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

ИССЛЕДОВАНИЕ ПРОГРАММНЫХ СРЕДСТВ АНАЛИЗА И ОЦЕНКИ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В работе проведено исследование широкого спектра существующего программного обеспечения анализа и оценки риска относительно набора параметров, характеризующих риск. К таким параметрам относятся событие, действие, характеристика ситуации, мера, вероятность, опасность, затраты и потери. К наиболее известным программным продуктам, которые использованы для исследования, относятся RiskWatch, RA2 art of risk, Risk Advisor, OCTAVE и др. 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.

На сегодняшний день существует достаточно широкое множество инструментальных средств анализа и оценки риска (АОР). 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 [9] 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) [7] проанализированы такие инструментальные средства как COBRA и CRAMM. Предложенный подход, в отличие от известных исследований [4, 8, 10, 11, 13] дает возможность относительно ИППР унифицировать процесс анализа соответствующих инструментальных средств и повысить эффективность осуществления их выбора.

В связи с этим, целью данной работы является проведение исследования широкого спектра существующего программного обеспечения (ПО) АОР (с использованием предложенного в [6, 7, 9] подхода) для определения набора параметров, по которым можно осуществить сравнительный анализ таких средств оценивания. В качестве исходного материала исследования, было взято множество наиболее известных и используемых на практике продуктов – RiskWatch, RA2 art of risk (RA Software Tool), КЭС управления ИБ “АванГард” (“РискМенеджер”), Risk Advisor, vsRisk, OCTAVE, Callio Secura 17799, Гриф 2006, @RISK, RiskPAC и Microsoft Security Assessment Tool.

Система RiskWatch (разработчик – компания RiskWatch, США) отображает требования стандартов ISO/IEC 27001 и ISO/IEC 27002, NIST а также COBIT IV. Процесс АОР производится в четыре фазы. Фаза 1 – описание информационной системы (ИС) организации с точки зрения ИБ (определение предмета исследования). Здесь описываются такие параметры предприятия, как тип организации, состав исследуемой системы, базовые требования в области ИБ. Для облегчения работы аналитика используются встроенные списки (категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты), в каждом из которых можно осуществлять выбор тех составляющих, которые реально присутствуют в организации, например, в категории потерь могут быть позиции: задержка и отказ в обслуживании, раскрытие информации, прямые потери (например, от уничтожения оборудования при пожаре), косвенные потери (например, затраты на восстановление), жизнь и здоровье (персонала, заказчиков и т.д.), изменение данных, репутация [10] и т.д. Фаза 2 – ввод данных. Для выявления уязвимостей инициализируется тематический вопросник (ТВ), база которого содержит более 600 запросов. Задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов (активов) (рис. 1), на основании чего рассчитывается эффективность внедрения средств ЗИ (СЗИ) [10]. По аналогии с ПО COBRA в RiskWatch (для упрощения ввода и обработки данных) множество запросов ТВ инициируются посредством выбора данных из набора вариантов, например, конкретные числовые значения (0, 1 – “никогда”, 2, 3 – “редко”, 4, 5, 6 – “иногда”; 7,8 – “обычно”; 9, 10 –

"всегда") или "нет", "не знаю". Посредством запросов отражаются и оцениваются текущие правила ИБ соответственно существующим стандартам. Запросом в RiskWatch, например, может быть – "Есть ли разграничение доступа к внутренней и внешней сети, точкам доступа, отдельным компьютерам и файловым серверам?". Фаза 3 – оценка риска. Рассчитывается профиль рисков, и выбираются меры обеспечения ИБ. Для этого устанавливаются связи между ранее определенными ресурсами, потерями, угрозами и уязвимостями, а риск оценивается посредством ожидаемых потерь за год. Например, если стоимость сервера $v = 150\,000$\$, а вероятность его уничтожения при пожаре в течение года p=0,01, то ожидаемые потери составят $m = 1\,500$\$, т.е. $m = p \times v$, где p – вероятность возникновения угрозы, а v – стоимость ресурса. Отметим, что RiskWatch базируется на таких данных NIST, как LAFE (Local Annual Frequency Estimate) и SAFE (Standard Annual Frequency Estimate), соответственно отражающих годовую частоту реализации угроз в локализованной (например, в городе) и глобализованной (например, в Северной Америке) области. Используется также поправочный коэффициент, учитывающий частичное уничтожение ресурса. Получить оценки LAFE и SAFE, например, для Украины проблематично, поскольку нет необходимой статистики. К примеру, в США существует национальная программа по сбору данных об инцидентах (The Uniform Crime Reporting), что позволяет сформировать соответствующую статистическую информацию об инцидентах ИБ в общегосударственной базе. Фаза 4 – генерация отчета (рис. 2). Формируются диаграммы и таблица детального представления соответствия и несоответствия (относительно запросов) требованиям стандарта, а также диаграмма потерь. С учетом стоимости ресурса осуществляется оценка ожидаемых потерь (по конкретному активу) от реализации одной угрозы (*ALE*) [10] $ALE = A \times EF \times F$, где: A (Asset Val) – стоимость ресурса (данные, программы, аппаратура и т.д.); EF (Exposure Factor) – коэффициент воздействия (процентная часть от стоимости актива, подвергаемой риску); F (Frequency) – частота возникновения нежелательного события. Например, пусть аппаратное средство стоит A=10 000\$, коэффициент воздействия на него EF=0,5, а частота F=0,2, то ожидаемые потери составят AEL=1000\$. После идентификации активов и воздействий оценивается общий риск для ИС (сумма всех частных значений). Дополнительно используются показатели ARO (Annualized Rate of Occurrence) – ожидаемая годовая частота происшествия и SLE (Single Loss Expectancy) – ожидаемый единичный ущерб (разница первоначальной и остаточной (после происшествия) стоимости актива). Для оценивания отдельно взятой пары "угроза-ресурс" используется формула $ALE = ARO \times SLE$. Также применяются сценарии "что, если:", позволяющие описать аналогичные ситуации при условии внедрения средств защиты. Сравнивая ожидаемые потери при условии внедрения защитных мер и без них, можно оценить эффект от таких мероприятий. Для этого в RiskWatch содержатся не только базы данных LAFE и SAFE, но и базы различных СЗИ. Эффект от внедрения средств безопасности определяется параметром *ROI* (Return on Investment – возврат инвестиций), показывающий отдачу от вложений за период времени.

