗН – значительное, ПВ – повреждающее, СЕ – серьезное, КР – критическое. 6. Определение УР для данной пары угроза – уязвимость существующих элементов управления.

Так, компоненте А соответствуют все угрозы которые определяются в фазе 2. Они могут привести к нарушению базовых характеристик ИБ и, следовательно, может быть связано со значениями компонента Е. Анализ показал, что прямого использования его в методике нет, но прослеживается с ним логическая связь. Инициализация данных осуществляется в лингвистической форме ($М_{кч}$). При оценке риска определяется вероятность угроз Р и воздействие, которое можно отобразить параметром D. Исследования показали, что кортеж для этой системы имеет вид: <E, A, C, M, P, D>.

На основе проведенного исследования и учитывая полученные в [17, 19] результаты, в табл. 1 приведены сводные данные об интегрированных параметрах риска, которые используются в анализируемых средствах.

Исходя из проведенного анализа, специалисты с защиты информации могут выбирать необходимые им программные средства и методики, соответственно имеющимся на входе данным, или тем результатам которые они хотят получить на выходе. Например, если необходимо получить на выходе информацию о мере и вероятности риска, а также информацию о возможных потерях, то можно воспользоваться методикой RiskWatch. Если же на входе мы имеем информацию о действии, мере и вероятности возникновения риска то можно воспользоваться программным обеспечением @RISK.

Таким образом, в работе проведено исследования широкого спектра существующих методик и ПО для АОР (с использованием предложенного в [16, 17, 19] подхода). Также, определен набор параметров, по которым можно осуществить сравнительный анализ таких средств и методов, что позволяет выбрать наиболее подходящее для решения соответствующих задач ЗИ. Согласно табл. 1 наиболее полный набор параметров, как на входе, так и на выходе имеют методики CRAMM, MAGERIT и ИББС-2.2-2009. Это позволяет расширить возможности специалиста при осуществлении АОР.

Сводная таблица результатов исследования методик и ПО для АОР Таблица 1

№	Название	Информация на входе	Информация на выходе
1.	COBRA	**E, A, M, C**	**P, M**
2.	CRAMM	**E, A, M, C, F, P, L**	**E, A, M, F, P, L**
3.	RiskWatch	**E, A, C, M, F,**	**M, P, L**
4.	RA2 art of risk (RA Software Tool)	**E, A, M, C, D**	**M, D**
5.	КЭС управления ИБ «АванГард» («РискМенеджер»)	**E, A, $М_{кл}$, D, P,**	**L, $М_{кл}$,**

6.	Risk Advisor	**E, A, C, $M_{кл}$, $M_{кч}$, P, L**	**D, $M_{кч}$**
7.	vsRisk	**E, A, C, $M_{кл}$, P, D,**	**P, $M_{кл}$**
8.	OCTAVE	**E, A, C, M**	**D, M**
9.	Callio Secura 17799	**E, A, $M_{и}$, P**	**$M_{и}$, P**
10.	ГРИФ 2006 и Digital Security Office 2006	**A, E, M**	**$M_{кл}$, P, L, D**
11.	@RISK	**A, $M_{кл}$, P**	**L, $M_{кл}$**
12.	Метод на основе байесовских сетей	**A, M, P**	**P, L, D, E, M**
13.	Методика OP NIST	**A, P, E, D, M**	**P, D, $M_{и}$**
14.	Value at Risk	**A, $M_{кл}$**	**P, D, L, $M_{кч}$**
15.	CSE	**A, M**	**P, D, M**
16.	RiskPAC	**A, M**	**P, D, L, M**
17.	Методика FRAP	**A, $M_{кл}$**	**P, D, $M_{кч}$**
18.	MSAT	**E, A, C, M**	**D, $M_{кч}$, $M_{кл}$**
19.	BSI-Standard 100-3	**E, A, C, $M_{кч}$**	**$M_{кч}$**
20.	ИББС-2.2-2009	**E, A, C, M, F**	**P, D, $M_{кч}$, L**
21.	ISO/IEC 27005	**E, A, C, $M_{кч}$, $M_{кл}$**	**P, D, $M_{и}$**
22.	Risk Matrix	**A, C, D, $M_{кч}$, $M_{кл}$**	**P, D**
23.	Mehari	**E, A, C, $M_{кч}$, $M_{кл}$**	**D, M**
24.	ISO/FDIS 31000	**E, A, C, M**	**P, D, M**
25.	MAGERIT	**E, A, C, M, F**	**F, L, D, P, M**
26.	Information Security RA	**E, A, C, $M_{кч}$**	**P, D, M**

