ISSN 2224-5227

2015 • 6

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

БАЯНДАМАЛАРЫ

ДОКЛАДЫ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

REPORTS

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

ЖУРНАЛ 1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ЖУРНАЛ ИЗДАЕТСЯ С 1944 г.
PUBLISHED SINCE 1944

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ
БАЯНДАМАЛАРЫ **2015 • 6**

ДОКЛАДЫ **2015 • 6**
НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

«Доклады Национальной академии наук Республики Казахстан» ISSN 2224-5227
Собственник: Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5540-Ж**, выданное 01.06.2006 г.
Периодичность: 6 раз в год. Тираж: 3000 экземпляров
Адрес редакции: 050010, г.Алматы, ул.Шевченко, 28, ком.218-220, тел. 272-13-19, 272-13-18
http://nauka-nanrk.kz, reports-science.kz
Адрес типографии: ИП «Аруна», г.Алматы, ул.Муратбаева, 75

REPORTS **2015 • 6**

OF NATIONAL ACADEMY OF SCIENCES OF THE
REPUBLIC OF KAZAKHSTAN

Reports of the National Academy of Sciences of the Republic of Kazakhstan.
ISSN 2224-5227
Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5540-Ж, issued 01.06.2006
Periodicity: 6 times a year
Circulation: 2000 copies
Editorial address: 28, Shevchenko str., of.219-220, Almaty, 050010, tel. 272-13-19, 272-13-18,
http://nauka-nanrk.kz / reports-science.kz
Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

REPORTS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
ISSN 2224-5227
Volume 6, Number 304 (2015), 43 – 54

UDC 004. 056

SOFTWARE OF ESTIMATION OF RISKS OF INFORMATION SECURITY

M. N.Zhekambayeva[1], S.V.Kazmirchuk[2]

[1]Kazakh national research technical university after K. I. Satpayev, Almaty,
[2]National aviation university, Ukraine
maia.kz@mail.ru

Key words: information security, risk, analysis of risk, risk assessment, management of risk, threat, vulnerability, characteristics of risk.

Abstract. Research of a wide range of the existing program systems of the analysis and estimation of risks of information security concerning a set of basic characteristics is conducted (action, an event, probability, danger, expenses and losses). Often before specialists of the companies for increase the efficiency of the solution of problems of information security there is a question of a choice of the corresponding technique which will meet adequate requirements. To the most known means which are used for research, belong – COBRA, CRAMM, RiskWatch, RA2 art of risk, KES of management of IB "Vanguard", etc. For these means taking into account the corresponding model of basic characteristics of risk the train which gives the chance to unify process of the comparative analysis of such means that will increase efficiency of implementation of their choice for the solution of problems of information security is made.

УДК 004. 056

Ироаммные средства оценивания рисков информационной безопасности

[1]Жекамбаева М.Н., [2]Казмирчук С.В.
[1]Казахский национальный исследовательский технический университет имени К.И.Сатпаева, г. Алматы
[2]Национальный авиационный университет, Украина
maia.kz@mail.ru

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

Аннотация. Проведено исследование широкого спектра существующих программных систем анализа и оценивания рисков информационной безопасности относительно набора базовых характеристик (действие, событие, вероятность, опасность, затраты и потери). Часто перед специалистами компаний для повышения эффективности решения задач защиты информации возникает вопрос о выборе соответствующей методики, которая будет удовлетворять адекватным требованиям. К наиболее известным средствам, которые использованы для исследования, относятся – COBRA, CRAMM, RiskWatch, RA2 artofrisk, КЭС управления ИБ «АванГард» и др. Для этих средств с учетом соответствующей модели базовых характеристик риска составлен кортеж, который дает возможность унифицировать процесс сравнительного анализа таких средств, что повысит эффективность осуществления их выбора для решения задач информационной безопасности.

На сегодняшний день существует достаточно широкое множество инструментальных средств анализа и оценивания риска (САОР). Часто перед специалистами компаний для повышения эффективности решения задач защиты информации (ЗИ) возникает вопрос о выборе

соответствующей методики, которая будет удовлетворять адекватным требованиям. В работе [2] осуществлен анализ понятия риска, в различных предметных областях человеческой деятельности, для последующей его интерпретаций в области информационной безопасности (ИБ). Также в [2] была предложена кортежная модель базовых характеристик риска (КМР). Такой подход дает возможность относительно КМР унифицировать процесс исследования соответствующих САОР и повысить эффективность осуществления их выбора. Также существует множество других подобных средств, для которых не определен набор характеристик риска, поскольку не осуществлялся соответствующий анализ.