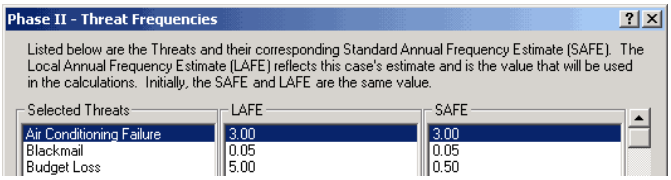

Рис. 1. Окно инициализации параметров

Theft - Company Property - AFE: 2.00
The various incident classes associated with this threat are shown in the following table:

Incident Class	SLE	ALE	% of total ALE
Delays/Denials, Communications Equipment	$26,401.	$52,801.	68.0%
Delays/Denials, Data/Information	$4,400.	$8,800.	11.3%
Delays/Denials, Physical Inventory/Product	$2,750.	$5,500.	7.1%
Direct Loss, Cash	$2,200.	$4,400.	5.7%
Delays/Denials, Production Resources	$1,100.	$2,200.	2.8%
Direct Loss, Physical Inventory/Product	$1,100.	$2,200.	2.8%
Direct Loss, Data/Information	$550.	$1,100.	1.4%
Direct Loss, Production Resources	$275.	$550.	0.7%
Direct Loss, Communications Equipment	$39.	$77.	0.1%

Рис. 2. Фрагмент отчета в RiskWatch

Относительно ИППР с учетом [9] для RiskWatch определим кортеж**.** Так компоненту **A** (исходя из указанного примера категорий потерь) соответствуют, например, значения A_1="Задержка и отказ в обслуживании", A_2="Раскрытие информации", A_3="Уничтожение оборудования" и т.д. Эти действия приводят к нарушению определенных характеристик ИБ атакованных ресурсов и соответственно связываются со значениями E_3="НД", E_1="НК",

E_5="НЦД". Анализ показал, что прямого использования параметра **E** в системе нет, но прослеживается логическая связь с ними, поэтому считаем его присутствие косвенным. Здесь и далее косвенные параметры в кортеже будут обозначаться не полужирным шрифтом. При оценивании риска, возможны случаи, когда респондент не осведомлен о ситуации, которая идентифицируется в запросе, тогда он использует вариант "не знаю", что характеризирует ситуацию как неопределенную, т.е. **C** соответствует значение $C_н$, иначе, как определённую $C_о$. Инициализация данных производится в числовой и лингвистической формах, что в свою очередь можно отобразить компонентом **M** ($M_{кл}$ и $M_{кч}$). Анализ риска происходит во время обработки данных инициируемых через ТВ, который используется при прохождении фазы 1. Для определения *ALE* используется оценочный компонент **F**, а риском являются ожидаемые потери за год, которые также можно интерпретировать как расходы **L.** С учетом ИППР, кортеж для этой методики можно представить в виде **<**E**, A, C, M, F, L>**, а например, относительно запроса о разграничении доступа его идентифицирующие параметры (ИП) принимают конкретные значения – $E_{нк}$, A_2, $C_о$, $M_{кл}$.

Инструментарий RA2 art of risk (RA Software Tool, разработчик – компании AEXIS Security Consultants и XiSEC Consultants Ltd., Великобритания) представляет собой ПО для реализации системы менеджмента информационной безопасности (СМИБ) соответственно требованиям ISO/IEC 27001:2005. Состоит из восьми модулей: область СМИБ и масштабы оценки риска; идентификация активов; оценка активов; оценка угроз/уязвимостей; идентификация и оценка риска; решения по обработке риска; утверждение принимаемых мер; выполнение мер и отбор средств управления. В процессе выполнения каждого модуля производится инициализация запросов с помощью выбора фиксированных значений в бинарно-лингвистической форме ("да", "нет"). Для оценки риска используются восемь уровней: 1 – тривиальный; 2, 3 – минорный; 4, 5 – значительный; 6, 7 – большой; 8 – катастрофический, а матрица риска, строится на основе уровней опасности предприятия и вероятности риска в лингвистических шкалах. Значение риска формируется в виде уровней по каждой представленной категории в лингвистическом и цифровом виде, например, значению "большой уровень" соответствует число 7 [11].

Относительно ИППР определим значения **E, A, C** и **M.** Все действия **(A)**, отображаемые запросами, представлены в виде требований стандарта, например, "Была ли проведена оценка для выявления рисков связанных с доступом третьих лиц (ДТЛ)?", "Была ли одобрена политика ИБ с руководством?" и т.д., в этой связи параметр **A** можно отразить комплексно A_i, $i = \overline{1,a}$ (где a – количество идентификаторов угроз). Так, например, в запросе о ДТЛ при невыполнении данной оценки, могут возникнуть действия, приводящие к нарушению базовых характеристик ИБ, тогда **A** можно представить множеством $A_{ДТЛ} \in \{A_{ДТЛi}\} i = \overline{1,a}$, где, например, $A_{ДТЛ1}$= "Кража". Относительно компонента **E**, следует отметить, что рассмотренные действия (исходя из указанного примера запросов) приводят к нарушению определенных характеристик ИБ и может быть косвенно связано со значением E_7="НКЦД". Анализ показал, что параметр E в ПО присутствует косвенно. Для инициализации данных, используются числовые и лингвистические значения ($M_{кл,}$ и $M_{кч}$), а характеристика ситуации всегда определена ($C_о$) поскольку четко фиксируется выполнение или невыполнение требования стандарта. В методике присутствуют оценочные компоненты **D** (уровни опасности) и **P** (вероятность риска), следовательно, риск отображается как опасность (**D**) для организации (при наступлении рисковой ситуации). С учетом ИППР кортеж для этой методики можем представить в виде: **<**E**, A,** C**, M, D, P>**, а например, относительно запроса ДТЛ, его ИП принимают конкретные значения – $E_{нкцд}$, $A_{дтл}$, $C_о$, $M_{кч}$**.**