ЛИТЕРАТУРА

1. A Guide to risk assessment and safeguard selection for Information Technology Systems, [Электронный ресурс] / MG-3, Government of Canada, Communications Security Establishment (CSE) P.O., Terminal, Ottawa, Ontario, Canada, K1G 3Z4 – 1996, P. 73 – Режим доступа: http://www.cse-cst.gc.ca.
2. Amril Syalim Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide [Электронный ресурс] // Amril Syalim, Yoshiaki Hori, Kouichi Sakurai – Режим доступа: http://itslab.inf.kyushu-u.ac.jp.
3. BSI-Standard 100-3: Risk analysis based on IT-Grundschutz // Bundesamt für Sicherheit in der Informationstechnik. – 2008. – version 2.5.
4. Callio Technologies: программный комплекс управления политикой информационной безопасности компании (международный стандарт BS7799 ISO 17799) [Электронный ресурс] – Режим доступа: http://businesssoft.ru.
5. Compliant Information Security Risk Assessment Tool [Электронный ресурс] / vsRisk – ISO 27001: 2005 – Режим доступа: http://www.27001.com/products/31
6. CMS Information Security Risk Assessment (RA) Methodology. – 2002. – Version 1.1
7. ISO/FDIS 31000:2009(E) international standard Risk management – Principles and guidelines. – 2009.
8. ISO/IEC 27005 Информационная технология – Методы защиты – Менеджмент рисков информационной безопасности. BS ISO/IEC 27005:2008. – 2008. – Технический перевод v.2.6 от 4.02.2011.
9. MAGERIT Methodology for Information Systems Risk Analysis and Management Book I [Электронный ресурс] / The Method – version 2 – Режим доступа: https://www.ccn-cert.cni.es/publico /herramientas/pilar44/en/magerit/meth-en-v11.pdf.
10. Mehari – Overview // Club de la Securit ´ e de l'Information Franc¸ais ´(CLUSIF). – 2010.
11. NIST 800 – 30 Risk Management Guide for Information Technology Systems. [Электронный ресурс] / Recommendations of the National Institute of Standards and Technologyhttp – Режим доступа: //csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.
12. OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM) [Электронный ресурс] // http://www.cert.org/octave/octavemethod.html – Названия титул. с экрана.
13. Thomas R. Peltier Information security risk analysis / Thomas R. Peltier – Auerbach Pub, 2001. – P 281.
14. Risk Management Tools. Program Risk Management Tools. [Электронный ресурс] – Режим доступа: http://mitre.org/work/systems_engineering/guide/risk_management_tools.html.
15. Value at Risk: A methodology for Information Security Risk [Электронный ресурс] / Assessment. Jeevan Jaisingh and Jackie Rees Krannert // Graduate School of Management Purdue University West Lafayette – Режим доступа: http://www.gloriamundi.org/picsresources/jjjr.pdf.

16. Корченко А.Г. Анализ и определение понятия риска для его интерпретации в области информационной безопасности / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2010. – №3. – С. 5-10.

17. Корченко А.Г. Интегрированное представление параметров риска / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2011. – №1. – С. 96-101.

18. Костров Д.Д. Анализ рисков и управление ими [Электронный ресурс] / Костров Д.Д. // Byte Россия – 2003. – №10 (62) – Режим доступа: http://www.bytemag.ru/articles/detail.php?ID=6655.

19. Луцкий М.Г. Базовые понятия управления риском в сфере информационной безопасности / Луцкий М.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2011. – №2. – С. 86-94.

20. Медведовский И.С. Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ [Электронный ресурс] / И.С. Медведовский // (Опубликовано на "SecurityLab") – 2004. – Режим доступа: http://www.ixbt.com/cm/informationsystem-risks012004.shtml.

21. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. – М.: Компания АйТи ; ДМК Пресс, 2004. - 384 с.

22. Рекомендации в области стандартизации банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности. РС БР ИББС-2.2-2009. [Электронный ресурс] / Режим доступа: http://dorlov.blogspot.com/2009/07/22-2009.html

23. 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.

24. Симонов С.В. Анализ рисков в информационных системах. Практические аспекты. Защита информации [Электронный ресурс] / Симонов С.В. // Конфидент. Безопасность компьютерных систем – 2001. – №2. – С. 48-53 http://www.compulink.ru/images/complink2.pdf – Названия титул. с экрана.

25. Частиков А.П. Использование байесовской сети при разработке экспертных систем с нечеткими знаниями / Частиков А.П., Леднева И.Ю. [Электронный ресурс] / Кубанский государственный технологический университет (КубГТУ), г.Краснодар – Режим доступа: http://ito.su/2000/II/5/5152.html.

Надійшла: 15.12.2011

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