В связи с этим, целью данной работы является проведение исследования широкого спектра существующих САОР (с использованием предложенного в [2] подхода) для определения их набора характеристик, по которым можно осуществить сравнительный анализ таких средств. Это повысит эффективность решения задач в области ИБ

В качестве исходного материала исследования, было взято множество наиболее известных и используемых на практике САОР – COBRA, CRAMM, RiskWatch, RA2 artofrisk (RASoftwareTool), КЭСуправленияИБ«АванГард» («РискМенеджер»), RiskAdvisor.

СОАР 1 -Методика COBRA(ConsultativeObjectiveandBi-FunctionalRiskAnalysis, разработчик – C & A SystemsSecurityLtd**,** Великобритания) ориентирована на поддержку требований стандарта ISO 17799 посредством тематических вопросников (checklist's), используемых в ходе оценки рисков информационных активов и электронных бизнестранзакций компании [8]. Продукт расширен инструментарием для консалтинга и проведения обзоров безопасности, который разработан на основании принципов построения экспертных систем. В комплект программного обеспечения(ПО) входят модули COBRA ISO 17799 SecurityConsultant, COBRA PolicyComplianceAnalyst и COBRA DataProtectionConsultant, 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; безопасности информационных технологий(ИТ); оперативная ИТ и бизнеса; инфраструктуры электронной коммерции. Модули тематического вопросника информационно поддерживают отдельные приложения, например: APP-MAN (Applicationlevelsecuritymanagement) – управления безопасностью; APPAUDIT (ApplicationlevelAuditing) – аудит; APPCNTRL (ApplicationStaffcontrol) – контроль штата; APPDEPND (ApplicationStaffdependency) – зависимость штата; AUDIT (SystemAudit) – 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 (ИС) повлиял тот или иной инцидент. Такой подход дает возможность реализовать лишь достаточно грубое оценивание риска. Воровство (с учетом [3]) 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 [3] 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 базовых характеристик риска [2] для методики COBRA можно получить отображения таких составляющих: $\boldsymbol{BC_1, BC_2}$. Так, компоненту $\boldsymbol{BC_1}$ (исходя из указанного примера) соответствует, например, значение BC_{11}= «Кража». Это действие приводит к нарушению определённых характеристик безопасности атакованных ресурсов и может быть связано со значением BC_{27}= «НКЦД».

После обработки инициализированых данных система генерирует отчет, в котором описана детальная оценка (DetailedRiskAssessment (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 базовыми характеристиками, первая и последняя из которых несут в себе BC_1 и BC_2. составляющие (название категории и комментарии к ней), а оставшаяся –составляющую, которой соответствует «УРОВЕНЬ РИСКА», представленный в процентах (вероятность наступления риска), в связи с этим (учитывая [2]) уровень риска можно отобразить через компонент BC_3. Анализ и оценивание риска происходит во время обработки данных инициируемых через тематический вопросник. Все рассматриваемые действия (BC_1), которые отображаются в запросах, собраны в категории риска, например, действие рассмотренное в примере запроса BC_{11}входит в категорию риска «Непредвиденная ситуация в бизнесе (НСБ)», следовательно характеристику в данной категории риска можно представить как $BC_{1НСБ} = \{BC_{1НСБ1}, BC_{1НСБ2}, ..., BC_{1НСБbc_1}\}$, где $BC_{1НСБ1}$ = «Кража» (bc_1 – количество идентификаторов угроз для категории НСБ) [2].

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&ResponseListing (continued)).

Анализ показал, что прямого использования компонента BC_2 в системе нет, но прослеживается логическая связь с ним, поэтому считаем его присутствие косвенным. Здесь и далее для обозначения косвенныххарактеристик в кортеже будет использоватьсясимвол *, т.е. BC_2^*.После проведенного анализа с учетом КМР [2] кортеж для этой методики можем представить в виде <BC_1, BC_2^*, BC_3>.