Система КЭС управления ИБ "АванГард" **(**Комплексная экспертная система "АванГард", разработчик – Лаборатория системного анализа проблем информатизации Института системного анализа РАН, Россия) включает комплекс методик: идентификации критически важных сегментов и объектов информационной инфраструктуры на основе АОР нарушения ИБ автоматизированных ИС (АИС); управления рисками нарушения ИБ больших

компьютеризированных организационных систем; построения системы требований ИБ критически важных сегментов и объектов АИС; мониторингового контроля над состоянием критически важных сегментов и объектов АИС. Основывается система на двух программных комплексах – “АванГард-Анализ” и “АванГард-Контроль” [8].

Изначально производится анализ событий риска (**A**) посредством построения их моделей с помощью интерфейса главной формы (рис. 3), где в верхнем секторе содержится таблица со списком моделей событий рисков, по каждой из которых в заданных графах указываются экспертные оценки цены риска (в условных единицах) и вероятности (в процентах) его событий. При материальном ущербе условной единице рекомендуется присваивать ценовой эквивалент, например, 1000 руб. При событиях риска, ущерб от которого сложно оценить в денежном выражении, используются балльные оценки, по которым ранжируются события риска по степени их опасности. В графе “Ущерб” идентифицируется расчетное значение риска по произведению его цены на вероятность. В следующем секторе представлена таблица угроз, реализация которых может привести к событию риска. Для каждой из угроз указывается вес заданного события (рискообразующий потенциал (РП) угрозы по событию риска). Для оценки необходимо: выбрать класс объекта с описанием действия, которое приводит к риску (определить его идентификатор); для каждого риска установить денежный эквивалент; рассмотреть события риска, которые могут возникнуть в результате реализации этих угроз (для определения значимости угроз, входящих в состав нормативной модели). Как правило, каждое событие это результат реализации некоторой совокупности угроз. Это дает возможность, путем анализа одного события, выявить значимость не одной, а сразу нескольких угроз. Совокупность описания события риска, перечня угроз, оценок вероятности события, цены риска, а также аналитическое обоснование данных оценок составляют то, что в данной системе называется моделью события риска, которая строится по каждому возможному с точки зрения экспертов событию [8].

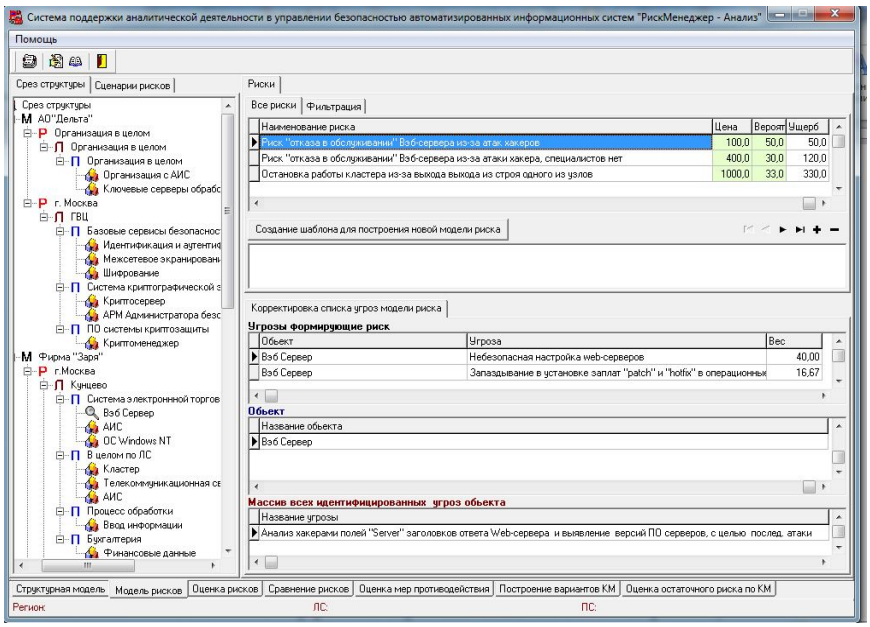

Рис. 3 Интерфейс построения моделей событий риска

Отметим, что относительно ИППР в КЭС рассматривается событие риска, отображаемое как действие **A,** которое приводит к нарушению ИБ, например, A_1= “Отказ обслуживания веб-сервера из-за атаки хакера”, A_2= “Падение криптосервера из-за перегрузки”, A_3= “Перехват пользовательских паролей” и т.д. В описании действий (наименований риска) используются статистические данные, собранные иностранными компаниями, и которые не всегда могут быть использованы для различных регионов (например, в Украине) из-за влияния на природу возникновения инцидентов ИБ многих специфических факторов, таких как, например, уровень жизни, образованности населения,

его менталитет и т.д. Рассмотренные в примере действия (**A**) могут быть связаны с событиями (**E**) нарушения базовых характеристик ИБ, например, A_1 с E_3="НД", A_2 с E_7="НКЦД", а A_3 с E_1="НК" и т.д., следовательно параметр Е в системе присутствует косвенно. Входные данные основываются на качественных и количественных шкалах ($M_{кл}$ и $M_{кч}$). Касательно оценочных компонент, которые используются в процессе анализа риска, присутствуют степень опасности **D** и вероятность события риска **P.** Так же используется показатель ущерба, который отображается посредством **L**. Определение уровня риска по объектам, подсистемам (процессам), локальным средам, регионам и для модели в целом, производится путем суммирования показателей значимостей угроз (относимых в рамках структурной иерархической модели к соответствующим структурам). То есть РП объекта, будет равен сумме РП угроз с ним связанных, а РП подсистемы (процесса) будет равен сумме РП включенных в нее объектов. Результат вычислений представляется в виде диаграммы. Оценкой ущерба, по аналогии с RiskWatch (фаза 3), соответствует произведению цены риска и вероятности его события. В отчете отображается общий риск организации в денежном эквиваленте. Отметим, что он представляется как общий ущерб от всех событий риска и может отображаться оценочным компонентом **L** который в системе присутствуют косвенно, а при оценке риска используется количественная шкала ($M_{кл}$). После проведенного анализа с учетом ИППР кортеж для КЭС будет **<E, A,** C**, M, D, P,** L**>.**

