МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»
Кафедра Системы информационной безопасности

«ДОПУЩЕН К ЗАЩИТЕ»
Заведующий кафедрой
доцент Бердибаев Р.Ш
(ученая степень, звание, Ф.И.О.)
_____ «___» _____2018 г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Методы анализа и оценки рисков информационных ресурсов

Специальность 5В100200 Системы информ. безопасно.
Выполнил(а) Толеев Кыдырхан Джамилович Группа СИБ-14-2
(Ф.И.О.)
Научный руководитель проф Ахметов Б.С
(ученая степень, звание, Ф.И.О.)
_____ «25» мая 2018 г.
(подпись)
Рецензент: к.т.н. доцент (ассоц. проф) Айтхожаева Е.Н.
(ученая степень, звание, Ф.И.О.)
_____ «___» 06 2018 г.
(подпись)
Консультанты:
по экономической части:
к.э.н. доцент Самибаева Р.Д
(ученая степень, звание, Ф.И.О.)
_____ «29» 05 2018 г.
(подпись)
по безопасности жизнедеятельности:
д.т.н Бекбасаров Ш.Ш
(ученая степень, звание, Ф.И.О.)
_____ «25» мая 2018 г.
(подпись)
по применению вычислительной техники:
_____
(ученая степень, звание, Ф.И.О.)
_____ «___» _____2018 г.
(подпись)
Нормоконтролер: ст. преп. Мирошниченко Е.А
(ученая степень, звание, Ф.И.О.)
_____ «1» июня 2018 г.
(подпись)

Алматы 2018

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Факультет Систем управления и информационных технол.

Кафедра Системы информационной безопасности

Специальность Системы информационной безопасности

ЗАДАНИЕ

на выполнение дипломного проекта

Студенту Толиев Карим Нурсон Джалгасович
(Ф.И.О)

Тема проекта Методы анализа и оценки рисков информационных ресурсов

Утверждена приказом по университету №_____от «__»_____201__г.

Срок сдачи законченного проекта «_____»_____201__г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): рассмотрение методы и средства анализа и оценивания рисков (САОР) ИБ, как на основе статистических данных, так и на основе экспертных оценок, сделанных в нечетко определенной либо формализованной среде

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Проанализировать основные концепции, связанные с угрозами, существующие стандарты, методы, методы и оценку и оценку рисков для определения наборов основных мероприятий.

Перечень графического материала (с точным указанием обязательных чертежей): рисунок 1.1 - Процесс оценки риска, рисунок 1.2 - диаграмма частот, рисунок 1.3 - матрица рисков FMAP, рисунок 1.4 - Пример оценки воздействия, рисунок 3.1 блоковый алгоритм работы системы анализа и оценивания рисков ИБ, рисунок 3.2 - пример сгенерированного отчета, рисунок 3.3 - внешний вид главного окна программного продукта, рисунок 3.4 - Интерактивный интерфейс ПС, рисунок 3.5 Сгенерированный отчет ПС

Основная рекомендуемая литература: Симонов С.В. Анализ рисков в информационных системах Ахметов Б.Б Использование нечеткой логики для оценки риска. Ахметов Б.С Система оценивания рисков на базе метода FirstM.

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
БЖСД	у.т.н. Бекбасаров И.М		
Экономич. часть	к.э.н. Самигбаева Р.О.	04.04.18 29.05.18	
Научный руководи	Ахметов Б.С.		

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Следственный анализ и оценивание рисков	28.10.2017 - 15.12.17	
Методы и методики	16.11.17 - 25.12.17	
Модель и метод анализа и оценивания рисков	26.12.17 - 02.01.18	
Когнитивная модель базовых характеристик сценариев рисков	03.01.18 - 20.01.18	
Метод FirstM оценивания рисков	22.01.18 - 03.02.18	
Экспериментальная система анализа	05.02.18 - 20.02.18	
Изучение FirstR - CAOP системы	22.02.18 - 06.03.18	
Расчет технико-экономического обоснования	09.03.2018 - 25.03.2018	
Расчет показателей условий труда	26.03.2018 - 10.04.2018	
Заключение	11.04.2018 - 30.04.2018	

Дата выдачи задания «10» января 2018 г.

Заведующий кафедрой _____ (_____)
(подпись) (Ф.И.О)

Научный руководитель проекта _____ (Ахметов Б.С.)
(подпись) (Ф.И.О)

Задание принял к исполнению студент _____ (Толиев К.Д.)
(подпись) (Ф.И.О)

Аннотация

Стремительное развитие IT-инфраструктуры предприятий влечет за собой неконтролируемый рост количества угроз и уязвимостей информационных ресурсов (ИР). В этих условиях анализ и оценивание рисков является необходимым условием создания системы управление рисками и менеджмента информационной безопасности (ИБ) объекта защиты.

На сегодняшний день существует множество средств анализа и оценивания риска (САОР), начиная нормативными документами (стандартами) и заканчивая конкретными программными приложениями .

Аңдатпа

Осы дипломдық жұмыста АҚ-дың тиісті тапсырмаларын шешудің ең тиімді аспабын құрастыру және таңдау үшін пайдаланылатын негізгі сипаттамалардың жиынтығын анықтау мақсатында тәуекелмен байланысты негізгі түсініктер, қолданыстағы стандарттар, әдістер, әдістемелер және бағдарламалық ТТБҚ талданды және зерттелді.

Алынған негізгі сипаттамалардың негізінде шамалар жиынтығын динамикалық түрде анықтауға мүмкіндік беретін КМР-нің негізгі сипаттамаларының кортежді үлгісін жасап шығару және осылайша тиісті әзірленетін АҚ ТТБҚ-ның икемділігін қамтамасыз ету.

Abstract

The rapid development of it-infrastructure of enterprises entails an uncontrolled increase in the number of threats and vulnerabilities of information resources (IR). Under these conditions, risk analysis and assessment is a necessary condition for the creation of a risk management system and information security management (is) of the object of protection.

Today, there are many tools for risk analysis and assessment (CAEP), ranging from regulatory documents (standards) to specific software applications.

Содержание

Введение

Актуальность стремительное развитие IT-инфраструктуры предприятий неизменно влечет за собой неконтролируемый рост количества угроз и уязвимостей информационных ресурсов (ИР). В этих условиях оценивание рисков информационной безопасности (ИБ) позволяет определить необходимый уровень защиты информации (ЗИ), осуществить его поддержку и разработать стратегию развития информационной структуры объекта защиты. Анализ и оценивание рисков является необходимым условием при создании системы управления рисками и плана работ по обеспечению ИБ. Согласно рекомендациям стандарта, ISO/IEC 27001 для обеспечения ИБ на предприятии любой формы собственности необходимо внедрять систему менеджмента информационной безопасности (СМИБ). Основой такого стандарта является менеджмент рисков, под которым подразумевается анализ, оценивание и обработка рисков ИБ. На сегодняшний день существует множество средств анализа и оценивания риска (САОР), используемых для оценивания, которые представлены в достаточно широком спектре, начинающемся нормативными документами (стандартами) и заканчивающемся конкретными программными приложениями.

Цель и задачи. Целью дипломной работы является разработка гибких в использовании методов и средств анализа и оценивания риска (САОР) ИБ, как на основе статистических данных, так и на основе экспертных оценок, сделанных в нечетко определенной слабо формализованной среде**.**

Для достижения поставленной цели необходимо решить следующие основные задачи:

1) Проанализировать и исследовать базовые понятия, связанные с риском, существующие стандарты, методы, методики, методологии и программные САОР, с целью определения набора базовых характеристик, используемых для создания и выбора наиболее эффективного инструментария решения соответствующих задач ЗИ;

2) На основе полученных базовых характеристик разработать модель кортежной модели базовых характеристик КМР, позволяющую динамически определять наборы величин и таким образом обеспечить гибкость соответствующих разрабатываемых САОР ИБ;

3) На основе предложенной модели КМР разработать методы анализа и оценивания рисков ИБ, что позволит создавать эффективные средства оценивания, использующие в качестве входных данных динамически изменяемые наборы детерминированных и нечетко определенных базовых характеристик;

Объект – процесс анализа и оценивания рисков информационной безопасности;

Предмет – модели, методы, системы, методики и программные средства анализа и оценивания рисков в сфере информационной безопасности.

1 Средства анализа и оценивания рисков информационной безопасности

1.1 Анализ определений риска

В литературе встречается определение риска как действие или деятельность: реализация которого ставит под угрозу удовлетворение какой-либо достаточно важной потребности; состоящая в неопределенности ее исхода и возможных неблагоприятных последствиях в случае неуспеха для субъекта в том, или ином отношении грозящее субъекту потерей (проигрышем, травмой, ущербом); в условиях неопределенности и деятельность субъекта, связанная с преодолением неопределённости; наудачу в надежде на счастливый исход.

Как известно, действие или деятельность, также как и вероятность (измеряемая или рассчитываемая), связаны с возникновениями каких-либо характерных для них событий. Также известно, что любые действия приводят к событиям и последствиям, которые могут представлять собой как потенциальные «положительные» возможности, так и «опасности». Исходя из сказанного, в этом контексте прослеживается общность указанных понятий.

Следующую базовую характеристику, можно определить как событие, которое может произойти, или не произойти или ожидание её наступления (потенциально нежелательных воздействий на актив или его характеристики, которые могут быть следствием некоторого прошлого, настоящего или будущего события).

В большинстве указанных источников риск часто отображается вероятностью или связанными с ней понятиями, например, измеряемая или рассчитываемая вероятность: потерь, появления неблагоприятного исхода или события,(например, в результате которого возможны непредвиденные потери) возможности опасности, неудачи, получения результата от принимаемого решения, не достижения цели, появления обстоятельств обусловливающих неуверенность или невозможность получения ожидаемых результатов от реализации поставленной цели понести убытки или упустить выгоду (количественно измеряемая неуверенность в получении соответствующего дохода или убытка); реализации определенной угрозы, вида и величины нанесенного ущерб; причинения вреда имуществу, окружающей среде или жизни (здоровью) граждан, животных, растений возникновения заданной угрозы и потенциально неблагоприятных последствий возникновения этой угрозы подразумевающую потенциальную возможность нарушения безопасности данной угрозы, с помощью которой будут использоваться уязвимости актива или группы активов, чтобы привести к потере и/или повреждению имущества а также как, сочетание или комбинация вероятности события и его последствий. Известно, что вероятность связанна с

наступлением определенного события, а соответственно с ним здесь связан и риск.

Вероятность часто разделяют на «объективную» (иногда называемую физической) и «субъективную». Под объективной вероятностью понимается относительная частота появления какого-либо события в общем объеме наблюдений или отношение числа благоприятных исходов к их общему количеству. Она, например, формируется при анализе результатов большого числа наблюдений. Под субъективной вероятностью понимается мера уверенности некоторого человека или группы людей в том, что данное событие произойдет. Эта вероятность может быть формально представлена различными способами, например, вероятностным распределением или бинарным отношением на множестве событий, но наиболее часто она представляет собой вероятностную меру, полученную экспертным путем.

Также встречаются определения риска, которые отображают его как опасность: предполагаемая (известная); неизвестная на данный момент, но которая может появиться; нанесения ущерба посредством атаки (реализации некоторой угрозы с использованием уязвимости актива или группы активов).

Известны понятия риска, которые определяют его как частоту, затраты или потери, которые напрямую связаны с возникновением того или иного события. Приведем некоторые из них, например, риск как: частота реализации «опасности»; как произведение величины события на меру ее возможности; затраты или потери экономического эффекта, связанные с реализацией определенного решения (например, планового варианта) в условиях, иных по сравнению с теми, при которых решение было бы оптимальным. Также риск в любом контексте рассматривается как суммарная величина угрозы (то есть события, которые наносят ущерб), уязвимости (открытость предприятия к угрозам) и стоимости имущества (стоимость актива при опасности). Увеличение любого из этих факторов соответственно увеличивает риски, а снижение ведет к его уменьшению.

После проведенного анализа понятия риска в различных сферах жизнедеятельности человека, можно выделить одну характеристику риска, которая встречается во всех определениях приведенных выше и объединяет их – это событие, которое должно произойти и которое авторы связывают с вероятностью, действием или деятельностью, частотой, потерями, опасностью и т.д.

В аспекте ИБ риск можно связать с событием реализации угрозы ресурсам информационной системы, вследствие которого произошло нарушение одной или более их базовых характеристик безопасности – конфиденциальности, целостности, доступности. Также его, можно описать как: вероятность события, которое привело к нарушению характеристик безопасности; событие которое произошло с участием или без участия субъекта – деятельность или бездействие субъекта; событие, которое происходит с определенной частой и т.д.

При раскрытии понятия риска также следует учитывать, что большинство решений по ИБ принимаются в условиях неопределенности.

Проведенный анализ показывает, что различные трактовки понятия риска имеют общее множество характеристик, например, связь риска с вероятностью и наступлением определенного события и др. Для интерпретации этого понятия в области ИБ необходимо выделить множество его базовых характеристик присущих для этой сферы.

1.2 Методы и методики оценки рисков

CAOP 1 - Метод на основе байесовских сетей (МБС) разработан для построения каузальных моделей оценки операционных рисков. В его основе лежит теорема Байеса, ценность которой применительно к оценке таких рисков заключается в её способности комбинировать данные о вероятности событий, получаемых экспертным и статистическим путём. Для отдельных факторов риска (угроз), не имеющих статистики потерь, оценки вероятности рисковых событий могут быть основаны только на экспертных знаниях, а для других – на статистике потерь, если объём собранных данных достаточен для целей моделирования. Каждому связанному с риском событию (например – «Хакерская атака», «Несанкционированный доступ (НСД)», «Несанкционированная модификация (НСМ)» и д.р.), проводится оценка вероятности его реализации и (по цепочке) связанных с ним операционных потерь. Вероятность реализации события может быть указана в виде непрерывной функции распределения или в виде таблицы вероятностей (дискретных вероятностей). Поскольку непрерывные функции распределения удается получить лишь в редких случаях (из-за недостаточности статистики), то используются дискретные распределения. Для концептов, которые на графе не имеют входящих стрелок (например, событий, которые являются драйверами (факторами) риска), должна быть указана абсолютная вероятность каждого из возможных исходов события, а для тех, на которые влияют другие концепты, указывается условная вероятность для каждой комбинации связанных концептов. Пример экспертного задания условной вероятности показан в таблице 1.1

Таблица 1.1 - Формирование вероятности

	Исходы - условия			
Хакерская атака	ДА		НЕТ	
Заражение вирусом	Да	Нет	Да	Нет
Вероятность исхода события «Остановка сервера» для различных условий				
Произойдет	0,3	0,15	0,10	0,02
Не произойдет	0,7	0,85	0,90	0,98

Определяется абсолютная вероятность и величина расходов. Рассматриваются три категории последствий: нарушение

конфиденциальности (К), целостности (Ц) и доступности (Д). Для материальных активов ущерб определяется по шкале – от полной утраты актива до сбоя (остановки, неполадки) на несущественный промежуток времени.

САОР 2 - Методология NIST 800-30 (Risk Management Guide for Information Technology Systems, рекомендации NIST, разработчик – National Institute of Standards and Technology, США**)** охватывает девять первичных шагов: характеристика системы; идентификация угроз (таблице 1.2); идентификация уязвимостей; анализ управления; определение вероятности; анализ воздействия; определение риска; рекомендации по управлению; документирование результатов.

Таблица 1.2 - Пример идентификации угроз

Источник Угрозы	Причина	Действие угрозы
Хакер, крекер	Вызов Эго Бунт	Хакинг Социоинжиниринг Вторжение в ИС, взломы НСД в ИС.
Кибер-преступник	Разрушение информации Информационное раскрытие Денежная выгода НСМ данных	Компьютерное преступление (кибер-преследование) Мошеннические действия Информационный подкуп Spoofing Вторжение в ИС

В процессе анализа риска производится сбор информации, идентификация угроз (определение источника, причины и действия угрозы). Для оценки используются следующие уровни вероятности: высокий «В», средний «С», низкий «Н». При анализе воздействия определяются события, связанные с потерей К, Ц и Д. Величина воздействия определяется по шкале: высокая (В), средняя (С), низкая (Н). Для определения риска используется матрица УР: «В»; «С»; «Н».

Таблица 1.3 - Пример идентификации пары уязвимость-угроза

Уязвимость	Источник угрозы	Действие угрозы
ID уволенных служащих не удалены из ИС	Уволенные служащие	Проникновения в ИС на основе личных данных
Брандмауэр компании разрешает входные	Несанкционированные пользователи (например, хакеры, уволенные служащие)	Использование telnet для доступа к серверу XYZ и чтение системных файлов по

Таблица 1.3 - Пример идентификации пары уязвимость-угроза

Уязвимость	Источник угрозы	Действие угрозы
соединения telnet и на сервере XYZ включен ID гостя		ID гостя

САОР 3 - Методика TRA (Threat and Risk Assessment, разработчик – компания Government (Communications Security Establishment), Канада) разработана на основе трех руководств для IT-систем по: управлению риском безопасности (Guide to Security Risk Management for Information Technology Systems – MG-02); сертификации и аккредитации (Guide to Certification and Accreditation of Information Technology Systems – MG-01); оценке риска и выбору гарантий (Guide to risk assessment and safeguard selection for Information Technology Systems MG-03). Для оценки риска, аналитик должен рассмотреть описание IT-системы, идентифицировать существенные сценарии угроз, оценить воздействие и их ВВ (рисунок. 1.1).

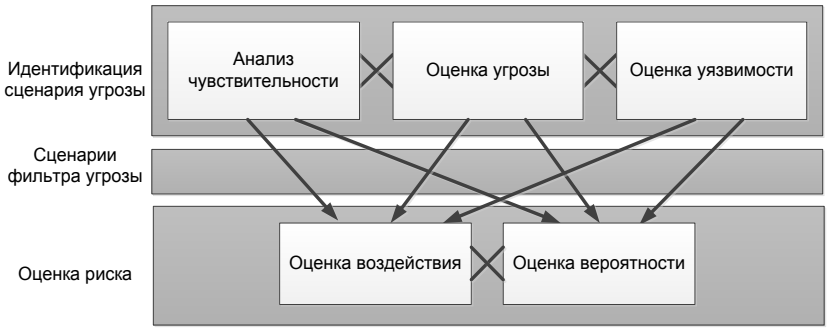


Рисунок 1.1 - Процесс оценки риска

В процессе оценки риска для каждого сценария угрозы, рассчитываются ее воздействие и вероятность. Такой подход отображает средние ожидаемые потери за определенный период времени. По сути, риск (R) описывается как функциональная связь между стоимостью активов (A_{Val}), угрозой (T) и уязвимостью (V): $R = f(A_{Val}, T, V)$. Оценка угрозы (например, «Хакерская атака») для такой подгруппы активов, как корпоративные данные (КД) осуществляется на основе таблице 1.4 , где уровень нарушения таких характеристик ИБ, как НК, НЦ и НД отображается трехуровневой КЧ шкалой («В», «С», «Н»).