COAP 2 -Метод CRAMM(CCTA RiskAnalysisandManagementMethod,разработчик – Центральное агентство по компьютерам и телекоммуникациям (CCTA – CentralComputerandTelecommunicationsAgency), Великобритания**)** реализован фирмой InsightConsultingLimited в одноимённом программном продукте, в котором предусматривается поэтапный и строгий подход к анализу и оценивания риска, охватывающий аспекты безопасности как технического (например, ИТ-оборудование и программное обеспечение), так и нетехнического характера (например, физического и человеческого) [7]. 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 [1, 7]: 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 [1]) 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).

Таблица 1 Шкалы для уровней и уязвимостей

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

Анализ риска проводится на первом и втором этапах, после чего осуществляется его оценивание. 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 [2] здесь можно выделить компоненты $\boldsymbol{BC_5}$ и $\boldsymbol{BC_3}$.

Исходя из оценок стоимости ресурсов, защищаемой ИС, угроз и уязвимостей, определяются «ожидаемые годовые потери». На рис. 1 приведен пример матрицы оценки ожидаемых потерь [1], 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).

		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

Рисунок 1 – Матрица ожидаемых годовых потерь

Значения ожидаемых годовых потерь (AnnualLossofExpectancy) переводятся в баллы,

показывающие уровень риска, согласно шкалы, представленной на рис. 2 (в этом примере размер потерь приводится в фунтах стерлингах) и далее в соответствии с матрицей (рис. 3) выводится оценка риска. Здесь, с учетом [2], годовые потери можно отразить через компонент BC_6.

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

Рисунок 2 – Шкала оценки

Третий этап исследования заключается в поиске адекватных контрмер. Здесь CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням.Относительно представления КМР для CRAMM (аналогично методике COBRA) можно определить значения: BC_1, BC_2^*. Компонент BC_1 отображается действием, которое привело к нарушению характеристик ИБ, что можно показать на примере «оценки угрозы», а именно BC_{12}= «Несанкционированный доступ» может привести к BC_{21}= «Нарушение конфиденциальности (НК)».

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

Рисунок 3 – Матрица оценки риска

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 [1, 7]. 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 следующая: 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 [2] составим КМР для данного метода: $<BC_1, BC_2^*, BC_3, BC_5, BC_6>$.

САОР 3 -Система RiskWatch (разработчик – компания RiskWatch, США) отображает требования стандартов ISO/IEC 27001 и ISO/IEC 27002, NIST а также COBIT IV. Процесс анализа и оценивания риска производится в четыре фазы. Фаза 1 – описание 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 издоровье (персонала, заказчиков и т.д.), изменение данных, репутация [7] 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. 4), на основании чего рассчитывается эффективность внедрения средств ЗИ [7].

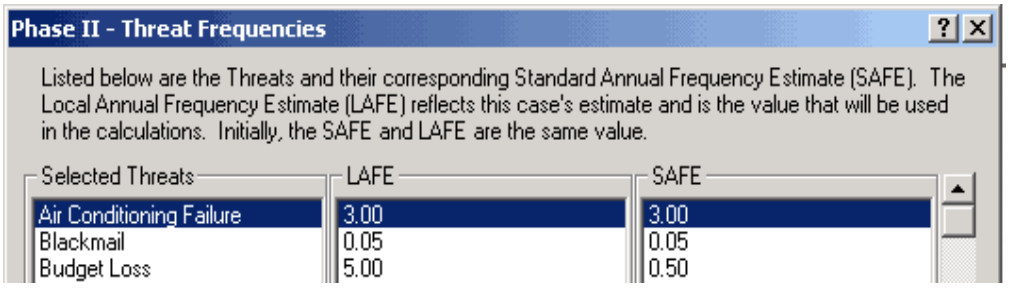

Рисунок 4 – Окно инициализации параметров

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 $\nu = 150\,000$\$, а вероятность его уничтожения при пожаре в течение года p=0,01, то ожидаемые потери составят $m = 1\,500$\$, т.е. $m = p \times \nu$, где p – вероятность возникновения угрозы, а ν – стоимость ресурса. Отметим, что RiskWatch базируется на таких данных NIST, как LAFE (LocalAnnualFrequencyEstimate) и SAFE (StandardAnnualFrequencyEstimate), 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 (TheUniformCrimeReporting), что позволяет сформировать соответствующую статистическую информацию об инцидентах ИБ в общегосударственной базе. Фаза 4 – генерация отчета (рис. 5).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*) [7] $ALE = A \times EF \times F$, где: A (AssetVal) – стоимость ресурса (данные, программы, аппаратура и т.д.); EF (ExposureFactor) – коэффициент воздействия (процентная часть от стоимости актива, подвергаемой риску); F (Frequency) – частота возникновения нежелательного события. Например, пусть аппаратное средство стоитA=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).