Система Enterprise Risk Assessor (Risk Advisor, разработчик – компания Methodware, Новая Зеландия) соответствует требованиям австралийского стандарта Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999) и ISO/IEC 17799. Представлена в трех продуктах: CobiT Advisor 3rd Edition (Audit); PRo Audit Advisor; Planning Advisor. Процесс АОР производится в три шага, что позволяет структурировать оценку, сделать её более точной. Шаг 1: Приложение The Builder Tool – инструмент для создания структуры оценки риска и аудита (сбор информации). Оно позволяет построить структуру ИС, включая способность добавлять или скрывать любую часть функциональных возможностей. Основные этапы работы в этом приложении состоят из описания ИС, рисков, угроз, потерь и анализа результатов. На этапе "Описание риска" создается матрица (рис. 4), позволяющая описать риски в соответствии с определенным шаблоном и задать их связи с другими элементами модели. Оценка происходит на основе $M_{кч}$, а риски разделяются на приемлемые и неприемлемые. Далее выбираются управляющие воздействия (контрмеры) с учетом зафиксированной ранее системы критериев, эффективности контрмер и их стоимости. Стоимость и эффективность также оцениваются в качественных шкалах. На этапе "Описание угроз" изначально формируется список угроз, осуществляется их классификация, и описываются связи с рисками. Описание также делается на качественном уровне, что позволяет зафиксировать их взаимосвязи. На этапе "Описание потерь" описываются события (последствия), связанные с нарушением режима ИБ. Потери оцениваются в выбранной системе критериев. Для упрощения сбора данных эксперты могут использовать ТВ, составляемый вручную. После сбора информации переходим к оценке риска. Шаг 2: The Assessor – экспертная оценка (анализ собранной информации). Шаг 3: The Consolidation Tool – инструмент консолидации (интегрирует все индивидуальные оценки риска). После построения модели формируется отчет (около 100 разделов) и агрегированное описание в виде графа рисков [11, 13]. В отчете (рис. 5) с вероятностно-лингвистической шкалой, риск представлен в виде матрицы с градациями: почти наверняка, вероятно, возможно, маловероятно, редко. Рассмотрим пример описания и оценки риска (рис. 6). В процессе описания экспертами указывается владелец и степень риска, последствия и вероятность, далее производится оценка.

При ИППР для данного ПО, можно получить отображение ИП **E, A, M, C** и оценочных – **P, L, D.** В Enterprise Risk Assessor в качестве риска рассматриваются действия, которые могут привести к нарушению ИБ, например, A_1= "Кража документов" может находится в логической связи с E_1="НК" и поэтому параметр Е в ПО присутствует косвенно,

что можно сказать и относительно характеристики ситуации (см. рис. 6), где С соответствует C_o.

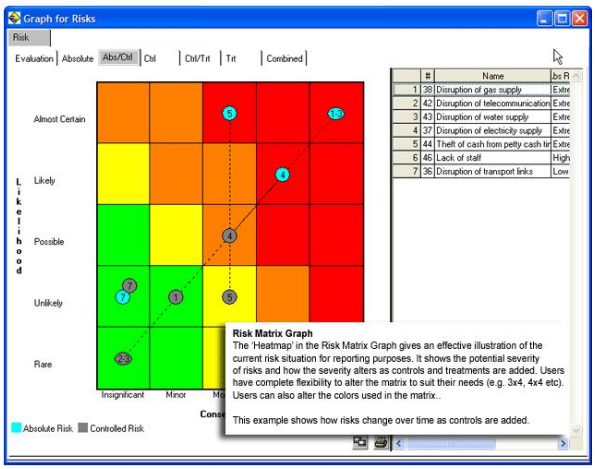

Рис. 4 Матрица риска

Также из рис. 4 и рис. 5 видно, что для отображения **M** используются качественные ($M_{кч}$) и количественные ($M_{кл}$) шкалы. В процессе анализа риска можно дополнительно идентифицировать оценочные компоненты в явном виде **P** и косвенном **L** (consequence – следствие, которое можно представить в виде L), а во время его оценки – устанавливается коэффициент значимости и уровень опасности **D,** следовательно, кортеж имеет вид: **<E, A,** C**, M, P,** L**, D>.**

Система vsRisk, Risk Assessment Tool (разработчик – компания Vigilant Software Ltd., Великобритания) предназначена для оценки риска ИБ в соответствии с требованиями ISO/IEC 27001 и BS 7799-3. Для упрощения процедуры АОР используются визарды, для чего выбираются шкалы (устанавливаются уровни) вероятности и воздействия. Далее каждому действию, например, “Отказ в обслуживании” определяется вероятность по выбранной шкале. В качестве ИП на этапе анализа риска служит **A** и, например, согласно рис. 7 он может принимать значение A_3= “Отказ в обслуживании”, что приводит к E_3=“НД” (рис. 8). Система предоставляет средства для оценки всех факторов рисков, включая угрозы, уязвимости, активы и механизмы