Таблица 1.4 - Пример оценки угрозы

Класс угрозы	Действие угрозы	Категория агента угрозы (АУ)	АУ	Событие угрозы	Уровень нарушения			Подгруппа активов
					К	Ц	Д	
Предна-	Шпионаж	Хакеры	-	НСД	В	-	-	КД

меренная	Саботаж	Хакеры	-	НСМ	-	-	В	КД
	Саботаж	Хакеры	-	DoS	-	Н	-	КД

САОР 4 - Методика FRAP (Facilitated Risk Analysis Process, разработчик – компания Peltier and Associates, США) ориентирована на обеспечение ИБ ИС, рассматриваемое в рамках процесса управления рисками, состоящего из пяти этапов. Этап 1 – Определение защищаемых активов (производится на основе опросников, изучения документации на систему, использования инструментов автоматизированного анализа (сканирования) сетей). Этап 2 – Идентификация угроз. При составлении списка угроз могут использоваться разные подходы, например: выбор актуальных для данной ИС угроз из заранее подготовленных экспертами перечней (checklists); анализируется статистика инцидентов ИБ связанных с данной ИС; оценивается их среднегодовая частота (по ряду угроз, например, возникновение пожара, данные можно получить у соответствующих государственных организаций); специалисты компании решают задачу посредством «мозгового штурма» и д.р. Этап 3 – Оценка риска (ОР). Каждой угрозе из составленного списка сопоставляют ее ВВ, далее оценивают ущерб, который может быть нанесен данной угрозой и по полученным значениям, оценивается ее уровень. При проведении анализа риска, как правило, принимают, что на начальном этапе в системе отсутствуют средства и механизмы защиты. Таким образом оценивается уровень риска (УР) для незащищенной ИС, что в последствии позволяет показать эффект от внедрения средств защиты информации (ЗИ). Оценка производится по ВВ угрозы и ущерба от её реализации в течение года с использованием следующих шкал. Для вероятности (Probability): высокая (High Probability) – вероятно; средняя (Medium Probability) – возможно; низкая (Low Probability) – маловероятно. Для ущерба (Impact – мера величины потерь или вреда, наносимого активу): «В» (High Impact) – остановка критически важных бизнес-подразделений, которая приводит к существенному ущербу для бизнеса, потере имиджа или неполучению существенной прибыли; «С» (Medium Impact) – кратковременное прерывание работы критических процессов или систем, которое приводит к ограниченным финансовым потерям в одном бизнес-подразделении; «Н» (Low Impact) – перерыв в работе, не вызывающий ощутимых финансовых потерь. Оценка осуществляется в соответствие с правилом, задаваемым матрицей рисков (см. рисунке1.16) и может интерпретироваться следующим образом: уровень *A* – связанные с риском меры (например, внедрение средств ЗИ) должны быть выполнены немедленно и в обязательном порядке; уровень *B* – связанные с риском меры должны быть предприняты; уровень *C* – требуется мониторинг ситуации (но непосредственных мер по противодействию угрозе принимать, возможно, не надо); уровень *D* – никаких мер в данный момент предпринимать не надо. Этап 4 – Определение контрмер. После идентификации угроз и оценки риска определяются контрмеры, позволяющие устранить риск или свести его до приемлемого уровня. Этап 5 – Документирование. После анализа и оценивания риска результаты подробно документируются в

стандартизованном формате. Полученный отчет может быть использован при определении политик, процедур, бюджета ИБ и т.д.

P IMPACT

	High	Medium	Low
High	*A*	*B*	*C*
Medium	*B*	*B*	*C*
Low	*B*	*C*	*D*

R O B A B I L I T Y

A – Corrective action must be implemented
B – Corrective action should be implemented
C – Requires monitor
D – No action required at this time

Рисунок 1.2 - Матрица рисков FRAP

САОР 5 - Методика BSI-Standard 100-3 (Risk Analysis based on IT-Grundschutz – анализ рисков на основе IT-Grundschutz, разработана Федеральным Агентством по ИБ (Federal Office for Information Security – BSI), Германия) основывается на процессе анализа и оценивания риска IT-безопасности, предложенного в BSI-Standard 100-3-й, включает семь этапов. Этап 1 – Предварительная подготовка. На этом этапе определяется область ИБ, требования к ней (нормальные, высокие и очень высокие), которые рассматриваются с точки зрения обеспечения К, Ц и Д. Также проводится анализ структуры предприятия, дополнительный анализ ИБ, оценивается её текущий уровень. Этап 2 – Подготовка описания угрозы. С помощью предложенного в методике списка угроз осуществляется их анализ для конкретного предприятия. Идентифицируются модули и целевые объекты (ЦО) защиты, которые заносятся в таблицу (таблице 1.5) .

Таблица 1.5 - Пример идентификации

№	Название модуля	ЦО
B 2.4	Серверная комната	Каб. М. 723
B 2.6	Производственная комната	Каб. М. 811
B 3.101	Сервер	S3
B 3.207	Главный клиент	C4
B 3.301	Шлюз безопасности (Firewall)	N3

Каждый модуль ЗИ связан со списком угроз, а номер и их название соответствует конкретному ЦО. Результатом прохождения этапа является список угроз конкретному объекту (таблице 1.6).

Таблица 1.6 - Пример описания угроз

Сервер S3
К: нормальная; Ц: высокая; Д: высокая
Т 1.2 Отказ IT-системы Т 3.2 Неумышленное уничтожение актива Т 4.1 Перебой в питании Т 5.57 Сетевое сканирование Т 5.85 Потеря Ц информации и т.д.

Далее в обобщенной таблице угрозы сортируются по каждому ЦО. Этап 3 – Определение дополнительных угроз. Здесь используется специальный набор запросов, например: «Какие потенциальные форс-мажорные обстоятельства представляют особые угрозы информационной области?»; «Каких организационных недостатков нужно избежать любой ценой для гарантирования ИБ?»; «Какие ошибки человека оказывают негативное влияние на ИБ?»; «Какие специальные проблемы ИБ могли произойти с рассматриваемым ЦО, из-за технического отказа?» и т.д. Этап 4 – Оценка угрозы (ОУ). Здесь производится тематический опрос специалистов на основе базовых запросов. Результаты фиксируются в таблице с указанием Y (если меры ИБ (осуществленные или предусматриваемые) обеспечивают надлежащую засщиту от соответствующей угрозы или, что угроза не важна для текущего анализа степени риска) или N (если меры ИБ (осуществленные или предусматриваемые) не обеспечивают надлежащую защиту от соответствующей угрозы) для каждой отдельной угрозы (таблице. 1.7)).

Таблица 1.7 - Угрозы

Сервер S3	ОУ
К: нормальная; Ц: высокая; Д: высокая	
Т 1.2 Отказ IT системы	N
Меры ИБ для сервера S3 не предотвращают реализацию угрозы. IT – меры по Каталогу Grundschutz не соответствуют	
Т 5.85 Потеря Ц информации	N
Информация клиента о заказе не должна подвергаться НСМ. Иначе это может привести к излишкам (нехватки) поставок, тем самым навлекая компании высокие затраты.	

Этап 5 – Обработка рисков. Здесь используется шкала: «*A»* – снижение риска посредством дополнительных мер; «*B»* – предотвращение риска посредством реструктурирования; «*C»* – принятие риска; «*D»* – передача риска; (таблице. 1.8) . Этап 6 – Консолидация концепции ИБ. Этап 7 – Обратная связь.

Таблица 1.8 - Пример таблицы обработки риска

Сервер S3	
К: нормальная; Ц: высокая; Д: высокая	
Т 1.2	Отказ IT-системы
«*A*» S 6. U1	Дополнительная IT-мера по ИБ: Осуществление полной замены системы для общения с клиентом. Реализуется полная замена системы для связи с клиентами. Это касается всех технических средств, включая каналы связи. Резервная система располагается в помещении Е.3. С возможностью использованием в любой момент времени, (не > 30 мин. задержки производства). Используется модемная связь с клиентом. Вся система замены, включая модемное соединение, проверяется не реже одного раза в квартал и всякий раз, при изменении конфигурации.
Т 5.85	Потеря Ц информации
«*C*»	Принятие риска: Хотя риск минимизирован до некоторой степени механизмами ИБ, которые встроены в систему передачи и IT-систему, но возможны дальнейшие инциденты, приводящие к НСМ информации о требовании заказа, что подвергает компанию высокому риску. Этот остаточный риск принят руководством, поскольку эффективные противодействия будут неэкономными.

САОР 6 - Методика РС БР ИББС-2.2-2009 (Рекомендации в области стандартизации Банка России, обеспечение ИБ организаций банковской системы, Российская Федерация) анализа и оценивание риска нарушения ИБ проводится для типов информационных активов (ИА), входящих в предварительно заданную область оценки. На начальном этапе определяется: полный перечень типов ИА, входящих в область оценки (на основе результатов их классификации); полный перечень типов объектов среды, соответствующих каждому из типов ИА области оценки; модель угроз ИБ, основанной на всех выделенных типах объектов среды всех уровней иерархии информационной инфраструктуры. Оценка риска нарушения ИБ определяется на основании КЧ оценок вероятности реализации угрозы (в оригинале СВР – степень возможности реализации угроз ИБ) и потенциального ущерба от ее реализации (в оригинале СТП – степень тяжести последствий от потери свойств ИБ для рассматриваемых типов ИА).

Оценка определяется на основе экспертного мнения специалистов службы ИБ с привлечением профессионалов в области IT. Дополнительно, следует привлекать сотрудников профильных подразделений, использующих рассматриваемые типы ИА. Для проведения оценки рисков нарушения ИБ

выполняются 6 процедур: 1. Определение перечня типов ИА, для которых выполняется оценка (т.е. области оценки рисков). Может рассматриваться компания в целом, ее отдельное подразделение, либо отдельный процесс. Для каждого типа ИА следует определить, какие для него свойства ИБ (К, Ц, Д и, при необходимости, другое) должны быть обеспечены; 2. Определение перечня типов объектов среды (разделяются по уровням информационной инфраструктуры) соответствующих каждому из типов ИА; 3. Определение перечня актуальных источников угроз (формируется на основе модели угроз компании) для каждого из указанных типов; 4. Определение СВР угроз в отношении типов объектов среды. На основе пятиступенчатой КЧ шкалы («нереализуемая» (НР), «минимальная» (МН), «средняя» (СР), «высокая» (ВС), «критическая» (КР)) проводится анализ возможности потери свойств ИБ для каждого из типов ИА в результате воздействия угроз. Основными факторами для оценки СВР угроз ИБ является: информация соответствующих моделей угроз (данные о расположении источника угрозы его мотивации и предположения о квалификации (ресурсах) источника), статистические данные о частоте реализации угрозы ее источником в прошлом, информация о способах осуществления угроз и сложности их обнаружения, а также данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих априорных защитных мер; 5. Определение СТП для типов ИА на основе анализа последствий потери каждого из значимых свойств ИБ для каждого из типов ИА в результате воздействия на соответствующие им типы объектов среды выделенных источников угроз. Используется четырехступенчатая КЧ шкала («МН», «СР», «ВС», «КР»). Основными факторами для оценки являются: степень влияния на непрерывность и репутацию деятельности компании; объем финансовых (материальных) потерь и затрат на восстановления свойств ИБ ИА (ликвидации последствий нарушения ИБ – финансовых, материальных, временных и людских ресурсов); степень нарушения законодательных требований (договорных обязательств компании), а также требований регулирующих и контролирующих органов в области ИБ; объем хранимой, передаваемой, обрабатываемой и уничтожаемой информации, соответствующей рассматриваемому типу объекта среды; данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих защитных мер, снижающих тяжесть последствий (апостериорных); 6. Оценивание рисков нарушения ИБ проводится на основании сопоставления СВР угроз и СТП нарушения ИБ вследствие реализации соответствующих угроз. Оценка проводиться для всех значимых свойств ИБ выделенных типов ИА, всех соответствующих им комбинаций типов объектов среды и воздействующих на них источников угроз. Используется следующая КЧ шкала рисков: допустимый (Д), недопустимый (НД). Для сопоставления СВР угроз и СТП заполняется таблица допустимых и недопустимых рисков нарушения ИБ (таблице. 1.9).

Таблица 1.9 - Д и НД риски

СВР угроз ИБ	СТП нарушения ИБ			
	МН	СР	ВС	КР
НР	Д	Д	Д	Д
МН	Д	Д	Д	НД
СР	Д	Д	НД	НД
ВС	Д	НД	НД	НД
КР	НД	НД	НД	НД

Риски нарушения ИБ могут быть оценены в КЛ (денежной) форме на основании оценок СВР угроз ИБ (например, в %) и СТП (например, в денежном виде от величины капитала компании (ВКК)). Количественные оценки также производятся экспертными методами. При необходимости, могут использоваться шкалы (таблице. 1.10) соответствия КЧ и КЛ оценок СВР угроз и СТП.

Таблица 1.10 - Шкалы соответствия

СВР угрозы		СТП нарушения ИБ	
($М_{кч}$)	($М_{кл}$), %	($М_{кч}$)	($М_{кл}$), %
НР	0	МН	[0; 0,5[
МН	]0; 20[	СР	[0,5; 1,5[
СР	[20; 50[	ВС	[1,5; 3,0[
ВС	[50; 100[	КР	[3,0; 100] (от ВВК)
КР	100		

Количественные оценки рисков нарушения ИБ является произведением оценок СВР угроз и СТП для каждого из значимых свойств ИБ выделенных типов ИА и всех соответствующих им комбинаций объектов среды и воздействующих на них источников угроз. Суммарная ОР компании вычисляется как сумма КЛ оценок по отдельным рискам нарушения ИБ. Также в методике есть перечни рекомендуемых классов и источников угроз ИБ.

1.3 Другие известные подходы к оцениванию рисков

СAOP 7 - Стандарт ISO/IEC 27005:2008 (Information technology – Security techniques – Information security risk management (Информационная технология – Методы защиты – Менеджмент рисков ИБ) представляет технический пересмотр стандартов, отмену и замену ISO/IEC TR 13335-3:1998 и ISO/IEC TR 13335-4:2000, Швейцария) предоставляет рекомендации для менеджмента риском ИБ организации, в особенности поддерживая

требования «Системы менеджмента информационной безопасности» (ISMS) согласно ISO/IEC 27001. Процесс менеджмента реализуется в шесть этапов.

Этап 1 – Создание контекста. Осуществляется общий анализ всей информации об организации, относящейся к созданию контекста, а также производится установка основных критериев, необходимых для менеджмента рисков ИБ и определение для него области применения и границ осуществления.

Этап 2 – Оценка рисков. Здесь осуществляется идентификация (активов, угроз, существующих требований, уязвимостей и последствий), оценка и описание (КЛ, КЧ или их комбинация), расположение по приоритетам рисков, относящимся к организации. Качественная оценка использует шкалу квалификации атрибутов, чтобы описать величину потенциальных последствий (например: низкие, средние или высокие) и вероятность, что эти последствия произойдут. Количественная оценка использует масштаб с числовыми значениями, как для последствий, так и вероятности. Количественная оценка в большинстве случаев использует статистику инцидентов. Результатами прохождения данного этапа будут оценки последствий, вероятности инцидента и УР.

Этап 3 – Обработка рисков. Включает общее описание обработки, а также снижение, сохранение, предотвращение и перенос риска.

Этап 4 – Принятие риска. Планы обработки риска должны описать, как оценённые риски были обработаны, до приемных критериев.

Этап 5 – Коммуникации риска. Обмен информацией о риске между лицами, принимающими решение и другими причастными сторонами с целью достижения соглашения по управлению рисками. Этап 6 – Мониторинг и пересмотр риска ИБ. Здесь осуществляется мониторинг и пересмотр факторов риска, а также улучшение его менеджмента. В стандарте присутствуют рекомендации и примеры: определения области применения и границ процесса менеджмента рисков (Приложение A); идентификации и определения ценности активов, стоимости воздействия (Приложение B); типичных угроз (Приложение C, табл. 1.11, где метки имеют следующее значения: D – преднамеренный (намеренные акции, нацеленные на ИА), A – случайный (непреднамеренные действия человека на ИА) и E – экологический (инциденты, которые не основаны на действиях человека)); уязвимостей и методы их оценивания (Приложение D, см. пример уязвимостей для аппаратных средств в табл.); подходов к оценке рисков; ограничения по снижению риска (Приложение F). Стандарт имеет реализации в ПС, например, Meycor KP (Knowledge Provider).

Таблица 1.11 - Пример типичных угроз

Тип	Угрозы	Метки
НСД	Несанкционированное использование Оборудования	D
	Мошенническое копирование ПС	D

	Использование поддельных или скопированных ПС	A, D
	Искажение данных	D
	Незаконная обработка данных	D

В ISO/IEC 27005:2008 предложена высокоуровневая и детальная ОР ИБ. Для последней может использоваться матрица с предопределёнными значениями (см. таблица. 1.12). Для каждого актива рассматриваются соответствующие уязвимости и угрозы, например, если ценность актива – ЦА = 3, ВВ угрозы – ВВУ = «В» и простота использования уязвимости – ПИУ = «Н» то мера риска – МР = 5.

Таблица 1.12 - Примеры

Уязвимости	Угрозы
Недостаточное обслуживание (дефектная инсталляция)	Брешь в возможности ремонта ИС
Изъяны схем для периодических замен	Разрушение оборудования (носителей)
Изъяны эффективного контроля внесения изменений конфигурации	Ошибка в использовании
Восприимчивость к перепадам питания	Потеря источника питания
Незащищённое Хранение	Воровство носителей (документов)
Недостаток в осторожности при уничтожении	Воровство носителей (документов)
Неконтролируемое копирование	Воровство носителей (документов)

Также предложена матрица определения вероятности сценария инцидента (ВСИ) (см. таблице 1.13 , где «ОН» (очень низкая), «Н» (низкая), «С» (средняя), «В» (высокая), «ОВ» (очень высокая)), что соответственно означает (очень маловероятно), (маловероятно), (возможно), (вероятно), (часто). Получаемое в результате значение риска измеряется по шкале от 0 до 8 (например, «Н» (0-2); «С» (3-5); «В» (6-8)), может быть оценено относительно критериев принятия риска.

Таблица 1.13 - Матрица оценки МР

ВВУ		Н			С			В		
ПИУ		Н	С	В	Н	С	В	Н	С	В
ЦА	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5

Таблица 1.14 - Матрица определения ВСИ

ВСИ		ОН	Н	С	В	ОВ
Влияние на бизнес	ОН	0	1	2	3	4
	Н	1	2	3	4	5
	С	2	3	4	5	6
	В	3	4	5	6	7
	ОВ	4	5	6	7	8

2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	**5**	6	7
4	4	5	6	5	6	7	6	7	8

В приложении стандарта рассмотрен пример ранжирования угроз посредством мер риска (см. таблице1.14).

Матрица может использоваться, для связи факторов последствий (ЦА) с ВВУ (принимая в расчет аспекты уязвимости). Изначально по определенной шкале (например, 1 ÷ 5) производится оценка ЦА для каждого находящегося под угрозой актива (колонка (b)). Далее, например, по той же шкале оценивается ВВУ, для каждой угрозы (колонка (c)) и по полученным результатам вычисляется мера риска (колонка (d)) путем умножения $d = b \times c$. Впоследствии проводится ранжирование угроз (колонка (e)) в порядке соответствующей меры риска (в таблице. 1.15 1 – самое низкое последствие и самая низкая ВВУ. В колонке (a) отображены идентификаторы угрозы).

Таблица 1.15 - Пример ранжирования угроз

(a)	(b)	(c)	(d)	(e)
A	5	2	10	2
B	2	4	8	3
C	3	5	15	1
D	1	3	3	5
E	4	1	4	4
F	2	4	8	3

Рассмотрим пример (предложенный в стандарте) оценки значения для вероятности рисков и их возможных последствий. Здесь особое внимание уделяется последствиям инцидентов ИБ (сценариям инцидентов) и определению того, каким системам следует отдавать предпочтение. Это выполняется путем оценки двух значений для каждого актива и угрозы,

комбинация которых будет определять баллы ($Б_{ij}$), где *i* и *j* – соответственно номер актива и угрозы. Суммирование всех баллов активов, дает возможность определить МР. Сначала каждому активу присваивается ЦА для каждого случая возникновения соответствующей угрозы. Это значение связано с возможными неблагоприятными последствиями, которые могут возникать, при реализации угрозы. Далее определяется показатель вероятности риска (ПВР). Он оценивается исходя из комбинации ВВУ и ПИУ. Затем, по пересечению линий значений ЦА и ПВР присваиваются соответствующие баллы. После чего они подсчитываются, для получения итоговых значений по каждому активу.