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%

Рисунок 5 – Фрагмент отчета в RiskWatch

Дополнительно используются показатели ARO (AnnualizedRateofOccurrence) – ожидаемая годовая частота происшествия и SLE (SingleLossExpectancy) – 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 систем защиты информации (СЗИ). Эффект от внедрения средств безопасности определяется параметром *ROI* (ReturnonInvestment – возврат инвестиций), показывающий отдачу от вложений за период времени.

Относительно КМР с учетом [2] для RiskWatch определим кортеж**.** Так компоненту$\boldsymbol{BC_1}$(исходя из указанного примера категорий потерь) соответствуют, например, значения BC_{11}= «Задержка и отказ в обслуживании», BC_{12}= «Раскрытие информации», BC_{13}= «Уничтожение оборудования» и т.д. Эти действия приводят к нарушению определенных характеристик ИБ атакованных ресурсов и соответственно связываются со значениями BC_{23}= «НД», BC_{21}=«НК», BC_{25}= «НЦД». Анализ показал, что прямого использования компонента $\boldsymbol{BC_2^*}$ в системе нет, но прослеживается логическая связь с ним, поэтому считаем его присутствие косвенным. Анализ риска происходит во время обработки данных инициируемых через ТВ, который используется при прохождении фазы 1. Для определения *ALE* используется компонент$\boldsymbol{BC_5}$,а риском являются ожидаемые потери за год, которые также можно интерпретировать как расходы($\boldsymbol{BC_6}$).С учетом КМР, кортеж для этой методики можно представить в виде $\boldsymbol{<BC_1,\ BC_2^*, BC_5, BC_6>}$.

САОР 4 -Инструментарий RA2 artofrisk (RA SoftwareTool,разработчик –компании AEXIS SecurityConsultants и XiSECConsultantsLtd., Великобритания)представляет собой ПОдля 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 [5].

Относительно КМР определим значения$\boldsymbol{BC_1, BC_2}$**.** Все действия ($\boldsymbol{BC_1}$), 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 компонент$\boldsymbol{BC_1}$ можно отразить комплексно BC_{1i}, $i=\overline{1,bc_1}$ (где bc_1 – количество идентификаторов угроз). Так, например, в запросе о ДТЛ при невыполнении данной оценки, могут возникнуть действия, приводящие к нарушению базовых характеристик ИБ, тогда $\boldsymbol{BC_1}$ можно представить множеством $\boldsymbol{BC_{1ДТЛ}} \in \left\{BC_{1ДТЛi}\right\} i=\overline{1,bc_1}$, где, например, $BC_{1ДТЛ1}$= «Кража». Относительно компонента$\boldsymbol{BC_2}$,следует отметить, что рассмотренные действия (исходя из указанного примера запросов) приводят к нарушению определенных характеристик ИБ и может быть косвенно связано со значением BC_{27}= «НКЦД». Анализ показал, что характеристика $\boldsymbol{BC_2^*}$ в ПО присутствует косвенно. В методике присутствуют характеристики$\boldsymbol{BC_4}$(уровни опасности) и$\boldsymbol{BC_3}$(вероятность риска), следовательно, риск отображается как опасность ($\boldsymbol{BC_4}$) для организации (при наступлении рисковой ситуации). С учетом КМР кортеж для этой методики можем представить в виде:$\boldsymbol{<BC_1,\ BC_2^*, BC_3, BC_4>}$.

САОР 5 -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» [4]. Изначально производится анализ событий риска ($\boldsymbol{BC_1}$) посредством построения их моделей с помощью интерфейса главной формы (рис. 6), 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.