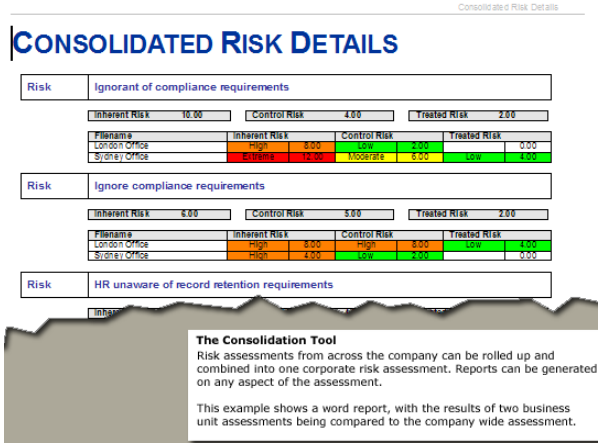

Рис. 5 Фрагмент отчета

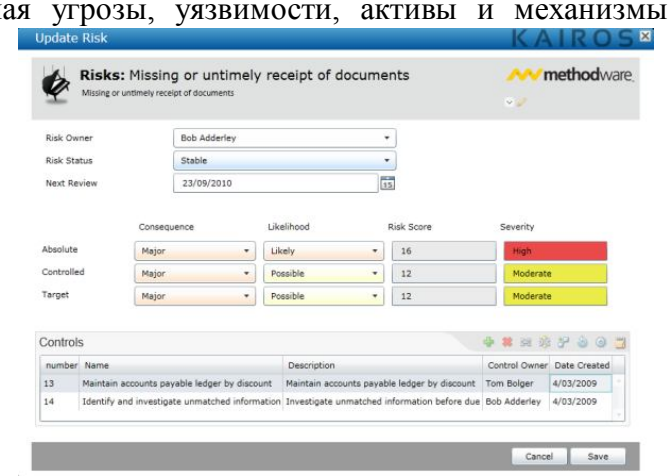

Рис. 6 Пример описания риска.

контроля и не содержит средств для количественной оценки величины риска, ограничиваясь только качественными шкалами ($M_{кч}$). Для таких оценок характеристика ситуации отображается через C_o. Отметим, что для оценки задаются масштабы вероятности **P** и воздействия рассматриваемых угроз, которое можно косвенно, отобразить через уровни **D.** Все изменения, вносимые в базу данных продукта по ходу работы, подробным образом фиксируются в журнале аудита. После анализа риска, выдается оценка в виде выбранного бала для вероятности, например, 2. По результатам оценки формируются “Декларации о применимости механизмов контроля” и “План обработки рисков” в соответствии с требованиями стандарта ISO/IEC 27001. В дальнейшем эта информация используется при выводе рекомендаций на соответствие этому стандарту. В vsRisk нет детальной оценки риска с описанием дальнейших рекомендуемых действий (рис. 8) [2]. Отметим, что с учетом ИППР кортеж для этого ПО следующий: **<E, A,** C**, M,** D**, P>.**

Система OCTAVE (разработчик – институт Carnegie Mellon Software Engineering Institute и Центр обучения, исследований и технологий (CERT), реализован в линейке продуктов: метод OCTAVE, OCTAVE-S и OCTAVE Allegro – для крупных, средних и малых организаций соответственно, США) использует трехэтапный подход для изучения

организационных и технических вопросов. Этап 1 – “Идентификация активов и уязвимостей” состоит из четырех процессов: “Идентификация ресурсов управления” (собирается информация о важных активах, требованиях ИБ, угрозах и уязвимостях от представителей компании); “Идентификация эксплуатационных ресурсов” (собирается информация, как в предыдущем процессе, с отобранных эксплуатационных областей); “Идентификация ресурсов штата” (собирается информация аналогично с предыдущими процессами, от общего штата отобранных эксплуатационных областей); “Создание профилей угроз” (выбирается 3 ÷ 5 критических ресурсов, для которых и определяются профили угроз). Для прохождения этого этапа в системе предлагается инициализировать ТВ (рис. 9). Этап 2 – “Идентификация угроз и уязвимостей инфраструктуры” содержит два процесса: “Идентификация ключевых компонент” (составляется представительный набор ключевых компонент системы, которые поддерживают или обрабатывают критические информационно-связанные активы); “Оценка отобранных компонент” (производится оценка отобранных компонент и анализ результатов). Угрозы разделяют на следующие категории: с участием человека и использованием технических средств; с участием человека и использованием физического доступа; технические проблемы; другие проблемы. В процессе прохождения этапа 2, риск определяется как функция $R(T,I)$, где T – угроза (threat)/условие (condition), а I – воздействие (impact)/следствие (consequence).

Также детально описывается, ущерб, который будет нанесен компании в случае наступления ситуации риска. Рассмотрим пример сценария угрозы (условие) – неправильная политика разграничения доступа позволяет сотруднику случайно получить доступ к медицинским записям другого сотрудника; воздействие (следствие) – медицинские записи сотрудника раскрываются, в результате поданного им иска, организация обязана выплатить штраф в размере 50 000$. Эта угроза оказывает прямое воздействие на репутацию предприятия, что может повлечь за собой потенциальные денежные потери (судебные иски, возможные штрафы, пеня др.). Этап 3 – “Развитие стратегии и планов безопасности” (идентифицируются риски к критическим активам организации и принимаются решения по их обработке) состоит из двух процессов: “Анализ и оценка риска” (определяется уровень воздействия (высокое, среднее, низкое) угроз критическим активам); “Развитие стратегии защиты” (команда развивает стратегию защиты всей организации, сосредотачиваясь на улучшении методов обеспечения ее ИБ [3]).

Используя указанный пример (с медицинскими записями) рассмотрим процесс оценки (при этом используется шкала – средний, низкий, высокий) относительно заданной сферы действия риска (табл. 1). В дальнейшем при общей оценке для каждой сферы присваивается коэффициент уровня риска: высокий – 3, средний – 2, низкий – 1. Полученные балы по

Container Type	Questions to Consider
Technical (*see* Worksheet 9a)	*Internal* ❑ What information systems use or process this information asset? *Example:* • *The vendor database (information asset) is used by the accounts payable system (system).* ❑ What automated processes are reliant on this information asset? *Example:* • *Paying an invoice (process) requires information in the vendor database (information asset) and is automated in the accounts payable system (system).* ❑ On what hardware might this information asset be found? Consider: • If the information asset is used by a system, application, or process, what underlying hardware is related to the information asset? *Examples:* • *The vendor database is stored on the “DIAMOND” server.* *External*