В следующих примерах все значения выбраны случайным образом. Предположим, что система С имеет три актива $А_1$, $А_2$, $А_3$ и существуют две угрозы $У_1$, $У_2$ этой системе. Пусть $ЦА_1 = 3$, $ЦА_2 = 2$ и $ЦА_3 = 4$. Если для $А_1$ и $У_1$ $ВВУ_{11}$ = «Н» и $ПИУ_{11}$ = «С», то значение $ПВР_{11} = 1$ (см. табл. 1.17). Баллы для $А_1$ и $У_1$ могут быть выведены из табл. 1.15 на пересечении линий $ЦА_1 = 3$ и $ПВР_{11} = 1$, т.е. $Б_{11} = 4$. Аналогичным образом, пусть для $А_1$ и $У_2$ $ВВУ_{12}$ = «С», а $ПИУ_{12}$ = «В», то $ПВР_{12} = 3$ т.е. $Б_{12} = 6$. Теперь могут быть вычислены итоговые баллы ($БИ_i$) актива относительно всех угроз $БИ_1=Б_{11}+Б_{12} = 10$ (для каждого актива и его угрозы). Вычисление итоговых баллов по всей системе (БИС) производится путем суммирование всех балов по каждому активу относительно всех угроз $БИС=БИ_1+БИ_2+БИ_3$. В стандартах ISO/IEC 27001 и 27002 на этапе оценки риска ИБ дается ссылка на документ ISO/IEC TR 13335-3, который теперь представлен как ISO/IEC 27005.

Таблица 1.17 - Балльник

ПВР	ЦА				
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

САОР 8 - Методика Risk Matrix (разработчик компания Mitre Corporation, США) ориентирована на оценивание риска и впоследствии была реализована приложением для Microsoft Excel. Основной процесс включает: планирование оценки степени риска; идентификацию задач или требований; определения; ранжирование; составление рейтинга рисков; управление планами действий; непрерывную оценку рисков. Оценки риска заключается в планировании деятельности.

Изначально производится идентификация риска с помощью применения экспертами «Мозгового штурма». Далее присваиваются различные атрибуты каждому риску, такие как, например, период времени (даты начала и окончания возможной реализации) и ВВ. С помощью сценария «Если риск …, то последствия …» составляется матрица риска. Для определения воздействия

используется шкала: C (критическое); S (серьезное); M_o (средние); M_i (низкое); N (незначительное), а для вероятности – (BC_3): 0-10% (очень низкая); 11-40% (низкая); 41-60% (средняя); 61-90% (выше среднего); 91-100% (высокая).

Таблица 1.18 - Шкала риска

ПВР (%)	Категории воздействия				
	N	M_i	M_o	S	C
0-10	H	H	H	C	C
11-40	H	H	C	C	B
41-60	H	C	C	C	B
61-90	C	C	C	C	B
91-100	C	B	B	B	B

На этапе ранжирования используется метод Borda и далее составляется рейтинг риска с определением его степени – «H», «C» или «B» табл. 1.23. Для определения наиболее приоритетных рисков используется диаграмма частот (см. рисунок. 1.17). Пример матрицы риска представлен на рисунок. 1.18.

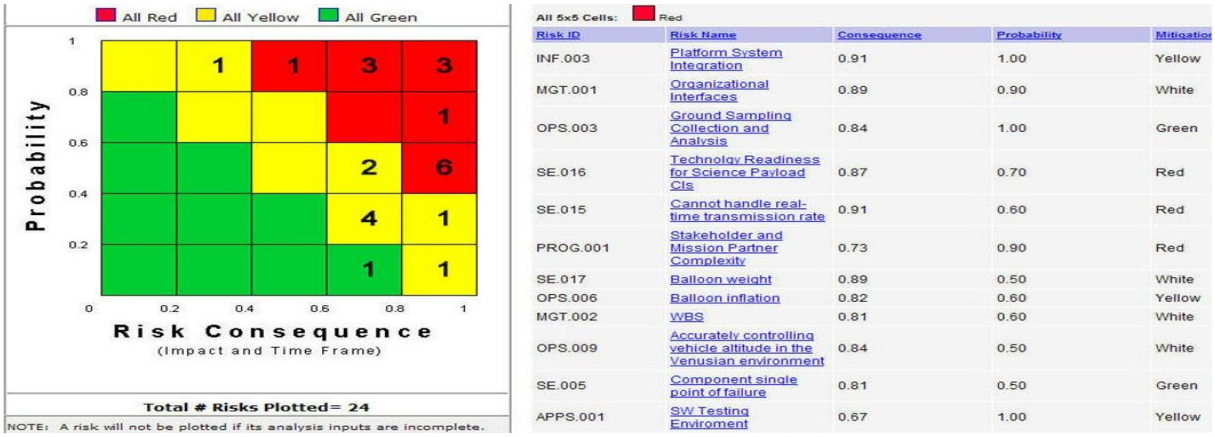


Рисунок 1.3 - Диаграмма частот

САОР 9 - Стандарт AS/NZS 4360:2004 (стандарт риск-менеджмента, Австралия и Новая Зеландия) предоставляет рекомендации по анализу и оцениванию риска, которые проводится в 7 этапов.

1) Определение контекста оценки степени риска. Устанавливается контекст риск-менеджмента, критерии оценки риска и определяется схема анализа.

2) Идентификация риска основывается на инициализации таблице 1.24

3) Анализ степени риска. Производится идентификация и оценка существующих средств управления. Определяются последствия, вероятность и УР с помощью матрицы риска .

4) Оценка риска. Сравниваются оцененные УР с предустановленными критериями, и рассматривается баланс между потенциальными выгодами и неблагоприятными последствиями.

5) Обработка риска.

6) Контроль.

7) Консультации

САОР 10 - Методика MAGERIT(Methodology for Information Systems Risk Analysis and Management, разработчик Ministerio De Administraciones Públicas, Испания) предназначена для реализации анализа и оценивания риска, которая проводится в 3 этапа:

Этап 0 – Планирование.

Этап 1 – Анализ риска. Состоит из 5 шагов: 1. Идентификация и оценка активов, являющихся элементами ИС (или тесно связанных с ней) ценными для организации. Активы предлагается разделять на 5 групп (окружающая среда, ИС, информация, функции организации, другие активы) для определения зависимости между ними. После ранжирования активов производится их оценка относительно стоимости. Далее определяются требования к К, Ц и Д и подлинности актива; 2. Анализ и ОУ ИБ. С помощью категории угроз, которые приведены в данной методике, производится их идентификация, реализуется оценка частоты (используется шкала: 100 – очень часто (ежедневно); 10 – часто (ежемесячно); 1 – обычно (ежегодно); 1/10 – редко (раз в несколько лет)) и ущерба; 3. Определение превентивных мер для предотвращения угрозы; 4. Оценка воздействия. Измерение повреждения активов связанного с угрозой; 5. Определение риска. Риск отражается вероятностью повреждения ИС и увеличивается с ростом воздействия и частоты.

Этап 2 – Управление рисками. Выбираются и реализуются защитные меры (технические, физические, защиты рабочей среды для людей и оборудования, организационные меры, кадровая политика), а также осуществляется интерпретация значения для воздействия и остаточных рисков, проводится анализ прибыли и убытков.

Таблица 1.21 - Пример потенциальных угроз файлам данных

Угрозы		Измерение ИБ (%)						
актив/угроза	F	D	I	C	AS	AD	TS	TD
[D_exp] Текущие файлы		50	50	100	100	100	100	100
[E.1] Ошибки пользователей	10	10	10					
[E.2] Ошибки администратора	1	20	20	10	10	10	20	20
[E.3] Ошибки мониторинга	1						50	50
[E.4] Ошибки конфигурации	0,5	50	10	10	50	50	50	50

[E.14] Утечка информации	1			1				
[E.15] Искажения информации	10		1					
[E.16] Введение ошибочных данных	100		1					
[E.18] Уничтожение информации	10	1						
[E.19] Раскрытие информации	1			10				
[A.4] Изменения конфигурации	0,1	50	10	50	100	100	100	100
[A.11] Несанкционированный доступ	100		10	50	50			

Методика реализована в ПО «Techniques Guide» примеры оценок показаны на рис. 1.19 и 1.20, где D, I и C – соответственно К, Ц и Д данных, AS и AD – соответственно подлинность пользовательских услуг и происхождения данных TS и TD – соответственно подотчетность использования услуг и доступа к данным.

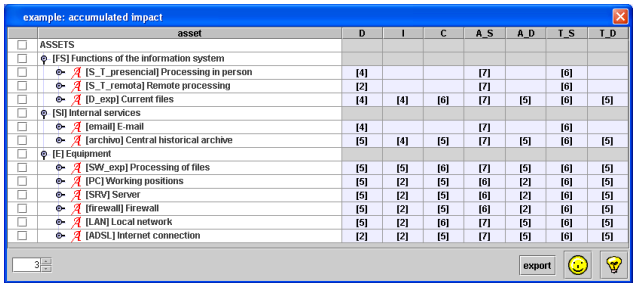


Рисунок1.4 - Пример оценки воздействия

САОР 11 - Методика Information Security RA (Risk Assessment, разработчик Centers for Medicare & Medicaid Services (CMS), США) предоставляет возможность реализации АОР в сфере ИБ. Методика состоит из 3 фаз:

Фаза 1. Документирование системы. Фаза реализуется в нескольких процессах – идентификация системной документации и активов, а также определение текущего уровня ИБ (с использованием шкалы: «В», «С» и «Н» табл.); Фаза 2. Определение риска. Расчет УР для каждой пары угрозы и уязвимости, на основе вероятности того, что угроза с использованием уязвимости будет осуществлена и степень воздействия, которую она окажет на ИС (ее данные и бизнес-функции) с точки зрения потери К, Ц и Д.

Фаза 2 состоит из 6 шагов: 1. Выявление угрозы; 2. Определение уязвимости; 3. Выявление существующих элементов управления для снижения риска реализации данной угрозы (с использования уязвимости). 4. Определение ее ВВ с учетом существующих элементов управления, для чего используется семиуровневая шкала: НЗ – незначительная (маловероятно); ОН – очень низкая (вероятно два/три раза в пять лет); Н – низкая (произойдет один раз в год или меньше); С – средняя (может произойти один раз в шесть месяцев или менее); В – высокая (произойдет один раз в месяц или меньше); ОВ – очень высокая вероятность (несколько раз в месяц); ЭВ – Экстремально вероятно (несколько раз в день). 5. Оценивание степени воздействия на систему осуществляется по шестиуровневой шкале: НЗ – незначительное, МЛ

– малое, ЗН – значительное, ПВ – повреждающее, СЕ – серьезное, КР – критическое. 6. Определение УР для данной пары угроза – уязвимость существующих элементов управления. Уровни риска определяются согласно таблице 1.22.

Таблица 1.22 -Уровни риска

ВВ	Воздействие					
	НЗ	МЛ	ЗН	ПВ	СЕ	КР
НЗ	Н	Н	Н	Н	Н	Н
ОН	Н	Н	Н	Н	С	С
НК	Н	Н	С	С	В	В
СР	Н	Н	С	В	В	В
ВС	Н	С	В	В	В	В
ОВ	Н	С	В	В	В	В
ЭВ	Н	С	В	В	В	В

Фаза 3 Определение защиты состоит из четырех шагов: 1. Определение элементов управления/мер безопасности для снижения уровня риска; 2. Определение остаточной вероятности возникновения угрозы; 3. Определение остаточного воздействия уязвимости; 4. Определение остаточного уровня риска для системы.

1.4 Вывод

1) Проанализировано базовые понятия, связанные с риском. Проведенный анализ показывает, что различные трактования риска имеют общее множество характеристик, например, связь риска с вероятностью и наступлением определенного события и др. Для интерпретации этого понятия в области ИБ необходимо выделить множество его базовых характеристик присущих для этой сферы.

2) Проведен анализ и исследования существующих стандартов, методов, методик, методологий и программных САОР, с целью определения входных, внутренних и выходных параметров, используемых для создания и выбора наиболее эффективного инструментария решения соответствующих задач ЗИ.

2 Модель и методы анализа и оценивания рисков информационной безопасности

2.1 Кортежная модель базовых характеристик риска

Стремительное развитие IT-инфраструктуры предприятий неизменно влечет за собой неконтролируемый рост количества информационных угроз и уязвимостей информационных ресурсов. В этих условиях оценивания рисков ИБ позволяет определить необходимый уровень ЗИ, осуществить его поддержку и разработать стратегию развития информационной структуры компании. Оценивание и анализ рисков ИБ является необходимым условием при создании системы управления рисками и плана обеспечения непрерывности и возобновления бизнеса.

В п. 1.1 проведен анализ толкований риска во многих отраслях человеческой деятельности с целью его отображения на сферу ИБ, а также выделены базовые характеристики риска.

В различных публикациях существует множество определений риска, несущих достаточно широкое его трактование. Только в Интернет-словарях содержится свыше 1500 толкований риска во многих сферах человеческой деятельности. Вследствие этого возникают различные неоднозначности, связанные с раскрытием сущности самого риска и связанных с ним понятий. Соответственно такое состояние характерно и для сферы ИБ.

Учитывая, что риски затрагивают различные предметные области, то это понятие следует рассмотреть с точки зрения:

1) Безопасности;
2) Психологии;
3) Экономики;
4) Страхования;
5) Медицины;
6) Геологии;

и т.д., которое раскрывается как в монографиях, статьях, учебниках, словарях так и различных нормативных, национальных и международных документах.

Для формализации процесса формирования базовых характеристик риска введем множество всех возможных характеристик

$$\boldsymbol{BC} = \bigcup_{i=1}^{n} \boldsymbol{BC}_i = \{\boldsymbol{BC_1}, \boldsymbol{BC_2}, ..., \boldsymbol{BC_n}\}, \quad (1)$$

где n – количество членов ВС.

Например, при n=6множество ВС может иметь следующий вид

$$\boldsymbol{BC} = \bigcup_{i=1}^{6} \boldsymbol{BC}_i = \{\boldsymbol{BC_1}, \boldsymbol{BC_2}, \boldsymbol{BC_3}, \boldsymbol{BC_4}, \boldsymbol{BC_5}, \boldsymbol{BC_6}\} = \{\text{«Действие»},$$

«Событие», «ВЕРОЯТНОСТЬ», «ОПАСНОСТЬ», «ЧАСТОТА», «РАСХОДЫ»}.

После проведенного анализа понятия риска в различных сферах жизнедеятельности человека, можно выделить следующую базовую характеристику риска – «Действие» (BC_1), которое привело к событию нарушения ИБ. С точки зрения ИБ BC_2 связано с реализацией потенциальных угроз базовым характеристикам безопасности ресурсов информационных систем (РИС), которые привели к возникновению нежелательного события**.** В связи с этим, базовую характеристику BC_1 можно отобразить множеством идентификаторов

$$\boldsymbol{BC_1} = \bigcup_{i=1}^{bc_1} BC_{1i} = \{BC_{11}, BC_{12}, ..., BC_{1bc_1}\}, \quad (1.2)$$

(где bc_1 – количество идентификаторов угроз), например, при bc_1=3 множество BC может иметь следующий вид

$\boldsymbol{BC_1} = \bigcup_{i=1}^{3} BC_{1i} = \{BC_{11}, BC_{12}, BC_{13}\}$={«Компьютерный шпионаж», «Шпионаж», «Сбой программного обеспечения»}.

Следующую базовую характеристику, можно определить как, – «Событие»(BC_2), которое можно отображать в виде символьной переменной, принимающей одно из значений конечного множества идентификаторов

$$\boldsymbol{BC_2} = \bigcup_{i=1}^{bc_2} BC_{2i} = \{BC_{21}, BC_{22}, ..., BC_{2bc_2}\}, \quad (1.3)$$

(bc_2 – количество идентификаторов событий). С учетом того, что в области ИБ риск связан с такими базовыми характеристиками безопасности РИС как конфиденциальность, целостность и доступность, то базовые события при bc_2=7 могут идентифицироваться как,

$$\boldsymbol{BC_2} = \bigcup_{i=1}^{7} BC_{2i} = \{BC_{21}, BC_{22}, BC_{23}, BC_{24}, BC_{25}, BC_{26}, BC_{27}\} = \{\text{«Нарушение}$$

конфиденциальности (НК)», «Нарушение целостности (НЦ)», «Нарушение доступности (НД)», «Нарушение целостности и конфиденциальности (НЦК)», «Нарушение целостности и доступности (НЦД)», «Нарушение конфиденциальности и доступности (НКД)», «Нарушение конфиденциальности, целостности и доступности (НКЦД)»}.

Следует отметить, что когда возникают сложности с получением статистических данных, а также для простоты интерпретации величин, эксперты используют логико-лингвистический подход. С его помощью осуществляется отображение соответствующей характеристики посредством ЛП «ВЕРОЯТНОСТЬ» с определенным базовым терм-множеством, например,

$$\boldsymbol{BC_3} = \bigcup_{i=1}^{bc_3} \underset{\sim}{BC}_{3i} \qquad (1.4)$$

(bc_3 – количество термов), для членов которого справедливо отношение порядка $\underset{\sim}{BC}_{31} < \underset{\sim}{BC}_{32} < ... < \underset{\sim}{BC}_{3bc_3}$. Следует отметить, что термы ЛП $\boldsymbol{BC_3}$ связываются указанным отношением посредством применения методов сравнения нечетких чисел [29]. Например, для указанной ЛП можно сформировать множество термов $\boldsymbol{BC_3} = \bigcup_{i=1}^{3} \underset{\sim}{BC}_{3i} = \{\underset{\sim}{BC}_{31}, \underset{\sim}{BC}_{32}, \underset{\sim}{BC}_{33}\} = \{\underset{\sim}{H}, \underset{\sim}{C}, \underset{\sim}{B}\}$, отображаемых нечеткими числами (НЧ) $\underset{\sim}{H}, \underset{\sim}{C}$ и $\underset{\sim}{B}$, имеющих лингвистический эквивалент «низкая» (Н), «средняя» (С) и «высокая» (В) соответственно. В дальнейшем для указанных НЧ на основе известных методов формируются необходимые функции принадлежности (ФП). Также могут быть введены и другие значения первичных термов, например, «очень низкая» (ОН), «выше среднего» (ВС), «ниже среднего» (НС) и др. Очевидно, что в этом случае характеристика BC_3 отображается набором лингвистических значений, но как частный случай, онаможет принимать четкое или интервальное значение, тогда для ее отображения будем использовать не полужирный шрифт, например, BC_3.

Определим еще одну базовую характеристику риска опасность(BC_4), которая рассматривается как величина, характеризующая опасность события нарушения ИБ, например, BC_{21} посредством BC_{12}.По аналогии с BC_3, базовая характеристика BC_4 может отображаться в четкой численной форме (например, в процентах) и обозначается как BC_4 или с помощью ЛП – «ОПАСНОСТЬ» с базовым терм-множеством

$$\boldsymbol{BC_4} = \bigcup_{i=1}^{bc_4} \underset{\sim}{BC}_{4i} \ (\underset{\sim}{BC}_{41} < \underset{\sim}{BC}_{42} < ... < \underset{\sim}{BC}_{4bc_4}). \qquad (1.5)$$

Например, при bc_4=3 можем определить

$$\boldsymbol{BC_4} = \bigcup_{i=1}^{3} \underset{\sim}{BC}_{4i} = \{\underset{\sim}{BC}_{41}, \underset{\sim}{BC}_{42}, \underset{\sim}{BC}_{43}\} = \{\underset{\sim}{H}, \underset{\sim}{C}, \underset{\sim}{B}\}$$

с соответствующими лингвистическими эквивалентами – «низкая» (Н), «средняя» (С) и «высокая» (В).