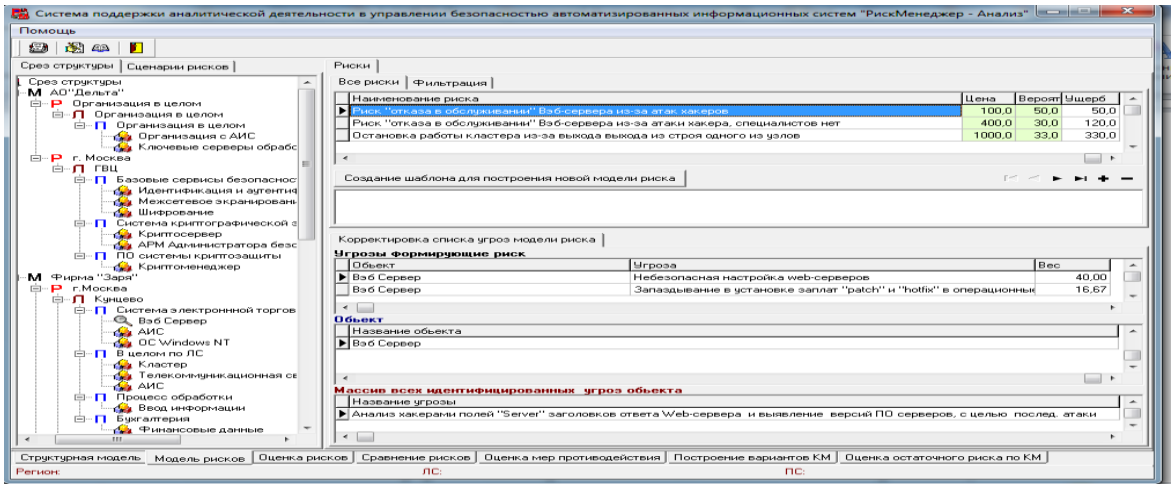

Рисунок 6 - Интерфейс построения моделей событий риска

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 [4].

Отметим, что относительно КМР в КЭС рассматривается событие риска, отображаемое как действие (***BC₁***),которое приводит к нарушению ИБ, например, BC_{11}= «Отказ обслуживания веб-сервера из-за атаки хакера», BC_{12}= «Падение криптосервера из-за перегрузки», BC_{13}= «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 (***BC₁***) могут быть связаны с событиями (***BC₂***) нарушения базовых характеристик ИБ, например, BC_{11} с BC_{23}= «НД», BC_{12} с BC_{27}= «НКЦД», а BC_{13} с BC_{21}= «НК» и т.д., следовательно, характеристика $\boldsymbol{BC_2^*}$ в системе присутствует косвенно. Касательно других компонент, которые используются в процессе анализа риска, присутствуют степень опасности (***BC₄***)ивероятность события риска(***BC₃***). Так же используется показатель ущерба, которыйотображается посредством***BC₆***. 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 характеристикой $\boldsymbol{BC_6^*}$ которая всистеме присутствуют косвенно.После проведенного анализа с учетом КМР кортеж для КЭС будет<$\boldsymbol{BC_1, BC_2^*, BC_3, BC_4, BC_6^*}$>.

СОАР 6 -Система EnterpriseRiskAssessor(RiskAdvisor, разработчик–компания Methodware,Новая Зеландия)соответствует требованиям австралийского стандарта Australian/NewZealandRiskManagementStandard (AS/NZS 4360:1999) и ISO/IEC 17799. Представленавтрехпродуктах: 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 TheBuilderTool – 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. 7), позволяющая описать риски в соответствии с определенным шаблоном и задать их связи с другими элементами модели. Оценка происходит на основе качественной шкалы, а риски разделяются на приемлемые и неприемлемые.