Рис. 9. Пример запросов для этапа 1

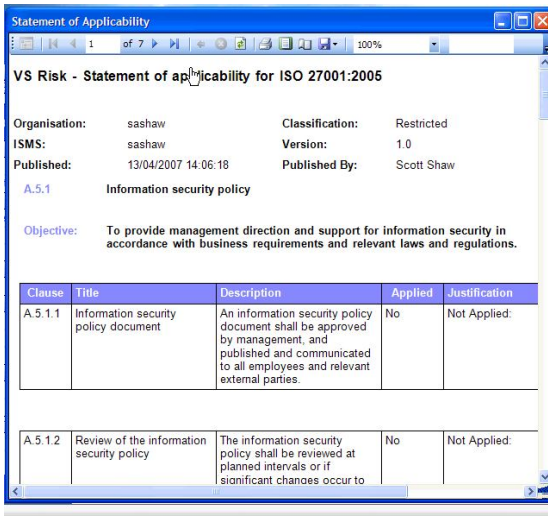

Рис. 10. Отчет соответствия

каждой угрозе в процессе AOP суммируются (рис. 11).

Пример процесса оценки риска Таблица 1

Сфера действия риска	Уровень риска
репутация / доверие клиентов	средний
финансы	низкий
производительность	низкий
безопасность и здоровье	низкий
штрафы	высокий

Приведем ИППР, относительно идентифицирующих компонент, в ПО присутствуют параметры **E, A, C** и **M**. В рассмотренном примере сценария угрозу можно представить как параметр A_1="Несанкционированный доступ к медицинским записям", который может логически привести к E_1= "НК". Для оценивания в OCTAVE используются качественные ($M_{кч}$) и количественные ($M_{кл}$) шкалы, а **C** соответствует C_o. Риск рассматривается как "Опасность", например, потеря репутации и т.д., что связывается с оценочным компонентом **D**. Как видно общая запись кортежа для OCTAVE: **<E, A, C, M, D>** а, например, относительно рассмотренного сценария угрозы его ИП принимают частные значения – $E_{нк}$, A_1, C_o, $M_{кл}$.

Инструментарий Callio Secura 17799 (разработчик – компания Callio Technologies, Канада) является web-приложением, включающим все необходимое для менеджера при разработке, внедрении, управлении и сертификации СМИБ, согласно ISO/IEC 17799 / BS7799 [4]. Система содержит четыре секции: "Методология" – помощник, объясняющий шаги правильного осуществления внедрения ISO/IEC 17799 и продвижения к сертификации BS 7799-2; "Администрирование" – инструментарий для правильного определения

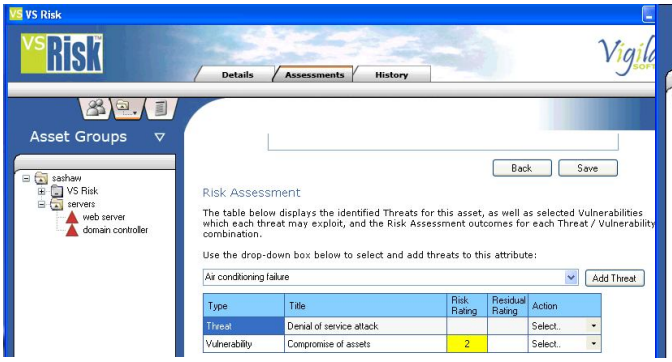

Рис. 7. Пример интерфейса оценки риска

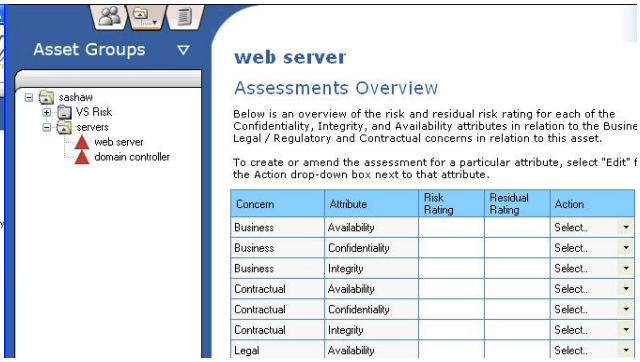

Рис. 8. Краткий обзор оценок

структуры управления СМИБ; "Инструменты" – набор инструментов для реализации правильного выполнения требований ISO/IEC 17799; "Управление ИБ" – модули, позволяющие эффективно управлять рисками организации и подготовиться к аудиту СМИБ.

Impact Area	Ranking	Impact Value	Score
Reputation	4	Moderate (2)	8
Financial	5	Low (1)	5
Productivity	3	Low (1)	3
Safety and Health	1	Low (1)	1
Fines/Legal	2	High (3)	6
		Total Score	**23**

Рис. 11. Результат оценки общего риска

Для оценки риска ИБ необходимо инициализировать ТВ составленный согласно требованиям стандарта. Рассмотрим пример запроса в ТВ: "Существуют ли документированные (утвержденные) политики, которые опубликованы и доведены до сведения всех сотрудников?". Процесс АОР проходит в два этапа, на первом – производится идентификация активов, угроз, уязвимостей и требований ИБ, оценивается величина уязвимостей, вероятность угроз и ценность активов, определяемая ущербом в результате нарушения конфиденциальности, целостности, доступности. С использованием этих данных вычисляется значение риска. На втором этапе принимается решение относительно способов обработки рисков и приемлемого уровня остаточных рисков, создается план обработки рисков, производится внедрение механизмов контроля и разработки политики ИБ и других организационно-распорядительных документов. В ходе описания необходимо задать данные относительно критериев "высокий" – (3), "средний" – (2), "низкий" – (1) [1]. Базируясь на информации о ценности активов и вероятности угроз, автоматически вычисляются значения

рисков и производится их упорядочивание по приоритетам (риск относительно конфиденциальности, целостности, доступности и законности).

Рис. 12. Пример оценки риска.