Для исследуемого выше множества толкований риска можно выделить еще такие базовые характеристики, как: частота (BC_5), которую в области ИБ можно связать с частотой реализации «угрозы», приведшей к событию нарушения ИБ. Такой компонент можно отображать численно (BC_5) или посредством ЛП – «ЧАСТОТА»:

$$\boldsymbol{BC_5} = \bigcup_{i=1}^{bc_5} \underset{\sim}{BC}_{5i} \; (\underset{\sim}{BC}_{51} < \underset{\sim}{BC}_{52} < ... < \underset{\sim}{BC}_{5bc_5}), \qquad (1.6)$$

например, если bc_5=3, то $\boldsymbol{BC_5} = \bigcup_{i=1}^{3} \underset{\sim}{BC}_{5i} = \{\underset{\sim}{BC}_{51}, \underset{\sim}{BC}_{52}, \underset{\sim}{BC}_{53}\} = \{\underset{\sim}{H}, \underset{\sim}{C}, \underset{\sim}{B}\}$,

где $\underset{\sim}{H}, \underset{\sim}{C}$ и $\underset{\sim}{B}$ имеют соответственно лингвистические эквиваленты - «низкая» (Н), «средняя» (С) и «высокая» (В).

Определим базовую характеристику затраты и потери, которую в области ИБ целесообразно определить через термин расходы (BC_6) и представить числено (BC_6), например, на заданных интервалах;

1) 0 - $100;
2) $100 - $1000;
3) $1000 - $10 000;
4) $10 000 - $100 000.

Также BC_6 можно определить с помощью ЛП «РАСХОДЫ»:

$$\boldsymbol{BC_6} = \bigcup_{i=1}^{bc_6} \underset{\sim}{BC}_{6i} \; (\underset{\sim}{BC}_{61} < \underset{\sim}{BC}_{62} < ... < \underset{\sim}{BC}_{6bc_6}), \qquad (1.7)$$

где, например, при bc_6 = 5 ЛП принимает вид

$$\boldsymbol{BC_6} = \bigcup_{i=1}^{5} \underset{\sim}{BC}_{6i} = \{\underset{\sim}{BC}_{61}, \underset{\sim}{BC}_{62}, \underset{\sim}{BC}_{63}, \underset{\sim}{BC}_{64}, \underset{\sim}{BC}_{65}\} = \{\underset{\sim}{H}, \underset{\sim}{HC}, \underset{\sim}{C}, \underset{\sim}{BC}, \underset{\sim}{B}\},$$

а лингвистическими эквивалентами используемых НЧ будут соответственно «низкие» (Н), «ниже среднего» (НС), «средние» (С), «выше среднего» (ВС) и «высокие» (В). На практике встречается и интегрированное представление BC_6, например;

1) *Negligible* (менее $100);
2) *Minor* (менее $1000);
3) *Moderate* (менее $10 000);
4) *Serious* (Существенное негативное влияние на бизнес);
5) *Critical* (Катастрофическое воздействие, возможно прекращение деятельности предприятия).

В этом случае характеристики обозначаются как BC_6/ BC_6.

Для исследуемого множества толкований риска, были выделены его базовые характеристики: риск рассматривается как измеряемая или рассчитываемая вероятность; риск связан с наступлением определенного события (как правило, не благоприятного); понятие риска раскрывается через деятельность субъекта; риск раскрывается через независящее от деятельности субъекта событие; риск воспринимается как опасность, частота, затраты и потери.

В качестве обобщения предлагается для интегрированного использования базовых характеристик риска, отображенных на сферу ИБ,

представить их в виде модели с m-компонентным базовым кортежем $< \boldsymbol{BC_1, BC_2, ..., BC_m} >$, где $m(m \leq n)$ – количество членов в кортеже. Например, при m=6 шестикомпонентный кортеж может иметь следующий вид:

$$<BC_1, BC_2, BC_3, BC_4, BC_5, BC_6>, \quad (1.8)$$

где BC_1 – действие, BC_2 – событие, BC_3 – вероятность, BC_4 – опасность, BC_5 – частота, BC_6 – затраты и потери (расходы). В результате конкретизации используемых характеристик образуется частная кортежная модель, например, для BC_{12} = «Шпионаж», BC_{22} = «НК», bc_3=3, bc_4=3, bc_5=3 и bc_6=5 она примет следующий вид:

$$<BC_{12},BC_{21},BC_3,BC_4,BC_5,BC_6>=<BC_{12},BC_{21},\bigcup_{i=1}^{3}\underset{\sim}{BC}_{3i},\bigcup_{i=1}^{3}\underset{\sim}{BC}_{4i},\bigcup_{i=1}^{3}\underset{\sim}{BC}_{5i},\bigcup_{i=1}^{5}\underset{\sim}{BC}_{6i}>.$$

Как видно, если базовые величины принимают четкие или нечеткие значения, то в частном кортеже (частной кортежной модели) они соответственно обозначаются не полужирным или полужирным шрифтом, например, BC_{12}, BC_{21} или BC_3, BC_4, BC_5, BC_6.

На основе представленной кортежной модели можно осуществлять исследование широкого спектра существующих средств анализа и оценивания риска с позиций формирования необходимых для их функционирования исходных данных, что позволит определить подходы к созданию новых систем или использованию существующих с целью эффективного решения соответствующих задач ЗИ.

2.2. Базовые характеристики, используемые в средствах анализа и оценивания рисков

На сегодняшний день существует достаточно широкое множество инструментальных САОР. Часто перед специалистами компаний для повышения эффективности решения задач ЗИ возникает вопрос о выборе соответствующей методики, которая будет удовлетворять адекватным требованиям. В п. 1.1 осуществлен анализ понятия риска, в различных предметных областях человеческой деятельности, для последующей его интерпретаций в области ИБ. Также в п. 2.1 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, проведено исследования широкого спектра существующих САОР (с использованием предложенного в п. 2.1 подхода) для определения их набора характеристик, по которым можно осуществить

сравнительный анализ таких средств. Это повысит эффективность решения задач в области ИБ.

САОР 1 -Методология NIST 800-30 (Risk Management Guide for Information Technology Systems, рекомендации NIST, разработчик –National Institute of Standards and Technology, США**)** [NIST 800].

Относительно КМР определим кортеж для этой методологии. Характеристика $ВС_1$ отображается «Действием угрозы» (таблице 1.1), которое может привести к нарушению характеристик ИБ, так напримерBC_{11} = «Проникновение в ИС на основе личных данных» может привести к BC_{21} = «НК». Для оценки УР в методологии используются базовые характеристики $ВС_3$ икосвенно $ВС_4$**,**который отображает значение параметра «Воздействие» (см. табл. 2.1). Следовательно, кортеж для методологии имеет вид:<BC_1,$ВС_2$, BC_3, $ВС_4$ >.

Таблица 2.1 - Матрица уровня риска

Вероятность Угрозы	Воздействие		
	Н (10)	*С (50)*	*В (100)*
В (1,0)	Н 10 × 1,0 = 10	С 50 × 1,0 = 50	В 100 × 1,0 = 100
С (0,5)	Н 10 × 0,5 = 5	С 50 × 0,5 = 25	С 100 × 0,5 = 50
Н (0,1)	Н 10 × 0,1 = 1	Н 50 × 0,1 = 5	Н 100 × 0,1 = 10

САОР 2 - Методика BSI-Standard100-3 (RiskAnalysisbasedon IT-Grundschutz – анализ рисков на основе IT-Grundschutz, разработана Федеральным Агентством по ИБ (FederalOfficeforInformationSecurity – BSI), Германия). [Методика BSI]**.**

Относительно КМР отметим, что все множество действий ($ВС_1$), представлено как угрозы, приводящие к нарушению ИБ, например, BC_{11}= «Отказ IT-системы», BC_{12}= «Неумышленное уничтожение актива», BC_{13}= «Потеря Ц информации» и т.д. Относительно характеристики $ВС_2$,следует отметить, что рассмотренные действия (исходя из указанного примера в. табл. 1.5) приводят к нарушению определенных характеристик ИБ и может быть косвенно связано со значением BC_{27} = «НКЦД». С учетом КМР кортеж для этой методики можем представить в виде:<BC_1, BC_2>.

САОР 3 - Методика РС БР ИББС-2.2-2009 (Рекомендации в области стандартизации Банка России, обеспечение ИБ организаций банковской системы, Российская Федерация).

Отметим, что в данном САОР угрозы отображаются как действия (BC_1)приводящие к нарушению ИБ, например (угрозы из рекомендуемого перечня в методике – Приложение 1 BC_{11}= «Сбои и отказы ПС», BC_{12}= «Ошибки в обеспечении безопасности ИС на стадиях жизненного цикла», BC_{13}= «Хищение» и т.д. Рассмотренные в примере действия ($ВС_1$) могут быть связаны с событиями ($ВС_2$) 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 $ВС_2$ в методике присутствует косвенно.

Касательно других характеристик, то при анализе риска используется степень потенциального ущерба, которую можно в КЧ шкалах косвенно отобразить посредством BC_4 (при переводе в КЛ шкалы – BC_6),а такжевероятность (BC_3) и статистические данные о частоте реализации угрозы (BC_5). После проведенного анализа с учетом КМР кортеж для этой методики следующий:<BC_1, BC_2, BC_3, BC_4, BC_5, BC_6>.

САОР 4 - Стандарт ISO/IEC 27005:2008 (Informationtechnology – Securitytechniques – Informationsecurityriskmanagement (Информационная технология – Методы защиты – Менеджмент рисков ИБ) представляет технический пересмотр стандартов, отмену и замену ISO/IEC TR 13335-3:1998 и ISO/IEC TR 13335-4:2000, Швейцария). Стандарт ISO/IEC 27005:2008

Отметим, что в ISO/IEC 27005:2008 в качестве риска рассматриваются действия, которые могут привести к нарушению ИБ, например, BC_{11}= «Воровство носителей или документов» может находится в логической связи с BC_{21}= «НК» и поэтому характеристика BC_2 в стандарте присутствует косвенно. В процессе анализа и оценки риска можно дополнительно идентифицировать компонент BC_3икосвенно – BC_4 (величина потенциальных последствий), следовательно, кортеж имеет вид:<BC_1, BC_2, BC_3, BC_4 >.

САОР 5 - Стандарт AS/NZS 4360:2004 (стандарт риск-менеджмента, Австралия и Новая Зеландия). Стандарт AS/NZS 4360:2004

Рассмотрим данный стандарт относительно КМР. Так, характеристике BC_1 соответствует действия которые могут привести к риску(что видно из таблица 1.16). Следовательно их можно представить как, например, BC_{11}= «Отказ системы» (пример взят исходя из описанных последствий в таблица 1.17), что может привести к нарушению характеристик ИБ атакованных ресурсов и может быть связано со значением BC_{25}= «НЦД». При оценивании риска определяется вероятность угроз(BC_3)и воздействие, которое можно интерпретировать как уровень опасности(BC_4).Проведенный анализ показал, что кортеж для этого стандарта имеет вид: <BC_1, BC_2,BC_3,BC_4>.

САОР 6 - Стандарт ISO/FDIS 31000 (Riskmanagement – Principlesandguidelines (Управление рисками – руководящие принципы), Швейцария).

Отметим, что относительно КМР в стандарте рассматривается событие риска, которые можно отобразить как действие (BC_1),приводящее к нарушению ИБ, например, BC_{11}= «Отказ в обслуживании веб-сервера из-за атаки хакера», BC_{12}= «Падение криптосервера из-за перегрузки», BC_{13}= «Перехват пользовательских паролей» и т.д. Эти действия могут быть соответственно связаны с событиями (BC_2) нарушения базовых характеристик ИБ BC_{23}= «НД», BC_{27}= «НКЦД», BC_{21}= «НК» и т.д., следовательно характеристики BC_1 и BC_2 в стандарте присутствуют косвенно. Характеристики, используемые в процессе анализа риска, представляются воздействием, которое можно отобразить через BC_4ивероятностью риска(BC_3). После проведенного анализа с учетом КМР кортеж для стандарта будет<BC_1,BC_2,BC_3,BC_4 >.

СОАР 7-Методика COBRA (Consultative Objective and Bi-Functional Risk Analysis, разработчик – C & A Systems Security Ltd**,** Великобритания).

Относительно базовых характеристик риска (см. п. 2.1) для методики COBRA можно получить отображения таких составляющих: BC_1, BC_2. Так, компоненту 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».

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 п. 2.1) уровень риска можно отобразить через компонент BC_3.

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 $\boldsymbol{BC_{1НСБ}} = \{BC_{1НСБ1}, BC_{1НСБ2}, ..., BC_{1НСБbc_1}\}$, где $BC_{1НСБ1}$ = «Кража» (bc_1 – количество идентификаторов угроз для категории НСБ).

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 косвенных характеристик в кортеже будет использоваться символ *, т.е. BC_2. После проведенного анализа с учетом КМР п. 2.1 кортеж для этой методики можем представить в виде <BC_1, BC_2,BC_3>.

СОАР 8- Метод CRAMM (CCTA Risk Analysisand Management Method, разработчик –Центральное агентство по компьютерам и телекоммуникациям (CCTA – Central Computerand Telecommunications Agency), Великобритания**).**

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 п. 2.1 здесь можно выделить компоненты BC_5 и BC_3.

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)».

После проведенного анализа с учетом п. 2.1 составим КМР для данного метода: <BC_1, $\boldsymbol{BC_2^*}$,BC_3, BC_5, BC_6>.

САОР 9 - Система RiskWatch (разработчик – компания RiskWatch, США).

Относительно КМР с учетом п. 2.1 для RiskWatch определим кортеж. Так компонентуBC_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 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 компонентBC_5,а риском являются ожидаемые потери за год, которые также можно интерпретировать как расходы(BC_6).С учетом КМР, кортеж для этой методики можно представить в виде <BC_1, BC_2, BC_5, BC_6>.

САОР 10 - Инструментарий RA2 artofrisk (RA SoftwareTool, разработчик –компании AEXIS SecurityConsultants и XiSECConsultantsLtd., Великобритания).

Относительно КМР определим значения BC_1, BC_2. Все действия (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 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 BC_1 можно представить множеством $\boldsymbol{BC_{1ДТЛ}} \in \{BC_{1ДТЛi}\}\, i=\overline{1,bc_1}$, где, например, $BC_{1ДТЛ1}$= «Кража». Относительно компонентаBC_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 BC_2 в ПО присутствует косвенно. В методике присутствуют характеристики BC_4(уровни опасности) иBC_3(вероятность риска), следовательно, риск отображается как опасность (BC_4) для организации (при наступлении рисковой ситуации). С учетом КМР кортеж для этой методики можем представить в виде:<BC_1, BC_2, BC_3, BC_4>.

САОР 11 - Система КЭС управления ИБ «АванГард» **(**Комплексная экспертная система «АванГард», разработчик – Лаборатория системного анализа проблем информатизации Института системного анализа РАН, Россия).

Отметим, что относительно КМР в КЭС рассматривается событие риска, отображаемое как действие (BC_1), которое приводит к нарушению ИБ,

например, $ВС_{11}$= «Отказ обслуживания веб-сервера из-за атаки хакера», $ВС_{12}$= «Падение крипто сервера из-за перегрузки», $ВС_{13}$= «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 Казахстане) 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 ($ВС_1$) могут быть связаны с событиями ($ВС_2$) нарушения базовых характеристик ИБ, например, $ВС_{11}$ с $ВС_{23}$= «НД», $ВС_{12}$ с $ВС_{27}$= «НКЦД», а $ВС_{13}$ с $ВС_{21}$= «НК» и т.д., следовательно, характеристика $ВС_2$ в системе присутствует косвенно. Касательно других компонент, которые используются в процессе анализа риска, присутствуют степень опасности ($ВС_4$)ивероятность события риска($ВС_3$). Так же используется показатель ущерба, которыйотображается посредством$ВС_6$. 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 $ВС_6$ которая всистеме присутствуют косвенно.После проведенного анализа с учетом КМР кортеж для КЭС будет<$ВС_1$, $ВС_2$, $ВС_3$, $ВС_4$, $ВС_5$ >.

СОАР 12 - Система EnterpriseRiskAssessor(RiskAdvisor, разработчик–компания Methodware,Новая Зеландия).

При КМР для данного ПО, можно получить отображение базовых характеристик $ВС_1$, $ВС_2$, $ВС_3$, $ВС_4$и $ВС_6$.В EnterpriseRiskAssessor в качестве риска рассматриваются действия, которые могут привести к нарушению ИБ, например, $ВС_{11}$= «Кража документов» может находится в логической связи с $ВС_{21}$= «НК» и поэтому характеристика $ВС_2$ в ПО присутствует косвенно. В процессе анализа риска можно дополнительно идентифицировать базовые характеристики в явном виде $ВС_3$икосвенном $ВС_6$ (consequence – следствие, которое можно представить в виде $ВС_6$), а во время его оценки – устанавливается коэффициент значимости и уровень опасности ($ВС_4$), следовательно, кортеж имеет вид:<$ВС_1$,$ВС_2$,$ВС_3$, $ВС_4$,$ВС_6$ >.

САОР 13 - Система vsRisk, RiskAssessmentTool (разработчик –компания VigilantSoftwareLtd., Великобритания).

В качестве исходных данных на этапе анализа риска служит $ВС_1$ и, например, согласно рисунок. 1.10 он может принимать значение BC_{13}= «Отказ в обслуживании», что приводит к BC_{23}= «НД» (рисунок 1.11).

Система предоставляет средства для оценки всех факторов рисков, включая угрозы, уязвимости, активы и механизмы контроля и не содержит средств для количественной оценки величины риска, ограничиваясь только качественными шкалами. Отметим, что для оценки задаются масштабы вероятности($\boldsymbol{BC_3}$)и воздействия рассматриваемых угроз, которое можно косвенно, отобразить через уровни $\boldsymbol{BC_4^*}$. Все изменения, вносимые в базу данных продукта по ходу работы, подробным образом фиксируются в журнале аудита.

Отметим, что с учетом КМР кортеж для этого ПО следующий:<BC_1, $ВС_2$ BC_3, $ВС_4$ >.

САОР 14 - Методология Mehari (разработчик Clusif, Франция).

В рассмотренном примере запроса «Существует ли система регулирования электропитания …» действия, например, можно представить как параметр $ВС_{11}$= «Отказ оборудования», $ВС_{12}$= «Сбой в приложений» и т.д., которые могут привести к $ВС_{23}$ = «НД».Риск рассматривается как воздействие, которое можно интерпретировать уровнем опасности ($ВС_4$). Отметим, чтокортеждляMehariследующий:<$ВС_1$, $ВС_2$, $ВС_4$, >.

САОР 15 -Методика MAGERIT (Methodology for Information Systems Risk Analysis and Management, разработчикMinisterio De AdministracionesPúblicas, Испания).

Относительно КМР отметим, что в рассмотренном примере (см. табл. 1.24) угрозы можно интерпретировать как характеристику $ВС_1$, например, $ВС_{11}$= «Несанкционированный доступ». Это действие может привести к событию $ВС_{21}$= «НК». В процессе оценивания также используются характеристики $ВС_5$, $ВС_6$, $ВС_4$ и $ВС_3$. Следовательно, общая запись кортежа для MAGERIT:<$ВС_1$, $ВС_2$, $ВС_3$, $ВС_4$, $ВС_5$, $ВС_6$>.

САОР 16 -Методика Information Security RA (Risk Assessment, разработчик Centers for Medicare & Medicaid Services (CMS), США).

Рассмотрим данную методику относительно КМР. Так, характеристике $ВС_1$ соответствует все угрозы которые определяются в фазе 2. Они могут привести к нарушению базовых характеристик ИБ и следовательно, может быть связано со значениями $ВС_2$. Анализ показал, что прямого использования его в методике нет, но прослеживается с ним логическая связь, следовательно присутствует косвенно. При оценке риска определяется вероятность угроз ($ВС_3$) и воздействие, которое можно отобразить характеристикой $\boldsymbol{BC_4^*}$.Исследования показали, что кортеж для этой системы имеет вид: <$ВС_1$,$ВС_2$, $ВС_3$,$ВС_4$ >.