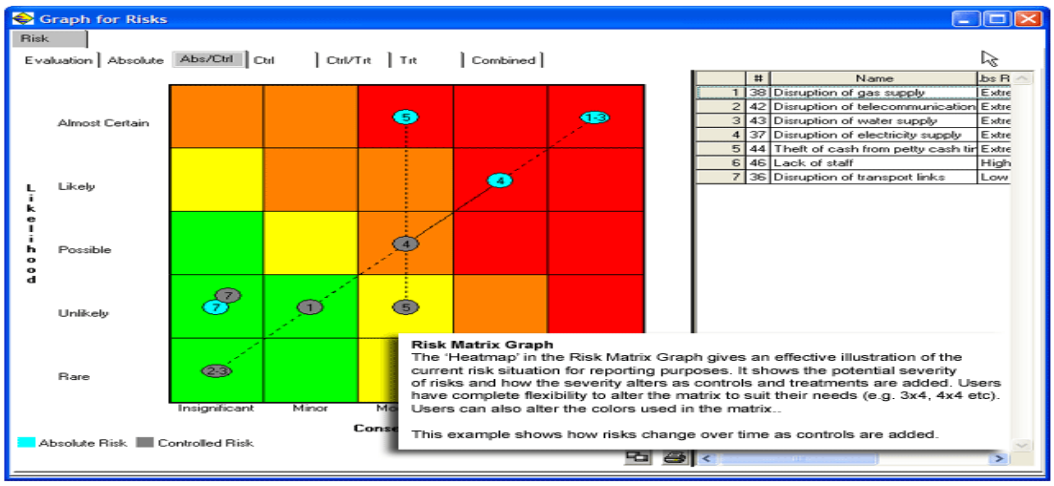

Рисунок 7 – Матрица риска

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: TheAssessor – экспертная оценка (анализ собранной информации). Шаг 3: TheConsolidationTool – инструмент консолидации (интегрирует все индивидуальные оценки риска). После построения модели формируется отчет (около 100 разделов) и агрегированное описание в виде графа рисков [5, 6]. В отчете (рис. 8) с вероятностно-лингвистической шкалой, риск представлен в виде матрицы с градациями: почти наверняка, вероятно, возможно, маловероятно, редко. Рассмотрим пример описания и оценки риска (рис. 9). В процессе описания экспертами указывается владелец и степень риска, последствия и вероятность, далее производится оценка.

При КМР для данного ПО, можно получить отображение базовых характеристик$\boldsymbol{BC_1}$, $\boldsymbol{BC_2}$, $\boldsymbol{BC_3}$, $\boldsymbol{BC_4}$и $\boldsymbol{BC_6}$.В EnterpriseRiskAssessor в качестве риска рассматриваются действия, которые могут привести к нарушению ИБ, например, BC_{11}= «Кража документов» может находиться в логической связи с BC_{21}= «НК» и поэтому характеристика $\boldsymbol{BC_2^*}$ в ПО присутствует косвенно. В процессе анализа риска можно дополнительно идентифицировать базовые характеристики в явном виде $\boldsymbol{BC_3}$икосвенном $\boldsymbol{BC_6^*}$ (consequence – следствие, которое можно представить в виде $\boldsymbol{BC_6^*}$), а во время его оценки – устанавливается коэффициент значимости и уровень опасности($\boldsymbol{BC_4}$),следовательно, кортеж имеет вид:<$\boldsymbol{BC_1}$, $\boldsymbol{BC_2^*}$,$\boldsymbol{BC_3}$, $\boldsymbol{BC_4}$, $\boldsymbol{BC_6^*}$>.