Относительно ИППР компонент **A** (исходя из указанного примера запроса), по антологии с RA2 art of risk, можно рассматривать как комплексный A_i, $i = \overline{1,a}$ (a – количество идентификаторов угроз). Так, например, в запросе относительно политики безопасности, при ее отсутствии, могут возникнуть действия, которые приведут к нарушению базовых характеристик ИБ. В этом случае параметр **A** можно представить, как: $A_{ПБ} \in \{A_{ПБi}\} i = \overline{1,a}$, где например, $A_{ПБ1}$= “Потеря конфиденциальной информации”. В свою очередь комплекс этих действий вероятно приведет к нарушению базовых характеристик ИБ и может связываться со значением E_7=“НКЦД”. Для оценивания используется количественная ($M_{кл}$) и качественная ($M_{кч}$) меры (рис. 12). Относительно оценочных компонент, можно отметить присутствие **P** (вероятность угрозы) и **L** (ценность активов – ущерб для организации, логически определяемый, как затраты или потери). Таким образом, отобразим кортеж: **<E, A,** C**, M,** L**, P>**, а например, относительно вышеуказанного запроса его ИП соответствует значения – $E_{нкцд}$, $A_{пб}$, C_o, $M_{кч}$.

Система Гриф 2006 (разработчик – компания Digital Security, Росия) направлен на обеспечение самостоятельной работы ИТ-менеджера (без привлечения сторонних экспертов) по оценке уровня рисков в ИС и эффективности существующей практики по обеспечению безопасности компании, а также предоставить возможность доказательно (в цифрах) убедить руководство в необходимости инвестиций в сферу ИБ. Процесс АОР в Гриф 2006 состоит из 3 этапов. Этап 1 – составление модели анализа информационных потоков (описание активов компании и всех бизнес-процессов). Этап 2 – создание модели анализа угроз и уязвимостей. Для оценки используется разработанная Digital Security классификация угроз, в которой описаны все действия, рассматриваемые во время оценки способные привести к нарушению базовых характеристик ИБ, то есть к событиям нарушения ИБ (**E**). Этап 3 – указание ущерба для каждой группы ценных ресурсов, по всем видам угроз. На этом этапе необходимо инициализировать ТВ по политике ИБ, реализованной в системе, что позволит оценить реальный уровень ее защищенности и детализировать оценку рисков. Запросы ТВ (например: “Может ли раскрытие какой-либо информации принести существенную выгоду посторонним лицам, заинтересованным организациям и т.п.? ”) инициализируются одним из двух фиксированных вариантов – “да” или “нет”, Анализ рисков ИБ осуществляется с помощью построения модели ИС организации [10]. Риск оценивается отдельно по каждой связке “группа пользователей – информация”, т.е. модель рассматривает взаимосвязь “субъект – объект”, с учетом всех их характеристик. Рассчитываются вероятность реализации угрозы, ее уровень по уязвимости на основе критичности и вероятности реализации через данную уязвимость и возможный ущерб. В системе используется шкала от 0 до 100%.

Рассмотрим Гриф 2006 с позиции ИППР**.** Так, компоненту **A** (исходя из указанного примера запроса) соответствует значение A_1=“Раскрытие информации”. Это действие приводит к нарушению конфиденциальности и связывается со значением E_1=“НК”. Характеристика ситуации (как видно из примера запроса) определена (C_o), а для отображения результатов используются $M_{кл}$ и $M_{кч}$. Оценивание риска осуществляется с помощью компонентов: **P** – вероятность реализации угроз, **L** – ущерб от ее реализации и **D** – уровень угрозы по уязвимости. Для указанного ПО составим кортеж: **<E, A,** C**, M,** L**, P,** D**>**, а например, относительно запроса о раскрытии информации его ИП принимают конкретные значения – $E_{нк}$, A_1, C_o, $M_{кч}$.

Система @RISK (разработчик – компания Palisade, США) предназначена для АОР с помощью метода Монте-Карло, реализуемого на основе Microsoft Excel. Система позволяет проследить возможность принятия и избежания рисков, а также принимать наилучшие решения в условиях неопределенности – $С_н$. В системе формируются различные запросы, например, “Какова вероятность прибыли, превышающей 10 млн. долларов?” или “Каковы шансы потерять деньги на этом предприятии?” Для оценки риска также используется метод Value at Risk (VAR) [5]. На начальном этапе работы производится создание модели оценки (анализ риска), посредством заполнения таблицы (см. пример табл. 2). Далее происходит расчет расходов если произойдёт ситуация нарушения ИБ.

Относительно ИППР которые используются в данной системе, отметим присутствие ИП **E, A, C** и **M.** Параметр **E** представлен косвенно, его можно логически определить, как событие нарушения характеристики ИБ к которому приводит действие **A**, например, $А_3$=“Мошенничество” может привести к $Е_7$=“НКЦД”. При оценке риска для отображения результатов используется $М_{кл}$ (табл. 2), а также задаются вероятности **P** и рассчитывается воздействие, что можно представить, как **L** – потери. Как видно кортеж для этой системы будет **<**E**, A,** C**, M, P,** L**>.**

Система RiskPAC (разработчик – компания CSCI, Нидерланды) предназначена для обнаружения и оказании помощи при устранении уязвимостей в ИС. Конструктор анкет, позволяет автоматизировать любую ручную методику оценки риска, для анализа которого необходимо инициализировать (с помощью фиксированных вариантов) запросы в ТВ, представленных в виде реляционных баз данных. Каждый запрос отображает определенное действие (**A**), приводящее к нарушению ИБ. Рассмотрим пример запроса: “Какие будут суточные финансовые потери при нарушении целостности клиентской базы?” ($А_1$=“Нарушение целостности клиентской базы”). Во время оценки риска для подсчета вероятности угроз используется шкала: маловероятно, вероятно и весьма вероятно. Также подсчитывается воздействие, по шкале: минимальное, значительное, серьёзное и катастрофическое. Дополнительно в системе содержится калькулятор ожидаемых среднегодовых потерь [13].