Таким образом, в работе с учетом предложенного в п. 2.1 подхода, проведено исследование широкого спектра САОР в виде соответствующего ПО и определен набор базовых характеристик (таблице. 2.2), по которым можно осуществить сравнительный анализ соответствующих средств

оценивания и выбрать наиболее подходящие для решения определенного класса задач ЗИ. Как видно только две системы ИББС-2.2-2009 и MAGERIT отображают более полный набор параметров риска, что расширяет возможности специалиста при осуществлении оценивания риска.

Таблица 2.2 - Результаты исследования САОР

САОР	$ВС_1$	$ВС_2$	$ВС_3$	$ВС_4$	$ВС_5$	$ВС_6$
1	+	+*	+	+	-	-
2	+	+	-	-	-	-
3	+	+*	+	+	+	+
4	+	+*	+	+	-	-
5	+	+*	+	+*	-	-
6	+*	+*	+	+*	-	-
7	+	+*	+	-	-	-
8	+	+*	+	-	+	+
9	+	+*	-	-	+	+
10	+	+*	+	+	-	-
11	+	+*	+	+	-	+*
12	+	+*	+	+	-	+*
13	+	+*	+	+*	-	-
14	+	+*	-	+	-	-
15	+	+	+	-	-	+
16	+	+	+	+*	-	+*
17	+	+*	+	-	-	+*
18	+	+*	+	+	-	+
19	+	+*	-	+	-	-
20	+	+	+	+*	-	+
21	+	+*	+	+	-	+
22	+	+	+	+*	-	-
23	+	+*	+	-	-	+
24	+	+*	+	+*	+	-
25	+*	+*	-	+*	-	-
26	+	+*	+	+	+	+
27	+	+*	+	+*	-	-

2.3 Метод FirstM оценивания рисков для систем управления информационной безопасностью

Согласно рекомендациям стандарта ISO/IEC 27001 для обеспечения ИБ на предприятии любой формы собственности необходимо внедрять систему менеджмента информационной безопасности. Основой такого стандарта

является менеджмент рисков ИБ, под которым подразумевается анализ, оценивание и обработка рисков ИБ.

В работе предложена кортежная модель базовых характеристик риска (п. 2.1), а также исследован широкий спектр САОР (п. 2.2) с определением их базовых характеристик, которые в дальнейшем можно использовать для анализа и сравнения соответствующих средств. Такое исследование показало, что в основном для анализа и оценивания рисков используются статистические данные об инцидентах и угрозах ИБ. Во многих странах (в том числе и в Казахстане) на государственном уровне подобная статистика не ведется, что ограничивает возможности существующих средств для национального использования. Также следует отметить, что исследуемый инструментарий устанавливает эксперту определенные ограничения (на используемый набор параметров) и не дает ему возможности применения для оценивания более широкого спектра величин.

В связи с этим, целью является разработка методов анализа и оценивания рисков, позволяющих использовать широкий спектр базовых характеристик, дающих возможность создавать более гибкие средства оценивания, а также определять риски, как на основе статистических данных, так и на экспертных оценках, сделанных в неопределенной, слабо формализованной среде, с учетом периода времени, отрасли, экономической и управленческой специфики предприятия и др. Кроме этого, разрабатываемые методы дадут возможность отражать результаты, как в числовой, так и в словесной форме, например, с использованием ЛП, часто применяемой для описания сложных систем, описываемых параметрами, представленными не только в количественном, но и в качественном виде. При этом ЛП позволяют поставить в соответствие качественным значениям определенный количественный эквивалент. Для решения поставленной задачи предлагается использовать подход, основанный на суждениях экспертов. При этом будем учитывать первую ситуацию, когда эксперт имеет четкие (бинарные) предпочтения относительно значений оцениваемых параметров, так и вторую ситуацию – с зоной неуверенности, когда эксперт сомневается в однозначности своих приоритетов. В соответствие с этим предлагается два метода оценивания – для детерминированной (FirstM).

Метод FirstM

Этап 1 - Определение множеств. На этом этапе определяются все используемые базовые множества параметров, которые будут задействованы в процессе анализа и оценивания рисков. Для определения множеств в качестве основы используем кортежную модель базовых характеристик риска (п. 2.1): $\boldsymbol{BC_1} = \bigcup_{i=1}^{bc_1} BC_{1i}$ – действие, которое может привести к BC_2 (например, для bc_1=5 эксперты могут идентифицировать, следующие

$\boldsymbol{BC_1} = \bigcup_{i=1}^{5} BC_{1i} = \{BC_{11}, BC_{12}, BC_{13}, BC_{14}, BC_{15}\}$={«Заражение вирусами», «Ошибки программирования», «Нарушение работы операционной системы», «Нарушение целостности системы безопасности», «Отказ в обслуживании»});

$\boldsymbol{BC_2} = \bigcup_{i=1}^{7} BC_{2i}$ – событие нарушения ИБ (например, BC_2 может отражаться значением BC_{27}= «НКЦД»).

Для отображения общего результата оценивания риска воспользуемся ЛП «УРОВЕНЬ РИСКА» (LR), которая определяется кортежем [29]<LR, $\underset{\sim}{T}_{LR}$, X_{LR}>, где базовые терм-множества задаются m термами $\underset{\sim}{\boldsymbol{T}}_{LR} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{LR_j}$ (например, для m=5 – $\bigcup_{j=1}^{5} \underset{\sim}{T}_{LR_j}$ = {«Уровень риска нарушения ИБ очень низкий» (НР), «Уровень риска нарушения ИБ низкий» (РН), «Уровень риска нарушения ИБ средний» (РС), «Уровень риска нарушения ИБ высокий» (РВ), «Уровень риск нарушения ИБ очень высокий» (ОР)}, которые могут быть отображены на универсальное множество $X_{LR} \in \{0, max_{LR}\}$). Для каждого из термов $\underset{\sim}{T}_{LR_1}, \ldots, \underset{\sim}{T}_{LR_j}, \ldots, \underset{\sim}{T}_{LR_m}$ задается свой интервал значений $[lr_{min}; lr_1[, \ldots, [lr_j; lr_{j+1}[, \ldots, [lr_m; lr_{max}]$ (например, при m=5 для $\underset{\sim}{T}_{LR_1}$, $\underset{\sim}{T}_{LR_2}$, $\underset{\sim}{T}_{LR_3}$, $\underset{\sim}{T}_{LR_4}$, $\underset{\sim}{T}_{LR_5}$ определим интервалы с использованием шкалы Харрингтона [26], которую модифицируем увеличением ее градуированных значений в два порядка, т.е. $[lr_{min}; lr_1[$, $[lr_2; lr_3[$, $[lr_4; lr_5[$, $[lr_6; lr_7[$, $[lr_8; lr_{max}]$ будут соответствовать следующим значениям – ([0; 20[, [20; 40[, [40; 60[, [60; 80[, [80; 100]). Далее, для создания возможности эксперту при оценивании использовать более широкий спектр величин, воспользуемся вышеуказанной моделью базовых характеристик риска и зададим множество таких характеристик $EC_{Fh} \in \{EC_i\}$={BC_3, BC_4, BC_5, BC_6} ($i = \overline{1,g}$), где Fh – шестнадцатеричный код, бинарное значение которого следующим образом отражает порядковый номер характеристики в множестве: BC_3 располагается в разряде 2^3, BC_4 в 2^2, BC_5 – 2^1, BC_6 – 2^0 (например, если эксперты хотят воспользоваться BC_3, BC_4 и BC_6 то g=3 ($i = \overline{1,3}$), а $EC_{Dh} \in \{EC_i\}$={EC_1, EC_2, EC_3}={BC_3, BC_4, BC_6}).

Введем ЛП «УРОВЕНЬ EC_i» (C_{EC_i}), которая определяется кортежем <C_{EC_i}, $\underset{\sim}{T}_{C_{EC_i}}$, X_{EC_i}>, где базовые терм-множества задаются m термами $\underset{\sim}{\boldsymbol{T}}_{C_{EC_i}} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{C_{EC_i}j}$ (например, при m=5– $\bigcup_{j=1}^{5} \underset{\sim}{T}_{C_{EC_i}j}$ = {«очень низкий» (ОН),

«низкий» (Н), «средний» (С), «высокий» (В), «очень высокий» (ОВ)}, которые в лингвистической форме характеризуют уровень характеристики и могут быть отображены на универсальное множество $X_{EC_i} \in \{0, \max_{C_{EC_i}}\}$). Для $\underset{\sim}{T}_{C_{EC_i 1}}$,…, $\underset{\sim}{T}_{C_{EC_i j}}$,…, $\underset{\sim}{T}_{C_{EC_i m}}$ соответственно задается свой интервал значений для каждого EC_i – $[c_{EC_i \min}; c_{EC_i 1}[$, …, $[c_{EC_i j}; c_{EC_i j+1}[$,…, $[c_{EC_i m}; c_{EC_i \max}]$ (например, при m=5 для термов $\underset{\sim}{T}_{C_{EC_3 1}}$, $\underset{\sim}{T}_{C_{EC_3 2}}$, $\underset{\sim}{T}_{C_{EC_3 3}}$, $\underset{\sim}{T}_{C_{EC_3 4}}$, $\underset{\sim}{T}_{C_{EC_3 5}}$ базовой характеристики EC_3={BC_6}, осуществим разбиения значения на интервалы - $[c_{EC_3 \min}; c_{EC_3 1}[$, $[c_{EC_3 2}; c_{EC_3 3}[$, $[c_{EC_3 4}; c_{EC_3 5}[$, $[c_{EC_3 6}; c_{EC_3 7}[$, $[c_{EC_3 8}; c_{EC_3 \max}]$, которым будут соответствовать значения ([0; 0,1[, [0,1; 0,2[, [0,2; 0,3[, [0,3; 0,4[, [0,4; 0,5]). Для удобства отображения базовых характеристик через интервалы допустимых значений воспользуемся табл. 2.3. Оценка значимости EC_iосуществляется параметрами из множества $\boldsymbol{LS} \in \{LS_i\}\ (i = \overline{1, g})$, а оценка текущего значения оценочного компонента – с помощью множества $\boldsymbol{ec} \in \{ec_i\}\ (i = \overline{1, g})$.

Таблица 2.3 - Отображение значений базовых характеристик

EC_i	Интервалы значений C_{EC_i} для $\underset{\sim}{T}_{C_{EC_i 1}} - \underset{\sim}{T}_{C_{EC_i m}}$				
	$\underset{\sim}{T}_{C_{EC_i 1}}$	…	$\underset{\sim}{T}_{C_{EC_i j}}$	…	$\underset{\sim}{T}_{C_{EC_i m}}$
EC_1	$[c_{EC_1 \min}; c_{EC_1 1}[$	…	$[c_{EC_1 j}; c_{EC_1 j+1}[$	…	$[c_{EC_1 m}; c_{EC_1 \max}]$
…	…	…	…	…	…
EC_i	$[c_{EC_i \min}; c_{EC_i 1}[$	…	$[c_{EC_i j}; c_{EC_i j+1}[$	…	$[c_{EC_i m}; c_{EC_i \max}]$
…	…	…	…	…	…
EC_g	$[c_{EC_g \min}; c_{EC_g 1}[$	…	$[c_{EC_g j}; c_{EC_g j+1}[$	…	$[c_{EC_g m}; c_{EC_g \max}]$

Этап 2 - Описание базовых характеристик. На этом этапе производится описание набора используемых базовых характеристик, которые, по мнению эксперта-аналитика, с одной стороны, влияют на оценивание рисков ИБ, а, с другой – оценивают его различные по природе стороны, например, учитывающие особенности организации (банк, архив, силовые ведомства, завод и д.р.). Для этого эксперт должен определить шестнадцатеричный код, по которому из {EC_i} выбираются значения соответствующих компонент, например, при коде *Dh* – g=3, а $EC_{Dh} \in \{EC_i\}$={EC_1, EC_2, EC_3}={BC_3, BC_4, BC_6} ($i = \overline{1, 3}$) или при коде *Fh* – *g*=4, а $EC_{Fh} \in \{EC_i\}$={EC_1, EC_2, EC_3,EC_4}={BC_3, BC_4, BC_5, BC_6} ($i = \overline{1, 4}$).

Этап 3 - Оценка уровня значимости базовых характеристик. На этом этапе каждому компоненту – EC_i ставиться в соответствие уровень его значимости – LS_i. Отметим, что если для всех LS справедливо отношение порядка

$$LS_i \geq LS_{i+1}, \quad (2.1)$$

то значимость i-гокомпонента определяется по правилу Фишберна:

$$LS_i = \frac{2(g-i+1)}{(g-1)g}. \quad (2.2)$$

Согласно этому правилу у эксперта отсутствует информация (кроме условия (2.1)) о значимости компонента и тогда (2.2) отображает максимум энтропии наличной информационной неопределенности об объекте исследования. Если же все компоненты обладают равной значимостью (равнопредпочтительны т.е. $LS_i = LS_{i+1}$ или системы предпочтений нет), то:

$$LS_i = 1/g. \quad (2.3)$$

Этап 4 - Определение эталонных значений уровня риска. На этом этапе экспертами определяются эталонные значения для LR, т.е. задается количество термов в базовом терм-множестве ЛП и ставиться им в соответствие свой интервал значений, лежащий в диапазоне $[lr_{min};lr_{max}]$ (см. пример на этапе 1).

Этап 5 - Определение эталонных значений базовых характеристик. Здесь экспертами производится определение эталонных значений для C_{EC_i}, т.е. задается количество термов в терм-множестве ЛП (см. пример на этапе 2.3 и таблице. 2.4).

Таблица 2.4 - Пример определения эталонных значений базовых компонент

EC_i	Интервалы значений C_{EC_i} для $T_{\sim C_{EC_i 1}} - T_{\sim C_{EC_i 5}}$				
	$T_{\sim C_{EC_i 1}}$	$T_{\sim C_{EC_i 2}}$	$T_{\sim C_{EC_i 3}}$	$T_{\sim C_{EC_i 4}}$	$T_{\sim C_{EC_i 5}}$
EC_1= BC_3	$T_{\sim C_{BC_3 1}} \in$ [0; 20[	[20; 40[	[40; 60[	[60; 80[	$T_{\sim C_{BC_3 5}} \in$ [80; 100]
EC_2= BC_4	$T_{\sim C_{BC_4 1}} \in$ [0; 2[	[2; 4[	[4; 6[	[6; 8[	$T_{\sim C_{BC_4 5}} \in$ [8; 10]
EC_3= BC_5	$T_{\sim C_{BC_5 1}} \in$ [0;0,2[	[0,2; 0,4[	[0,4; 0,6[	[0,6; 0,8[	$T_{\sim C_{BC_5 5}} \in$ [0,8; 1]
EC_4= BC_6	$T_{\sim C_{BC_6 1}} \in$ [0; 0,1[	[0,1; 0,2[	[0,2; 0,3[	[0,3; 0,4[	$T_{\sim C_{BC_6 5}} \in$ [0,4; 0,5]

Этап 6 - Оценка текущих значений характеристик. На этом этапе по каждой базовой характеристике $\{EC_i\}=\{BC_3,BC_4, BC_5, BC_6\}$ ($i=\overline{1,g}$) эксперты соответствующей предметной области определяют ес для всех BC_1при

($bc_1 = \overline{1,n}$)т.е. $\{ec_i^{BC_{1bc_1}}\}=\{ec_{BC_3}^{BC_{1bc_1}}, ec_{BC_4}^{BC_{1bc_1}}, ec_{BC_5}^{BC_{1bc_1}}, ec_{BC_6}^{BC_{1bc_1}}\}$. Значения выставляются на основании предпочтений экспертов, статистической информации и др. данных. В табл. 2.5 показан пример определения текущих значений для $\boldsymbol{BC_1} = \bigcup_{i=1}^{5} BC_{1i}$, описанных на этапе 1 при g=4, а $EC_{Fh} \in \{EC_i\}=\{BC_3, BC_4, BC_5, BC_6\}$ ($i = \overline{1,4}$).

Таблица 2.5 Пример 1 – определение текущих значений базовых характеристик

EC_i	$ec_i^{BC_{11}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{12}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{13}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{14}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{15}}$	$\underset{\sim}{T}_{C_{EC_i}}$
BC_3,(i=1)	72	В	58	С	64	С	70	В	66	С
BC_4,(i=2)	5,4	С	6	С	2,2	ОН	9	ОВ	5,5	С
BC_5,(i=3)	0,72	В	0,58	С	0,64	С	0,7	В	0,66	С
BC_6,(i=4)	0,23	С	0,33	С	0,12	Н	0,4	В	0,24	Н

Этап 7 - Классификация текущих значений. При прохождении этого шага определяется принадлежность $ec_i^{BC_{1bc_1}}$ заданному диапазону, по которому формируется бинарное значение λ:

$$\lambda_{ij}^{(BC_{1bc_1})} = \begin{cases} 1, \textit{при } ec_i^{BC_{1bc_1}} \in [\, c_{EC_i(j-1)}; c_{EC_i j}[\\ 0, \textit{при } ec_i^{BC_{1bc_1}} \notin [\, c_{EC_i(j-1)}; c_{EC_i j}[\end{cases}, \qquad (2.4)$$

отражающее предпочтение эксперта относительно значений оценочных параметров, а результаты вычислений для удобства заносятся в табл. 2.6.

Таблица 2.6 - Классификация текущих значений базовых характеристик

EC_i	$\lambda_{ij}^{(BC_{1bc_1})}$ для $\underset{\sim}{T}_{C_{EC_i j}}$ ($i = \overline{1,g}$, $j = \overline{1,m}$)				
	$\underset{\sim}{T}_{C_{EC_i 1}}$	…	$\underset{\sim}{T}_{C_{EC_i j}}$	…	$\underset{\sim}{T}_{C_{EC_i m}}$
EC_1	λ_{11}	…	λ_{1j}	…	λ_{1m}
…	…	…	…	…	…
EC_i	λ_{i1}	…	λ_{ij}	…	λ_{im}
…	…	…	…	…	…
EC_g	λ_{g1}	…	λ_{gj}	…	λ_{gm}

Аналогичные преобразования производятся для всех BC_1, например, для тех, которые определенны на этапе 1. Все вычисленные значения $\lambda_{ij}^{(BC_{11})}, \lambda_{ij}^{(BC_{12})} \ldots \lambda_{ij}^{(BC_{15})}$ занесем в табл. 2.7.

Этап 8 - Оценка уровня риска. На этом этапе производится вычисление показателя уровня риска нарушения ИБ $lr^{(BC_{1bc_1})}$ по формуле:

$$lr^{(BC_{1bc_1})} = \sum_{j=1}^{m}\left(lr_j \sum_{i=1}^{g} LS_i \lambda_{ij}^{(BC_{1bc_1})} \right), \qquad (2.5)$$

где lr_j=90-20(j-1) $\lambda_{ij}^{(BC_{1bc_1})}$ определяется по формуле (2.4) для каждой BC_{1bc_1} $(bc_1 = \overline{1,n})$, а $LS_i (i = \overline{1,g})$ – по формуле (2.2) или (2.3) $(j = \overline{1,m})$.