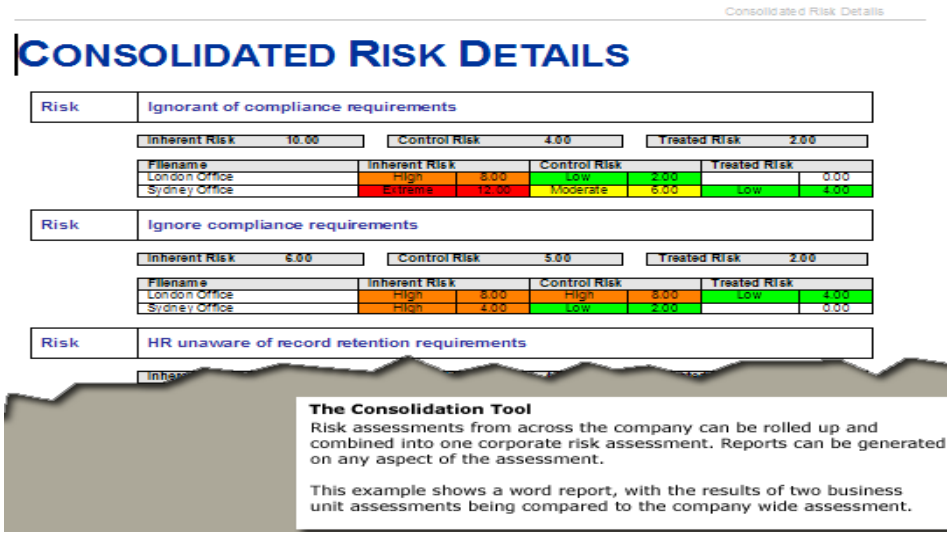

Рисунок 8 – Фрагмент отчета

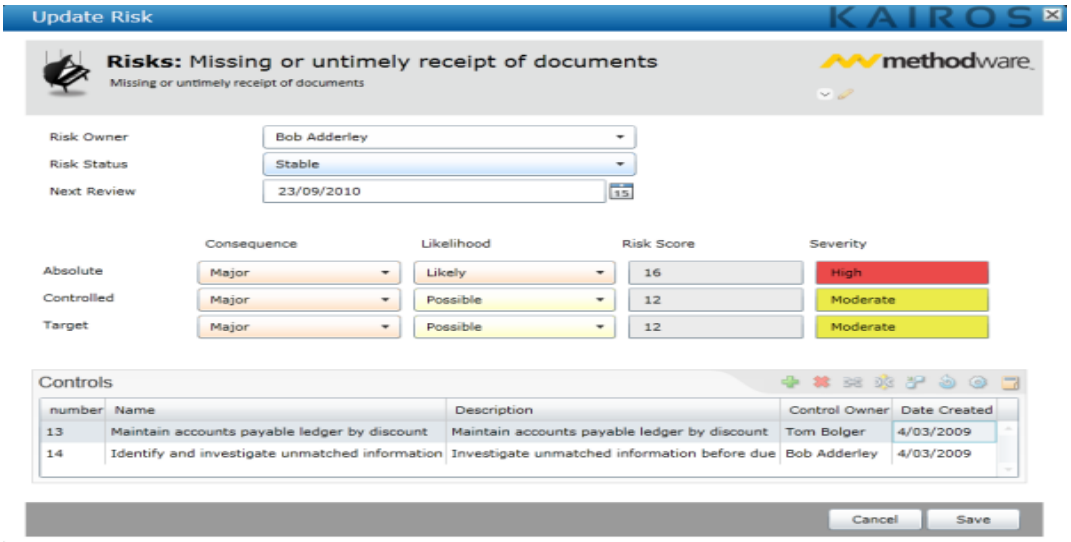

Рисунок 9 - Пример описания риска

Таким образом, в работе, с учетом предложенного в [2] подхода, проведено исследование широкого спектра САОР в виде соответствующего ПО и определен наборбазовых характеристик (см. табл. 2), по которым можно осуществить сравнительный анализ соответствующих средств оценивания и выбрать наиболее подходящие для решения определенного класса задач ЗИ.

Таблица 2 Результаты исследования САОР

BC	**САОР**					
	1	**2**	**3**	**4**	**5**	**6**
BC_1	+	+	+	+	+	+
BC_2	+*	+*	+*	+*	+*	+*
BC_3	+	+	-	+	+	+
BC_4	-	-	-	+	+	+
BC_5	-	+	+	-	-	-

BC_6	-	+	+	-	+ *	+ *

ЛИТЕРАТУРА

[1] Алексеев А. Управление рисками. Метод CRAMM / А. Алексеев // IT Expert. – Электрон.дан. – М. : ЗАО “ИТ Эксперт”, 2010. – Режим доступа: WorldWideWeb.– URL: http://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf.– Загл. с экрана (просмотрено 19 декабря 2014).

[2] Ахметов Б.С., Корченко А.Г., Казмирчук С.В., Жекамбаева М.Н. Кортежная модель базовых характеристика риска / ВестникКазНИТУ – 2015. - №6/

[3] Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А.Г. – К. : «МК-Пресс», 2006. – 320с.

[4] Костров Д.Д. Анализ рисков и управление ими / Костров Д.Д. // Byte Россия. – 2003. – №10 (62) – С. 15–20.