Пример таблицы эксплуатационных рисков Таблица 2

Эксплуатационные риски	Вероятность (годовая) %	Воздействие ($)	Среднее воздействие ($)
Отказ IT системы	0,1	1000	5
Проблема с производственным процессом	0,05	50	3
Тяжелое заболевание члена правления	0,05	100	5
Служащий выигрывает судебный процесс	0,08	250	20
Появления нового конкурента	0,25	400	100
Отказ выпуска нового товара	0,15	300	45
Укрепление ставки $	0,35	100	35
Пожар в главном офисе	0,02	250	5
Мошенничество	0,005	500	3
Потеря конфиденциальных данных	0,01	300	3
Банкротство главного клиента должника	0,02	150	3
Общие количества		**2900**	**226**

Рассмотрим данное ПО относительно ИППР. Так, компоненту **A** (что видно из примера запроса) соответствует, например, значение $А_1$. Это действие приводит к нарушению определенных характеристик ИБ атакованных ресурсов и может быть связано со значением $Е_5$=“НЦД”, а параметр **C** отображается $С_о$, поскольку подсчитывается точные финансовые потери. Инициализация данных осуществляется в числовой и лингвистической формах, что отображается $М_{кл}$ и $М_{кч}$. При оценке риска определяется вероятность угроз **P,** воздействие, которое можно интерпретировать как уровень опасности **D** и потери **L.** Проведенный анализ показал, что кортеж для этой системы имеет вид: **<**E**, A,** C**, M, L, P,** D**>**, а например, относительно запроса про финансовые потери его ИП принимают конкретные значения – $Е_{нцд}$, $А_1$, $С_о$, $М_{кл}$.

Система Microsoft Security Assessment Tool (MSAT, разработчик – компания Microsoft, США) базируется на материалах «Руководства по управлению рисками» [12]) 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. 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: этап 1 – "Параметры компании" (название, число компьютеров, серверов и т.д.); этап 2 – "Безопасность инфраструктуры" (рассмотрим примеры запросов для этого этапа: "Размещаются ли службы, используемые как внешними, так и внутренними клиентами, в одном и том же сегменте?", "Повлияет ли на доходность события, которые нанесут вред приложениям или инфраструктуре клиента, например, бездействие узла, отказ оборудования или сбой в приложении?" и т.д.); этап 3 – "Безопасность приложений"; этап 4 – "Безопасность операций"; этап 5 –"Безопасность персонала"; этап 6 – "Среда". После реализации этапов этой группы осуществляется обработка (посредством подключения к Интернет) полученной информации и осуществляется переход к второй группе запросов. Для технических специалистов она более интересен, т.к. касается используемых в компании политик, средств и механизмов ИБ. Запросы организованы в соответствии с концепцией многоуровневой (эшелонированной) ЗИ на уровне: инфраструктуры (защита периметра, аутентификации и д.р.); приложений; безопасности операций (определена ли политика ИБ, политика резервного копирования и т.д.); работы с персоналом (обучение, проверка при приеме на работу и т.д.). Во многом ТВ соответствует разделам стандартов ISO/IEC 17799 и ISO/IEC 27001. 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). При оценке частоты возникновения угроз используются градации: высокая (вероятно возникновение одного или нескольких событий в пределах года); средняя (влияние может возникнуть в пределах двух-трех лет); низкая (возникновение влияния в пределах трех лет маловероятно).

Сведенные данные Таблица 3

ПО	**Параметры риска**							
	E	**A**	**C**	**M**	**P**	**F**	**L**	**D**
COBRA	К	П	К	П	П	О	О	О
CRAMM	К	П	К	П	П	П	К	О
RiskWatch	К	П	К	П	О	П	П	О
RA2 art of risk	К	П	К	П	П	О	О	П
КЭС	К	П	К	П	П	О	К	П
Risk Advisor	К	П	К	П	П	О	К	П
vsRisk	П	П	К	П	П	О	О	К
OCTAVE	К	П	К	П	О	О	О	П
Callio Secura	П	П	К	П	П	О	К	О
Гриф 2006	П	П	К	П	П	О	К	К
@RISK	К	П	К	П	П	О	К	О
RiskPAC	К	П	К	П	П	О	П	К
MSAT	К	П	К	П	О	О	О	П

Относительно ИППР в ПО отображены **E, A, C, M.** В рассмотренном примере запроса "Повлияет ли на доходность события…" события можно представить как параметр A_1="Бездействие узла", A_2= "Отказ оборудования" и A_3= "Сбой в приложений", которые могут привести к E_3="НД". 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>.**

С учетом [9] в табл. 3 приведены сводные данные о интегрированных параметрах риска, которые используются в анализируемых средствах, где П и К соответственно указывают на прямое и косвенное наличие параметра в системе, а О – его отсутствие.

Таким образом, в работе проведено исследования широкого спектра существующего ПО АОР (с использованием предложенного в [6, 7, 9] подхода) и определен набора параметров, по которым можно осуществить сравнительный анализ таких средств оценивания и выбрать наиболее подходящие для решения соответствующих задач ЗИ.

ЛИТЕРАТУРА

1. Callio Technologies: программный комплекс управления политикой информационной безопасности компании (международный стандарт BS7799 ISO 17799) [Электронный ресурс] – Режим доступа: .http://businesssoft.ru.
2. Compliant Information Security Risk Assessment Tool [Электронный ресурс] / vsRisk – ISO 27001: 2005 – Режим доступа: http://www.27001.com/products/31
3. OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM) [Электронный ресурс] // http://www.cert.org/octave/octavemethod.html – Названия титул. с экрана.
4. Thomas R. Peltier Information security risk analysis / Thomas R. Peltier – Auerbach Pub, 2001. – P 281.
5. 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.
6. 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.
7. Корченко А.Г. Интегрированное представление параметров риска / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2011. – №1. – С. 96-101.
8. 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.
9. 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.
10. 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.
11. Петренко С. А Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. – М.: Компания АйТи ; ДМК Пресс, 2004. - 384 с.
12. 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.
13. 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.

Надійшла: 05.10.2011

Рецензент: д.т.н., проф. Щербак Л.М.