Таблица 2.7 - Пример 1 – классификация текущих значений характеристик

EC_i	Значение λ для $BC_1 \in \{BC_{1bc_1}\}$ $(bc_1 = \overline{1,5})$																									
	$\lambda_{ij}^{(BC_{11})}$ для $\underset{\sim}{T}_{C_{EC_i m}}$ $(i = \overline{1,4},$ $j = \overline{1,5})$					$\lambda_{ij}^{(BC_{12})}$ для $\underset{\sim}{T}_{C_{EC_i m}}$ $(i = \overline{1,4},$ $j = \overline{1,5})$					$\lambda_{ij}^{(BC_{13})}$ для $\underset{\sim}{T}_{C_{EC_i m}}$ $(i = \overline{1,4},$ $j = \overline{1,5})$					$\lambda_{ij}^{(BC_{14})}$ для $\underset{\sim}{T}_{C_{EC_i m}}$ $(i = \overline{1,4},$ $j = \overline{1,5})$					$\lambda_{ij}^{(BC_{15})}$ для $\underset{\sim}{T}_{C_{EC_i m}}$ $(i = \overline{1,4},$ $j = \overline{1,5})$				
BC3	0	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0
BC4	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0
BC5	0	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0
BC6	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0

Этап 9 - Лингвистическое распознавание. На завершающем этапе осуществляется лингвистическое распознавание полученного значения $lr^{(BC_{1bc_1})}$ посредством терм-множеств LR, например, по формуле (2.6) при m=5:

$$\underset{\sim}{T}_{LR} = \begin{cases} HP, \text{ при } lr^{(BC_{1bc_1})} \in [\, lr_{\min}; lr_1[\\ PH, \text{ при } lr^{(BC_{1bc_1})} \in [\, lr_2; lr_3[\\ PC, \text{ при } lr^{(BC_{1bc_1})} \in [\, lr_4; lr_5[\\ PB, \text{ при } lr^{(BC_{1bc_1})} \in [\, lr_6; lr_7[\\ OP, \text{ при } lr^{(BC_{1bc_1})} \in [lr_8; lr_{\max}] \end{cases}, \qquad (2.6)$$

где LR отображает вычисленное $lr^{(BC_{1bc_1})}$ с помощью значений терм-множеств ЛП «УРОВЕНЬ РИСКА». Также по выражению (2.7) можно вычислить среднее значение $lr^{(cp)}$ по оцениваемому ресурсу:

$$lr^{(cp)} = (\sum_{bc_1=1}^{m} lr^{(BC_{1bc_1})}) / m. \qquad (2.7)$$

Рассмотрим пример анализа и оценивания риска на основе использования такого ресурса (актива) информационной системы, как почтовый сервер, воспользовавшись при этом примером для параметров BC_1 и BC_2, определенных на этапе 1. Их идентификацию наиболее часто осуществляют на основе суждений экспертов или с помощью запросов, посредством составленных экспертами опросников. Приведем пример запросов в соответствие со стандартом ISO/IEC 27002:

1) Существует ли в организации определенная, внедренная и утвержденная процедура получения разрешения относительно использования новых средств обработки информации? (пункт 6.1.4 стандарта). Для ответа на данный запрос предлагается выбрать ответ ДА или НЕТ. Если эксперт отвечает ДА, тогда происходит уточнение, как эта процедура организована на предприятии.

1.1 Одобрены ли новые средства обработки информации со стороны:

а) руководства пользователей; если ответ ДА – переход к следующему, если НЕТ – могут быть реализованы все BC_{1bc_1} $(bc_1 = \overline{1,5})$;

б) администраторов средств управления; если ответ ДА – переход к следующему, если НЕТ – могут быть реализованы BC_{13}- BC_{15};

в) менеджером локальной информационной системы. Если эксперт ответил ДА – переход к следующему, если НЕТ – могут быть реализованы BC_{12}- BC_{15};

1.2 Проверена ли совместимость с другими компонентами системы? Если ДА – переход к следующему, если НЕТ – могут быть реализованы BC_{13}- BC_{15};

1.3 Используются ли средства обработки информации личной или частной собственности: портативные компьютеры, домашние компьютеры или приборы, для обработки деловой информации и определены, внедрены ли необходимые меры контроля? Если ответ ДА – переход к следующему, если НЕТ – могут быть реализованы все BC_{1bc_1}.

В случае если экспертом был дан ответ НЕТ на запрос 1 то это может привести к BC_{17} и ко всем BC_1.

Проведём опрос по данному запросу и обработаем варианты ответов. Предположим, что на запрос 1 эксперт дал положительный ответ, следовательно, перешел к уточнению данных, на что дал следующие ответы: 1.1а – ДА; 1.1б – ДА; 1.1в – НЕТ; 1.2 ДА; 1.3 НЕТ.

Этап 1. Произведем обработку ответов и определение базовых характеристик. И так, относительно данного актива могут быть направлены все $BC_{1bc_1}.(bc_1=\overline{1,n})$, при реализации которых возможно наступления определенных BC_1, что описывается связками: BC_{11} => BC_{25}= «НЦД»; BC_{12} =>BC_{27}= «НКЦД»; BC_{13} =>BC_{25}= «НЦД»; BC_{14} =>BC_{27}= «НКЦД»; BC_{15} =>BC_{23}= «НД» (например, последняя связка интерпретируется так: относительно почтового сервера может быть реализовано действие (реализация потенциальных угроз) приводящее к отказу в обслуживании и инициирующее событие нарушения доступности ресурса). Таким образом, множество BC_2 для данного актива, отображается как $BC_2=\{BC_{23}, BC_{25}, BC_{27}\}$. При оценки степени риска используем соответствующую ЛП с терм-множеством и интервалами значений, которые в качестве примера, рассмотрены на этапе 1.

Этап 2. Воспользуемся базовыми характеристиками определенными в примере этапа 1 при g=4, $EC_{Fh}\in\{EC_i\}=\{EC_1$ – вероятность (BC_3), EC_2 – опасность (BC_4), EC_3 – частота (BC_5), EC_4 – расходы (BC_6)$\}$, $(i=\overline{1,g})$.

Этап 3. Оценку LS осуществим по формуле (2.3) $LS_i=1/g=$ 0,25 $(i=\overline{1,4})$.

Этап 4. Для определения эталонных значений уровня риска воспользуемся примером, описанным на этапе 1 где $[lr_{min};lr_{max}]$ соответствует [0; 100].

Этап 5. На основе предварительного экспертного анализа получаем эталонные значения C_{EC_i} с заданными интервалами. Для этого воспользуемся данными из примера этапа 1 и таблица. 2.4, где разбиение на интервалы компонента BC_5 основывается на шкале Харрингтона, а BC_3– на ее модификации путем увеличения в два порядка градуированных значений. Диапазон значений BC_4 и BC_6 определяется по усмотрению экспертов.

Этап 6. Текущее состояние ИБ актива характеризуется значениями базовых характеристик *ec* по каждому BC_1 (таблица. 2.5), которые определяются на основе экспертных суждений. Для осуществления дальнейших расчетов будут использоваться данные из табл. 2.6.

Этап 7. Для каждого BC_{1bc_1} $(bc_1=\overline{1,5})$ на основании выражения (2.4) относительно заданных диапазонов (см. табл. 2.4) осуществляется классификация текущих значений $ec_i^{BC_{1bc_1}}$ (см. таблица. 2.6) с помощью бинарной переменной $\lambda_{ij}^{(BC_{1bc_1})}$, конкретные значения которой занесены в таблица. 2.7.

Этап 8. Произведем вычисления показателя уровня риска нарушения ИБ по формуле (2.5), где m = 5, $j=\overline{1,5}$, $i=\overline{1,4}$, $bc_1=\overline{1,5}$, lr_1=10, lr_2=30, lr_3=50, lr_4=70, lr_5=90, тогда $lr^{(BC_{11})}$=0+35+25+0+0=60, $lr^{(BC_{12})}$=60, $lr^{(BC_{13})}$=50, $lr^{(BC_{14})}$=80, $lr^{(BC_{15})}$=50.

Этап 9. Для лингвистического распознавания полученного значения $lr^{(BC_{1bc_1})}$ воспользуемся формулой (2.6), где $[lr_{min};lr_{max}]$ соответствует [0; 100], а

$$\underset{\sim}{T}_{LR} = \begin{cases} HP, \text{ при } lr^{(BC_{1bc_1})} \in [0;20[\\ PH, \text{ при } lr^{(BC_{1bc_1})} \in [20;40[\\ PC, \text{ при } lr^{(BC_{1bc_1})} \in [40;60[\\ PB, \text{ при } lr^{(BC_{1bc_1})} \in [60;80[\\ OP, \text{ при } lr^{(BC_{1bc_1})} \in [80;100] \end{cases} . \quad (2.8)$$

Тогда показателям $lr^{(BC_{11})}, lr^{(BC_{12})}$, $lr^{(BC_{13})}$, $lr^{(BC_{14})}, lr^{(BC_{15})}$ соответственно определенны значения ЛП: «РВ», «РВ», «РС», «ОР», «РС».

Также для данного актива по выражению (2.7) вычисляется среднее значение уровня риска $lr^{(cp)} = (\sum_{bc_1=1}^{5} lr^{(BC_{1bc_1})}) / 5$=(60+60+50+80+50)/5=60 и далее, по формуле (2.6) определяется его лингвистический эквивалент – «РВ».

В целях верификации метода выполним аналогичные вычисления при среде окружения заданного ресурса с повышенным уровнем риска, то есть экспертами было оценено текущее значения $ec_i^{BC_{1bc_1}}$ для всех BC_{1bc_1} на уровне $\underset{\sim}{T}_{C_{EC_i 4}}$={«В»} и $\underset{\sim}{T}_{C_{EC_i 5}}$={«ОВ»} (см. пример этапа 1). Результаты вычислений (по аналогии с табл. 2.5) занесем в таблице. 2.8.

Таблица 2.8 - Пример 2 - определение текущих значений базовых характеристик

EC_i		$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{12}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{13}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{14}}$	$\underset{\sim}{T}_{C_{EC_i}}$	$ec_i^{BC_{15}}$	$\underset{\sim}{T}_{C_{EC_i}}$
BC_3, (i=1)	0	В	9	В	5	ОВ	6	ОВ	1	В
BC_4, (i=4)	4	В		ОВ		В	3	ОВ	9	ОВ
BC_5, (i=2)	92	ОВ	83	В	9	ОВ	61	В	2	В
BC_6, (i=3)	44	ОВ	39	В	45	ОВ	48	В	43	ОВ

Далее проводится классификация текущих значений $ec_i^{BC_{1bc_1}}$ по формуле (2.4), а результаты заносятся в таблице 2.9.

Таблица 2.9 - Пример 2 – классификация текущих значений характеристик

	Значение λ для $BC_1 \in \{BC_{1bc_1}\}$ $(bc_1 = \overline{1,5})$

C_i	$\lambda_{ij}^{(BC_{11})}$ Для $\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$					$\lambda_{ij}^{(BC_{12})}$ Для $\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$					$\lambda_{ij}^{(BC_{13})}$ Для $\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$					$\lambda_{ij}^{(BC_{14})}$ Для $\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$					$\lambda_{ij}^{(BC_{15})}$ Для $\underset{\sim}{T}_{C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$				
C_3																									
C_4																									
C_5																									
C_6																									

Осуществим вычисления показателя уровня риска поформуле (2.5) $lr^{(BC_{11})}$=85, $lr^{(BC_{12})}$=80, $lr^{(BC_{13})}$=85, $lr^{(BC_{14})}$=80, $lr^{(BC_{15})}$=85 и для лингвистического распознавания полученных результатов воспользуемся формулой (2.6), тогда всем показателям $lr^{(BC_{11})}$, $lr^{(BC_{12})}$, $lr^{(BC_{13})}$, $lr^{(BC_{14})}$, $lr^{(BC_{15})}$ соответствуют значения ЛП: «ОР». Далее вычисляется среднее значение уровня риска $lr^{(cp)}$=(85+80+85+80+85)/5=83 и по формуле (2.6) определяется его лингвистический эквивалент – «ОР».Как видно, при увеличении агрессивности среды окружения соответственно увеличился, как средний риск, так и отдельные значения по BC_{1bc_1} $(bc_1=\overline{1,5})$

2.4 Вывод

Кортежная модель базовых характеристик риска, которая за счет композиции базовых характеристик, отображенных шестикомпонентным кортежем, позволяет строить более гибкие и эффективные методы анализа и оценивания рисков относительно динамически изменяемых наборов характеристик.

Проведено исследования широкого спектра существующих САОР с учетом предложенной модели и определен набора базовых характеристик, по которым можно осуществить сравнительный анализ таких САОР и выбрать наиболее подходящие для решения соответствующих задач ЗИ.

3 Экспериментальное система анализа и оценивания рисков

3.1 Базовый алгоритм работы системы анализа и оценивания рисков информационной безопасности

На основании предложенных структурных схем First-CAOP и Second-CAOP систем можно реализовать программные приложения, позволяющие производить анализ и оценивание рисков ИБ в автоматизированном режиме, их базовый алгоритм работы (рис. 4.1) можно описать следующими этапами:

1) Создание нового ПП или открытие существующего;

2) Указание имени существующего ПП;

3) Открытие ПП с сохраненными настройками и имеющимися данными, которые хранятся в БДПП;

4) Указание имени нового ПП и осуществление выбора метода FirstM или SecondM;

5) Создание проекта с выбранными параметрами, реализуется посредством создания таблицы ПП в БД и загрузки пустого проекта;

6) Выбор IR, BC_{1bc_1} и указание значения $ec_i^{BC_{1bc_1}}$;

7) Оценка $lr^{(BC_{1bc_1})}$ для указанного набора IR_h, BC_{1bc_1} и BC_{2bc_2};

8) Запись в БД пользовательских данных и рассчитанного $lr^{(BC_{1bc_1})}$;

9) Расчет $lr^{(cp)}$ для каждого ИР указанного в ПП;

10) Генерация отчетов с указанием всех IR_h и соответствующих им BC_{1bc_1}, а также информации о $lr^{(cp)}$ для ИР в числовой и лингвистической форме и $lr^{(BC_{1bc_1})}$ для каждой угрозы в отдельности.

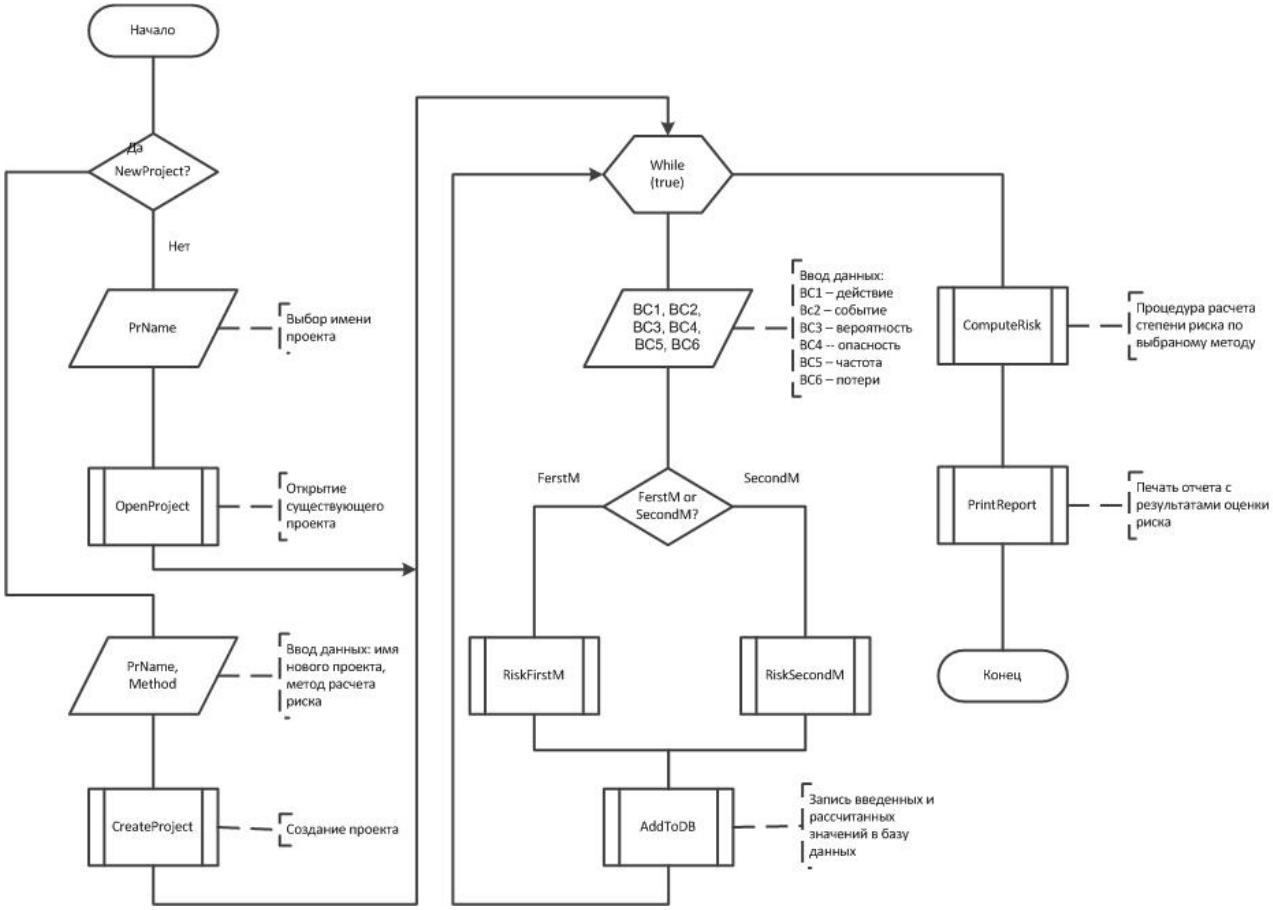
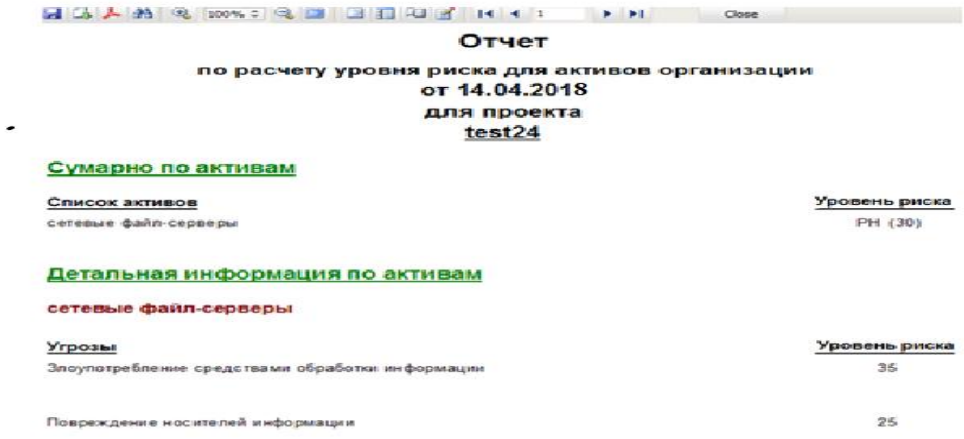


Рис. 3.1 - Базовый алгоритм работы систем анализа и оценивания рисков ИБ

Примеры сформированных отчетов МГО Second-CAOP и First-CAOP систем представлены соответственно на рис. 4.2 а и б.



Отчет

по расчету уровня риска для активов организации
от 14.04.2018
для проекта
test24

Сумарно по активам

Список активов	Уровень риска
сетевые файл-серверы	РН ((30))

Детальная информация по активам

сетевые файл-серверы

Угрозы	Уровень риска
Злоупотребление средствами обработки информации	35
Повреждение носителей информации	25

First-CAOP система

Рис. 3.2 - Пример сгенерированного отчета

На основании предложенной методологии можно строить как программные, так и программно-аппаратные системы, предназначенные для эффективного анализа и оценивания риска ИБ, которые используют в качестве входных данных различные наборы базовых характеристик, что позволяет повысить гибкость и расширяет возможности проектируемых САОР, функционирующих как в детерминированной, так и в нечетко определенной слабоформализованной среде. С использованием этой методологии были представлены структурные решения САОР.

На основе разработанных структур First-САОР систем созданы программные средства (рис. 4.3), которые в отличие от известных п. 2.2 используют в качестве входных данных различные наборы базовых характеристик, что повышает гибкость, удобство использования, интеграцию возможностей и расширяет возможность проектируемых средств анализа и оценивания рисков ИБ функционирующих как в детерминированной, так и в нечеткой, слабо формализованной среде.