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

[6] Симонов С. В. Анализ рисков в информационных системах. Практические аспекты. Защита информации / С. В. Симонов // Конфидент. Безопасность компьютерных систем – 2001. – №2. – С. 48-53.

[7] Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ [Электронный ресурс] / И.С. Медведовский // SecurityLab. Электрон.дан.– Мн.: SecurityLab, 2004. – Режим доступа: WorldWideWeb.– URL: http://www.ixbt.com/cm/informationsystem-risks012004.shtml. – Загл. с экрана (просмотрено 18 декабря 2014).

[8] Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance: COBRA. [Electronic resource] / Security Risk Analysis & Assessment, and ISO 27000 Compliance –Electronic data – Macclesfield: The Leading Security Risk, 2010– Access mode: World Wide Web.– URL: http://www.riskworld.net/.

REFERENCES

[1] Alekseev A. Risk management. CRAMM method / A. Alekseev//IT Expert. – Electron. it is given. – M.: JSC IT Ekspert, 2010. – Access mode: World Wide Web. – URL: http://www.itexpert.ru/rus/ITEMS/ITEMS_CRAMM.pdf. – Zagl. from the screen (it is seen on December 19, 2014). (in Russ.)

[2] Akhmetov B. S., Korchenko A.G., Kazmirchuk S.V., Zhekambayeva M. N. Kortezhnaya model basic the characteristic the risk / Messenger of KAZNITU – 2015. - No. 6/(in Russ.)

[3] Korchenko A.G. Creation of systems of information security on indistinct sets. Theory and practical decisions / Korchenko A.G. – To.: "MK-Press", 2006. – 320p. (in Russ.)

[4] D. D fires. Risk analysis and management of them / D.D.'s Fires//Byte Russia. – 2003. – No. 10 (62) – P. 15-20. (in Russ.)

[5] Petrenko S. A. Management of information risks. Economically justified safety / S. A. Petrenko, S. V. Simonov. – M.: Press IT, DMK company, 2004. – 384 p. (in Russ.)

[6] Simonov S. V. Risk analysis in information systems. Practical aspects. Information security / S. V. Simonov//Confidant. Safety of computer systems – 2001.– No. 2. – p. 48-53. (in Russ.)

[7] Modern methods and means of the analysis and control of risks of information systems of the companies CRAMM, RiskWatch and SIGNATURE STAMP [An electronic resource] / I. S. Medvedovsky//SecurityLab. Electron.it is given. – Мн.:SecurityLab, 2004. – Access mode: World Wide Web. – URL: http://www .ixbt.com/cm/informationsystem-risks012004.shtml. – Zagl. from the screen (it is seen on December 18, 2014). (in Russ.)

[8] Security Risk Analysis & Assessment, and ISO 17799/BS7799 Compliance: COBRA. [Electronic resource]/Security Risk Analysis & Assessment, and ISO 27000 Compliance – Electronic data – Macclesfield: The Leading Security Risk, 2010 Access mode: World Wide Web. – URL: http://www.riskworld.net/.

Ақпараттық қауіпсіздік қатерін бағалау амалдарын программалау

Жекамбаева М.Н., Казмирчук С.В.,
Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы
Ұлттық авиациялық университеті, Украина
maia.kz@mail.ru

Түйін сөздер: ақпараттық қауапсіздік, қауіп, қауіп анализі, қауіпті бағалау, қауіпті басқару, қауіп-қатер, әлсіздік, қауіпке мінездеме.

Аннотация. Қауіпті бағалау мен анализдеу амалдары, қор тізбегін анықтау үшін кең спектрлік зерттелуін өткізу арқылы амалдардың салыстырмалы анализдерін жүзеге асыруға болады. САОР – COBRA, CRAMM, RiskWatch, RA2 art of risk (RA Software Tool) тәжірбиелері қолданылды.

PUBLICATION ETHICS AND PUBLICATION MALPRACTICE IN THE JOURNALS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the work described has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the originality detection service Cross Check http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

http://www.reports-science.kz/index.php/ru/

Редакторы *М. С. Ахметова, Д. С. Аленов, Т.А. Апендиев*
Верстка на компьютере *С.К. Досаевой*

Подписано в печать 05.12.2015.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
16,8 п.л. Тираж 2000. Заказ 6.