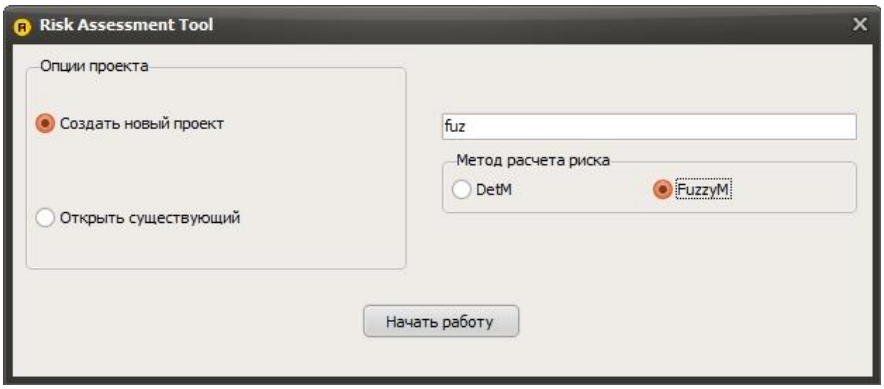


Рис. 3.3 - Внешний вид главного окна программного продукта

3.2 Изучение First-САОР системы

Параллельно со стремительным развитием и внедрением IT-технологий во все сферы деятельности человечества, растет и число угроз связанных с нарушением конфиденциальности, целостности и доступности ИР, которые обрабатываются с помощью этих технологий. Поэтому безопасность таких ресурсов становится приоритетной задачей, как для предпринимательской деятельности, так и для государства в целом. На сегодняшний день решать такую задачу целесообразно с помощью системы управления ИБ. Для построения такой системы необходимо проводить анализ и оценивания рисков ИБ,которые часто характеризуются высокой неопределенностью.

На данный момент существует необходимость в эффективных средствах, которые позволили бы в автоматизированном режиме осуществлять оценивания рисков. Для решения такой задачи, используя методологию синтеза САОР ИБ п. 3.1, которая основана на логико-лингвистическом подходе, известных методах п. 2.3 и п. 2.4 и кортежной модели базовых характеристик риска п. 2.1, было предложено новые соответствующие структурные решения систем оценивания п. 3.2. и п. 3.3.

Для практического применения разработанных методов и соответствующих структурных реализаций систем, необходимо решить актуальную задачу по разработке ПС САОР, которые позволят на практике осуществлять оценивание при различных исходных величинах, а также учитывать возможности эксперта относительно четкого детерминирования оцениваемых базовых характеристик и его неуверенности в своих суждениях.

В связи с этим, целью работы является создание и верификация средств оценивания, которые позволят проводить анализ и оценивание рисков ИБ на основе выбранного базиса характеристик в детерминированной и нечеткой, слабоформализованной среде.

Достижение поставленной цели осуществим на основе предложенных структурных решений First-САОР систем п. 3.2 и п. 3.3. Соответствующие ПС основываются на разработках, которые в отличие от известных п. 2.2 используют в качестве входных данных различные наборы базовых характеристик. Это повышает гибкость, удобство использования, интеграцию возможностей и расширяет спектр функций инструментальных средств работающих в детерминированной среде, для которой в большей степени характерна определенность и стабильность и она достаточно устойчива к влиянию разнообразных возмущений во времени. Также эти средства ориентированы для работы в нечеткой среде, которая характеризуется большой степенью неопределенности, случайности, нестабильности, влиянием разнообразных возмущений во времени и т.п., а для формализации ее процессов используется математический аппарат теории нечетких множеств.

Разработанные ПС были реализованы на основе методологии синтеза систем анализа и оценивания рисков ИБ п. 3.1, согласно которой на первом этапе необходимо осуществить выбор метода оценивания. Далее согласно методологии, для идентификации ИР, а также действий и событий нарушения ИБ, осуществляется формирование соответствующих баз данных (БД):

– действий $BC_{1bc_1}\,(bc_1 = \overline{1,n})$, составленной на основе перечня угроз из ISO / IEC 27002:2005;

– информационных ресурсов IR_h, содержащей в себе список ресурсов согласно метода CRAMM для профиля Commercial;

– базовых характеристик $ec_i^{BC_{1bc_1}}$ (БХ).

Для удобства и последующего использования полученных результатов в ПС все данные сохраняются в проектах пользователей (ПП), которые в свою очередь собраны в БД. Отметим, что здесь в качестве входных данных выступают:

$$IR \in \{IR_h\}\,(h = \overline{1,20});$$

$$BC_1 \in \{BC_{1bc_1}\}\,(bc_1 = \overline{1,60});$$

$$BC_2 \in \{BC_{2bc_2}\}\,(bc_2 = \overline{1,7}),$$

а значение $ec_i^{BC_{1bc_1}}$: $\{ec_i^{BC_{1bc_1}}\}=\{ec_{BC_3}^{BC_{1bc_1}}, ec_{BC_4}^{BC_{1bc_1}}, ec_{BC_5}^{BC_{1bc_1}}, ec_{BC_6}^{BC_{1bc_1}}\}$, где $i=\overline{1,4}$. Идентификаторы IR_h и BC_{1bc_1} принимают текстовые значения соответствующие наименованиям из указанных перечней.

Рассмотрим работу First-CAOP системы. Для последующего оценивания УР, отображаемого параметром *LR*, согласно методологии п. 3.1, осуществляется формирование эталонных значений УР. В предложенном ПС диапазон числовых значений для уровня риска лежит в приделах от 0 до 100. В лингвистической форме *LR* может отображаться следующими значениями:

– «Уровень риска нарушения ИБ очень низкий» (*HP*);

– «Уровень риска нарушения ИБ низкий» (*PH*);

– «Уровень риска нарушения ИБ средний» (*PC*);

– «Уровень риска нарушения ИБ высокий» (*PB*);

– «Уровень риска нарушения ИБ высокий» (*OP*).

Для определения соответствия (лингвистическое распознавание) полученного числового значения УР $lr^{(BC_{1bc_1})}$ лингвистическому, применяется формула (4.1):

$$\underset{\sim}{T}_{LR}=\begin{cases} HP, при\ lr^{(BC_{1bc_1})}\in[\ lr_{\min};\ lr_1[\\ PH, при\ lr^{(BC_{1bc_1})}\in[\ lr_2;\ lr_3[\\ PC, при\ lr^{(BC_{1bc_1})}\in[\ lr_4;\ lr_5[\\ PB, при\ lr^{(BC_{1bc_1})}\in[\ lr_6;\ lr_7[\\ OP, при\ lr^{(BC_{1bc_1})}\in[lr_8;\ lr_{\max}] \end{cases}, \quad (3.1)$$

где [lr_{min}; lr_1[, [lr_2; lr_3[, [lr_4; lr_5[, [lr_6; lr_7[, [lr_8; lr_{max}], например, будут соответствовать значения [0; 20[, [20; 40[, [40; 60[, [60; 80[, [80; 100].Формирование эталонных значений для БХ в ПС было реализовано в следующем виде:

– BC_3 (принимает значение в диапазоне от 0 до 100, шаг дискретизации – 1);

– BC_4 (принимает значения от 0 до 10, шаг дискретизации – 1);

– BC_5 (находится в диапазоне от 0 до 1, шаг дискретизации – 0,01);

– BC_6 (лежит в пределах от 0 до 0,5, шаг дискретизации – 0,01).

На этапах формирования уровня значимости и определения текущего значения БХ в ПС для ввода данных используется интерактивный интерфейс, который представлен на рис. 4.4 (верхнее окно).

Классификация текущих значений и оценка УР в ПС осуществляется в автоматизированном режиме. При этом, для каждого действия (угрозы) реализуется расчет значения $lr^{(BC_{1bc_1})}$ по выражению

$$lr^{(BC_{1bc_1})} = \sum_{j=1}^{m}\left(lr_j \sum_{i=1}^{g} LS_i \lambda_{ij}^{(BC_{1bc_1})} \right),$$

где lr_j=90-20(j-1),

$$\lambda_{ij}^{(BC_{1bc_1})} = \begin{cases} 1, \textit{при } ec_i^{BC_{1bc_1}} \in [\, c_{EC_i(j-1)}; c_{EC_i j}[\\ 0, \textit{при } ec_i^{BC_{1bc_1}} \notin [\, c_{EC_i(j-1)}; c_{EC_i j}[\end{cases} (bc_1 = \overline{1,n}),$$

$$LS_i = \frac{2(g-i+1)}{(g-1)g} \; (i = \overline{1,g}) \text{ или } LS_i = 1/g \; (j = \overline{1,m}).$$

Для ИР значение $lr^{(cp)}$ вычисляется на основе выражения $lr^{(cp)} = (\sum_{bc_1=1}^{m} lr^{(BC_{1bc_1})}) / m$.

Полученные результаты имеют соответствующую интерпретацию, а ПС генерирует необходимый отчет.

Для тестирования основных функций и отражения принципа работы ПС САОР выполним его верификацию, с помощью компьютера под управлением операционной системы MicrosoftWindows 7 HomePremium x64. Разработанное приложение для своей работы не требует дополнительных библиотек и системных файлов, поскольку при компиляции проекта были указаны следующие опции: Usedynamic RTL = false; Buildwithruntimepackages = false. Также дополнительно для функционирования БД был установлен сервер MySQL 5.1.60 x64. С помощью разработанного ПС создан тестовый проект «test24», а в качестве IR_1 для верификации выбран «сетевой файл-сервер» из категории «Сетевые серверы». Тестирование проводилось при четко определенных исходных данных, т.е. в так называемой детерминированной среде.

Для данного ИР были установлены следующие BC_{1bc_1} ($bc_1 = \overline{1,3}$):

BC_{11}=«Злоупотребление средствами обработки информации» (из категории «Нецелевое использование компьютерного оборудования и сети Интернет сотрудниками организации»);

BC_{12}=«Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика» (из категории «Угрозы утечки конфиденциальной информации»);

BC_{13}=«Повреждение носителей информации» (из категории «Угрозы доступности IT-сервисов и разрушения (потери) информационных активов»).

После этого по каждой угрозе осуществляются расчеты значений $lr^{(BC_{1bc_1})}$, результаты которых также представлены в табл. 4.1, из которой видно, что значение уровня риска для данного ИР по всем угрозам низкое.

Таблица 4.1 - Результаты оценивания ПС First-CAOP

BC_{1bc_1}	BC_3	BC_4	BC_5	BC_6	$lr^{(BC_{1bc_1})}$	$\underset{\sim}{T}_{LR}$
BC_{11}	42	1	0,67	0,05	35	PH
BC_{12}	25	4	0,13	0,31	35	PH
BC_{13}	33	3	0,07	0,17	25	PH

Далее производится расчет среднего значения $lr^{(cp)}$ для данного ИР, в результате чего получаем $lr^{(cp)} = 31{,}67$, что соответствует $\underset{\sim}{T}_{LR}$ – PH (см. выражение (4.1)).

Дальнейшая верификация ПС выполнялась на основе моделирования для нескольких состояний среды оценивания:

1-е состояние – начальные условия с установленным количеством угроз для ИР;

2-е состояние – увеличено количество угроз для ИР;

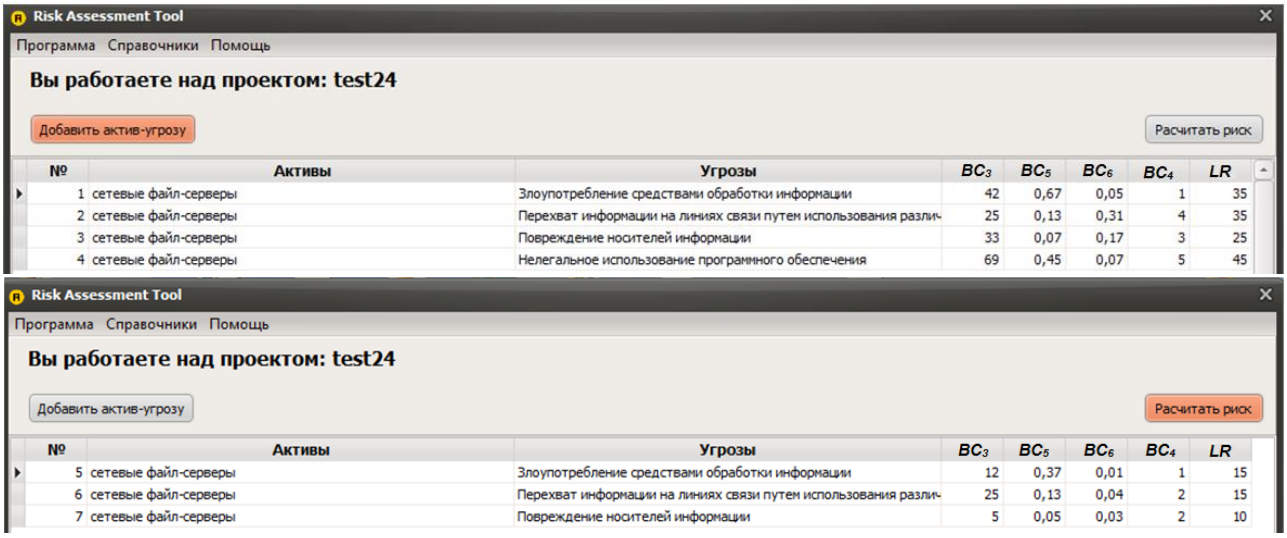


Рисунок. 3.4 - Интерактивный интерфейс ПС First-CAOP

3-е состояние – блокировано одну угрозу для ИР;

4-е состояние – изменение значений базовых характеристик (уменьшение или увеличение).

1-е состояние с начальными условиями, а также результаты вычисления УР, приведены в таблице 1. Рассмотрим результаты моделирования для следующих состояний.

2-е состояние

К ПП были внесены изменения, путем введения дополнительного BC_{14} для IR_1=«Сетевой файл-сервер», т.е. BC_{14}=«Нелегальное использование программного обеспечения», которое входит в категорию «Юридические

угрозы». В табл. 4.2 приведены значения $ec_i^{BC_{1bc_1}}$, которые были определены по оценкам экспертов. В результате этого осуществлен расчет значения УР для BC_{14}т.е. $lr^{(BC_{14})}$=45 (см. рис. 1 первое окно), а среднее $lr^{(cp)}$ после интегрирования с BC_{14} составило $lr^{(cp)}$= 35, что соответствует значению $\underset{\sim}{T}_{LR}$ – *РН*.

Таблица 4.2 - Значение $ec_i^{BC_{1bc_1}}$ ПСFirst-САОР

BC_{1bc_1}	***BC₃***	***BC₄***	***BC₅***	***BC₅***
BC_{11}	42	1	0,67	0,05
BC_{12}	25	4	0,13	0,31
BC_{13}	33	3	0,07	0,17
BC_{14}	69	5	0,45	0,07

3-е состояние

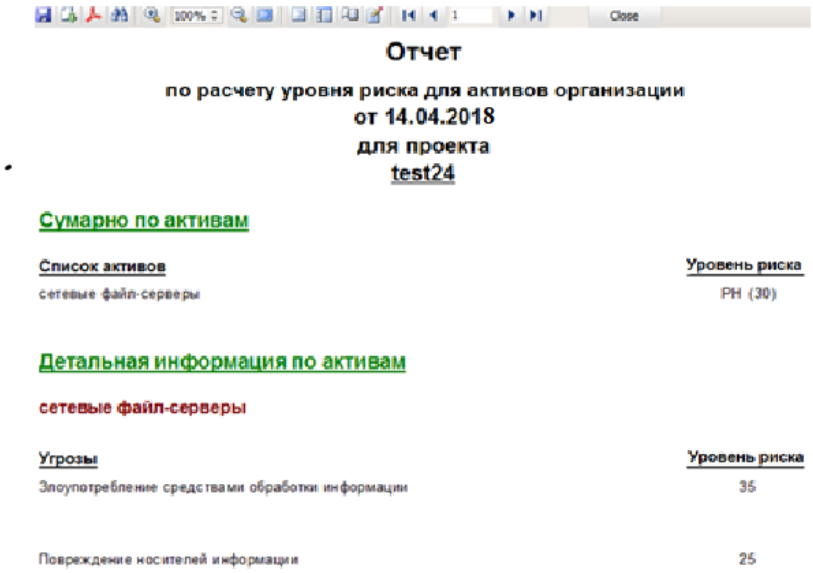
Далее было проведено моделирование в условиях, когда на оцениваемом объекте защиты проведены мероприятия по устранению BC_{12}=«Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика». Здесь также выполнено повторное измерение $lr^{(BC_{1bc_1})}$ и$lr^{(cp)}$. Используя разработанную систему, с учетом моделируемой ситуации, полученное значение $lr^{(cp)}$ дляIR_1 уменьшилось до 30, т.е. $lr^{(cp)}\underset{\sim}{T}_{LR}$ = 30 (РН). Это можно увидеть из сформированного разработанным инструментальным средством отчета, представленного на рис. 4.5. Здесь значение $lr^{(cp)}$меняется при изменении количества BC_{1bc_1}, а УР нарушения ИБ во всех случаях, определяется как низкая. Дальнейшее экспериментальное исследование показало, что при значительном увеличении или уменьшении числа BC_{1bc_1} значение$lr^{(cp)}$может соответственно адекватно измениться.

4-е состояние

После выполненных расчетов, согласно 1-го состояния, было проведено моделирование для двух ситуаций:

– первая (на объекте защиты учтены предыдущие результаты анализа и оценивания рисков ИБ и внедрены меры для минимизации рисков);

– вторая (на объекте защиты не учтены предыдущие результаты оценивания – не приняты решения по внедрению мер для снижения рисков).



Отчет

по расчету уровня риска для активов организации
от 14.04.2018
для проекта
test24

Сумарно по активам

Список активов	Уровень риска
сетевые файл-серверы	РН (30)

Детальная информация по активам

сетевые файл-серверы

Угрозы	Уровень риска
Злоупотребление средствами обработки информации	35
Повреждение носителей информации	25

Рисунок. 3.5 - Сгенерированный отчет ПС First-CAOP

С учетом первой ситуации, на объекте защиты, был проведен ряд мероприятий, направленных на уменьшение уровня угроз для заданного ИР, а именно:

– внедрена система разграничения доступа, пользователям предоставлены права и привилегии в соответствии с их должностными обязанностями для минимизацииBC_{11} = «Злоупотребление средствами обработки информации»;

– разработана система шифрования сетевого трафика для устраненияBC_{12}=«Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика»;

– реализованы системы мониторинга состояния жестких дисков, настроена политика регулярного создания резервных копий критической информации, внедрены технологии RAID 1 для нейтрализации BC_{13}=«Повреждение носителей информации».

После повторной реализации анализа и оценивания рисков ИБ экспертами были установлены величины базовых характеристик, значения которых приведены в табл. 4.3.

Результаты проведенных изменений в проекте имеют вид, показанный на рис. 4.4 (нижнее окно).

Для каждой BC_{1bc_1} был повторно осуществлен расчет значений $lr^{(BC_{1bc_1})}$, результаты которого отображены в таблице 3.3.

Таблица 3.3 - Значение оценочных компонент и $lr^{(BC_{1bc_1})}$ ПСFirst-CAOP

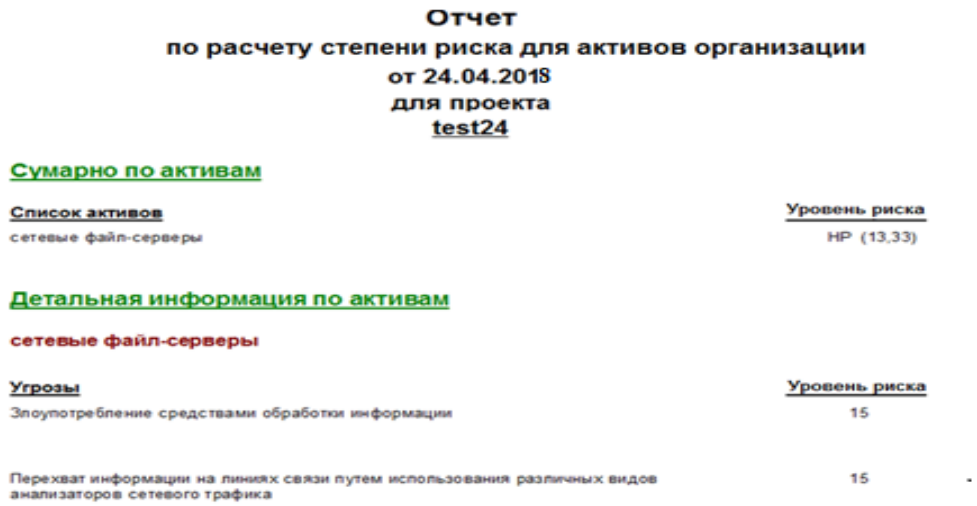
BC_{1bc_1}	BC_3	BC_4	BC_5	BC_6	$lr^{(BC_{1bc_1})}$	$\underset{\sim}{T}_{LR}$
BC_{11}	12	1	0,37	0,01	15	НР
BC_{12}	25	2	0,13	0,04	15	НР
BC_{13}	5	2	0,05	0,03	10	НР

Как видно для каждой BC_{1bc_1} значение $lr^{(BC_{1bc_1})}$ интерпретируется на уровне «Уровень риска нарушения ИБ очень низкий». Очевидно,дляIR_1 величина $lr^{(cp)}$=13,33, что соответствует ЛП – *HP* (рисунок 4.6).

Из приведенного отчета (рис. 4.6) прослеживается существенное уменьшение значений $lr^{(BC_{1bc_1})}$, что позволяет, в свою очередь, сделать вывод об адекватности работы ПС First-CAOP при изменении условий среды оценивания.

С учетом второй ситуации, осуществляется моделирование, при котором на объекте защиты не учтены предыдущие результаты оценок. После первичной реализации анализа и оценивания рисков ИБ, не приняты во внимание полученные результаты и не внедрены меры по обеспечению ИБ. В результате этого, после повторного оценивания состояния с выбранным IR_1 ухудшилась, о чем свидетельствуют проставленные экспертами значения базовых характеристик (таблице 4.4). Как видно из таблице 4.4, величины $lr^{(BC_{1bc_1})}$ по каждой BC_{1bc_1} существенно увеличились, а для двух угроз значение «*PH*» изменилось на «*PC*» (Уровень риска нарушения ИБ средний). Для IR_1 значение $lr^{(cp)}$=43,33, что в свою очередь соответствует, согласно выражению (4.1), величине $\underset{\sim}{T}_{LR}$=«*PC*». Это свидетельствует о негативных тенденциях относительно ИБ для объекта защиты (по сравнению со значением $lr^{(cp)}$=31,67, $\underset{\sim}{T}_{LR}$ =«РН» в первичном отчете).

.



Отчет
по расчету степени риска для активов организации
от 24.04.2018
для проекта
test24

Сумарно по активам

Список активов	Уровень риска
сетевые файл-серверы	HP (13,33)

Детальная информация по активам

сетевые файл-серверы

Угрозы	Уровень риска
Злоупотребление средствами обработки информации	15
Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика	15

Рисунок. 3.6 - Результаты оценки $lr^{(BC_{1bc_1})}$ ПСFirst-CAOP

Также с учетом первого и второго состояния было произведено оценивание рисков для дополнительных трех ИР. В таблице 3.5 и на рисунке 3.7 показаны значения $lr^{(cp)}$ для этих ИР.

Таблица 3.4 - Результаты оценивания ПС First-CAOP

BC_{1bc_1}	BC_3	BC_4	BC_5	BC_6	$lr^{(BC_{1bc_1})}$	$\underset{\sim}{T}_{LR}$
BC_{11}	52	1	0,81	0,05	40	*PH*
BC_{12}	45	4	0,23	0,31	45	*PC*
BC_{13}	43	3	0,47	0,27	45	*PC*

Сравнивая полученные результаты, можно сделать вывод, что при изменении значений базовых характеристик разработанное ПС First-CAOP адекватно реагирует на соответствующие условия среды оценивания.

Таблица 3.5 - Значение $lr^{(cp)}$ ПСFirst-CAOP

ИР	$lr^{(cp)}$		
	Средний уровень риска (начальные условия)	Пониженный уровень риска	Повышенный уровень риска
IR_1	31,67 (*PH*)	13,33 (*HP*)	43,33 (*PC*)
IR_2	20 (*HP*)	15 (*HP*)	26,5 (*PH*)
IR_3	28,33 (*PH*)	23,33 (*PH*)	30 (*PH*)
IR_4	28,33 (*PH*)	22,5 (*PH*)	31,25 (*PH*)

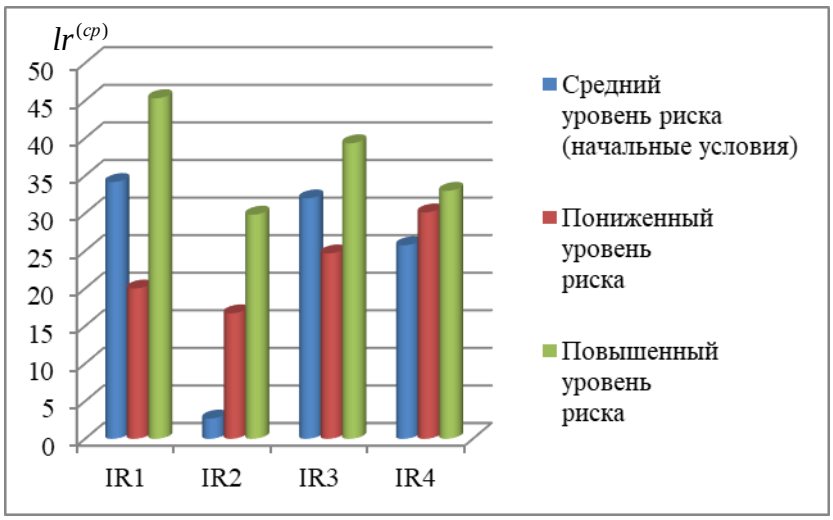


Рисунок. 3.7 - Гистограмма средних значений уровня риска ПСFirst-CAOP

По аналогии с предыдущими экспериментами были проведены дополнительные исследования для других BC_{1bc_1}, результаты которых занесены в соответствующие таблице. 3.6-3.8.

Таблица 3.6 - Результаты оценивания ПСFirst-CAOP

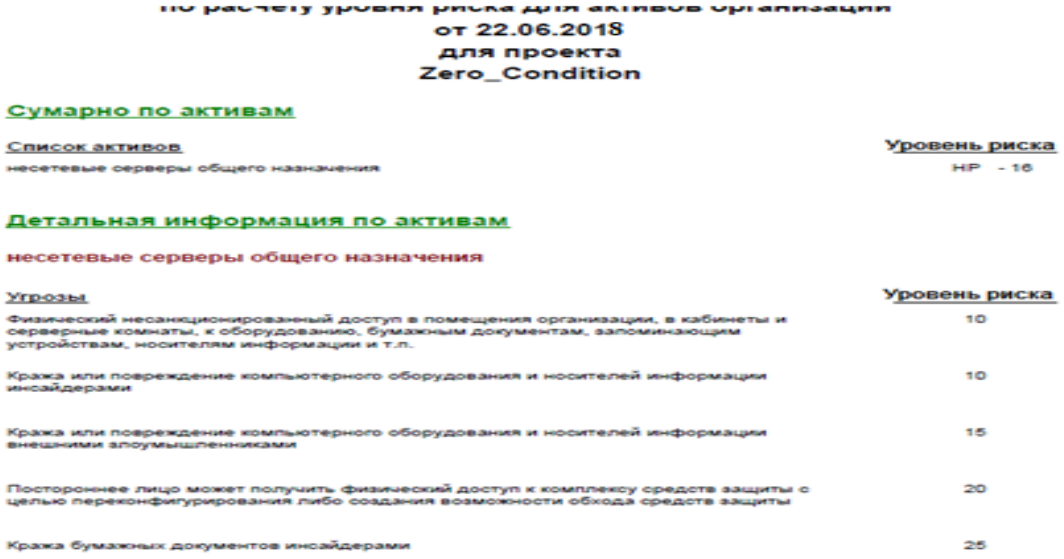
ССО	БХ	В C_{11}	В C_{12}	В C_{13}	В C_{14}	$lr^{(cp)}(\underset{\sim}{T}_{LR})$
1	BC_3	30	41	12	-	-
	BC_4	2	2	3	-	-
	BC_5	0,15	0,36	0,17	-	-
	BC_6	0,12	0,01	0,05	-	-
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	20 (НР)	25 (РН)	15 (НР)	-	20 (НР)
2	BC_3	30	41	12	16	-
	BC_4	2	2	3	5	-
	BC_5	0,15	0,36	0,17	0,23	-
	BC_6	0,12	0,01	0,05	0,17	-
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	20 (НР)	25 (РН)	15 (НР)	30 (РН)	22,5 (РН)
3	BC_3	23	23	9	-	-
	BC_4	2	1	1	-	-

	BC_5	0,07	0,3	0,06	-	-
	BC_6	0,03	0,01	0,05	-	-
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	15 (HP)	20 (HP)	10 (HP)	-	15 (HP)
4	BC_3	36	47	23	-	-
	BC_4	2	5	4	-	-
	BC_5	0,15	0,39	0,21	-	-
	BC_6	0,16	0,08	0,08	-	-
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	20 (HP)	35 (PH)	25 (PH)	-	26,67 (PH)
5	BC_3	32	23	47	-	-
	BC_4	4	2	3	-	-
	BC_5	0,21	0,12	0,2	-	-
	BC_6	0,3	0,03	0,06	-	-
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	40 (PH)	15 (HP)	30 (PH)	-	28,33 (PH)
6	BC_3	32	23	47	41	-
	BC_4	4	2	3	5	-
	BC_5	0,21	0,12	0,2	0,33	-
	BC_6	0,3	0,03	0,06	0,1	-
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	40 (PH)	15 (HP)	30 (PH)	40 (PH)	31,25 (PH)
7	BC_3	26	17	22	-	-
	BC_4	3	1	3	-	-
	BC_5	0,16	0,12	0,2	-	-
	BC_6	0,3	0,01	0,03	-	-
	$lr^{(BC_{1bc_1})}(\underset{\sim}{T}_{LR})$	35 (PH)	10 (HP)	25 (PH)	-	23,33 (PH)

8	BC_3	38	31	52	-	-
	BC_4	4	2	4	-	-
	BC_5	0,27	0,16	0,25	-	-
	BC_6	0,33	0,04	0,12	-	-
	$lr^{(BC_{1bc1})}(\underset{\sim}{T}_{LR})$	40 (РН)	15 (НР)	35 (РН)	-	30 (РН)

В таблице. 3.6 используются следующие сокращения, ССО – состояние среды окружения, для которой позиции 1 и 5 отображают начальные условия, 2 и 6 – изменение количества угроз заданным ИР, 3 и 8 – изменение значений оценочных компонент (3 и 7 – уменьшение значений базовых характеристик; 4 и 8 – увеличение значений базовых характеристик), а БХ – базовые характеристики.

Приведем результаты еще нескольких экспериментов. Для подтверждения гипотезы относительно использования базовых характеристик осуществим анализ и оценивание рисков ИБ при различных наборах этих характеристик (рисунок 4.8). Полученные результаты исследования подтверждают, что ПС First-CAOP адекватно реагирует на изменение значений базовых характеристик при различных условиях среды оценивания, а значение риска существенно не изменяется при смене их базиса.



по расчету уровня риска для активов организации
от 22.06.2018
для проекта
Zero_Condition

Сумарно по активам

Список активов	Уровень риска
несетевые серверы общего назначения	НР - 16

Детальная информация по активам

несетевые серверы общего назначения

Угрозы	Уровень риска
Физический несанкционированный доступ в помещения организации, в кабинеты и серверные комнаты, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и т.п.	10
Кража или повреждение компьютерного оборудования и носителей информации инсайдерами	10
Кража или повреждение компьютерного оборудования и носителей информации внешними злоумышленниками	15
Постороннее лицо может получить физический доступ к комплексу средств защиты с целью переконфигурирования либо создания возможности обхода средств защиты	20
Кража бумажных документов инсайдерами	25

Рисунок. 3.8 - Пример отчета ПС First-CAOP при выборе одной базовой характеристики

3.3 Вывод

Проведено экспериментальное ПО САОР, с целью верификации разработанных методов, модели, структурных решений и ПС. Экспериментальное исследование САОР показало, что при любом базисе характеристик можно реализовывать адекватную оценку. Также были проведены расчеты при различных условиях среды оценивания: на начальном этапе состояния объекта защиты; с реализацией мер по снижению риска; при ситуации.

4 Технико-экономическая обоснование дипломного проекта

4.1 Характеристика дипломной работы

Данная дипломная работа на тему «Методы анализа и оценки рисков в информационных ресурсов» было реализован при помощи сторонных програм обеспечения. Этот комплекс дипломной работы осуществлен на платформах Windows 8 и включает в себя:

- применение методик и стандартов ISO 27001
- применение утилитов security tools , rick assessments;
- применение программных продуктов.

Экономическое обоснование для создания комплекса дипломной работы заключается в исследование уязвимостей серверного ПО для обеспечения достоверных данных на данную тему и реализацию данной работы.

4.2 Расчет финансовой части

Определение трудоемкости разработки данного комплекса дипмломных работ на тему «Методы анализа и оценки рисков в информационных ресурсов».

Затраты на материальные ресурсы определяется по формуле:

$$З_{мат} = \sum_{i=1}^{n} P_i \times Ц_i \qquad (4.1)$$

где P_i – расход i–того вида материального ресурса;

$Ц_i$ – цена за единицу i–того вида материального ресурса, тг;

i - вид материального ресурса;

n - количество видов материальных ресурсов.

Таблица 4.1 –Распределение работ по этапам и видам, оценка их трудоемкости

Этап разработки	Вид работы	Трудоемкость, чел*ч
этап	Постановка задачи: определение требуемых технических средств и программного обеспечения, реализация данного проекта.	1*580
этап	Конфигурация оборудования и настройка ПО. Ввод технического оборудования в эксплуатацию.	1*290
этап	Демонстрация уязвимостей серверов и разработка комплекса лабораторных работ.	1*240

Итого	1110

Расчет затрат на выполнение данного проекта. Затраты на материальные ресурсы указаны в таблице 4.2

Таблица 4.2 – Затраты на материальные ресурсы

Наименование материального ресурса	Единица измерения	Количество	Цена за единицу, тг	Итого, тг
Ноутбук	Шт.	2	220 000	440 000
Модем TP-Link	Шт.	1	20 000	20 000
Лицензионная ОС Windows 8	Шт.	2	20 000	40 000
Программные продукты	Шт.	1	100 000	100 000
Итог				600 000

Расчет затрат на материальные ресурсы:

$$З_{МАТ} = 440\,000 + 20\,000 + 40\,000 + 100\,000 = 600\,000т$$

Для разработки проекта использовалось электрооборудование, необходимо рассчитать затраты на электроэнергию по форме, приведенной в таблице 4.3

Таблица 4.3 – Затраты на электроэнергию

Оборудование	Паспортная мощность, кВт	Время работы для НИР, час	Цена электроэнергии, тенге	Сумма, тенге
Ноутбук (2 шт.)	0,3	360	18,42	1989,36
Освещение	0,5	370	18,42	3407,7
Программные продукты	0,1	240	18,42	4420,8
Модем TP-Link	0,1	350	18,42	644,7

Итого затраты на электроэнергию	10461,06

Общая сумма затрат на электроэнергию (ЗЭ) рассчитывается по формуле:

$$З_э = \sum_{i=1}^{n} M_i \text{ x } K_i \text{ x } T_i \text{ x Ц} \qquad (4.2)$$

где M_i – паспортная мощность i–го электрооборудования, кВт;

K_i – коэффициент использования мощности i-го электрооборудования

T_i - время работы

Ц – цена электрооборудования;

i – вид электрооборудования;

n – количество электрооборудования;

Дневная ставка (с 7.00 до 20.00) –18,42 тенге за 1 кВтч; Расходы на электроэнергию (ноутбуки):

$$З_{эл\text{-}н} = 0,3 * 360 * 18,42 = 1989,36$$

Расходы на электроэнергию (освещение):

$$З_{эл\text{-}пр} = 0,5 * 370 * 18,42 = 3407,7$$

Расходы на электроэнергию (маршрутизатор):

$$З_{эл\text{-}мэ} = 0,1 * 240 * 18,42 = 4420,8$$

Расходы на электроэнергию (модем):

$$З_{эл\text{-}мэ} = 0,1 * 350 * 18,42 = 644,7$$

$$З_э = 1989,36 + 3407,7 + 4420,8 + 644,7 = 10461,06$$

Затраты на оплату труда сотрудникам указаны в таблице 4.4

Таблица 4.4 – Затраты на оплату труда

Категория работника	Квалификация	Трудоёмкость, чел*ч	Часовая ставка, тг/ч	Сумма, тг
Сетевой администратор	Специалист	1*640	300	192 000
Риск менеджер	Специалист	1*640	250	160 000
Итого				352 000

Фонд оплаты труда (ФОТ) определяется суммой основной заработной платы (ОЗП) и резервной заработной платы (РЗП) [12].

РЗП составляет 15% от основной заработной платы (ОЗП):

$$РЗП=0,15ОЗП \quad (4.3)$$

РЗП = 0,15 · 192 000 = 28 800 тенге.
РЗП = 0.15 · 160 000 = 24 000 тенге.

$$ФОТ=ОЗП+РЗП \quad (4.4)$$

ФОТ = 192 000 + 28 800 = 220 800 тенге.
ФОТ = 160 000 + 24 000 = 184 000 тенге.

При расчете фонда заработной платы, нужно учитывать, социальный налог в размере 11% от общего фонда оплаты труда после отчисления в пенсионный фонд:

$$С_н = 0.11(ФОТ – 0,1·ФОТ) \quad (4.5)$$

$С_н$ = 0.11· (220 800 – 0.1·220 800) = 21 859.2тенге

$С_н$ = 0.11· (184 000 – 0.1·184 000) = 18 216 тенге

Далее будет выполнен расчет амортизации основных фондов. Сумма амортизационных отчислений начисляется по единым нормам и рассчитывается по формуле:

$$\sum^{n}_{i+1} = Ф_i + Н_а + Т\ 100 * Т_{ЭФ} \quad (4.6)$$

где $Ф_i$ – стоимость оборудования, тг.;

$Н_а$– годовая норма амортизации оборудования, %;

$Т_н$– время работы оборудования за весь период выполнения

Данные амортизации основных фондов показаны в таблице 4.5

Таблица 4.5 – Амортизация основных фондов (ОФ)

Наименование оборудования	Стоимость оборудования, тенге	Норма амортизации, %	Эффективный фонд времени работы оборудования и ПО, год	Фактич. время использ. оборудов., ч
Ноутбук (2 шт.)	300 000	25	5	350
Модем TP-Link	20 000	25	5	350
Программный продукт	40 000	25	5	240

Выполнение проекта заняло 940 часов, из которых:

Ноутбуки использовались 350 ч.;

Модем – 350 ч.;

Программный продукт – 240 ч.

Годовые нормы амортизации ОФ принимаются по налоговому кодексу РК или определяются, исходя из возможного срока полезного использования ОФ:

$$H_{AI} = T_{NI}$$

где H_{AI} – годовая норма амортизации i–го оборудования, %;

T_{NI} - возможный срок полезного использования i–го оборудования,Возможный срок полезного использования ОФ может быть принят от 3 до 10 лет (по согласованию с консультантом по экономической части). Планируемое использование составляет 4 года.

$$H_{AI} = 100 /4 = 25\%$$

Таблица 5.6 – Смета затрат на разработку ПП

Наименование статей расходов	Значение затрат, тенге
Оборудование и ПО	420 000
Электроэнергия	7 717
Затраты на оплату труда	192 000
Социальные налоги	21854
Прочие расходы (кабели, RJ-45, интернет)	5 500
Итого	647 076,2

Диаграмма структуры эксплуатационных затрат приведена на рисунке

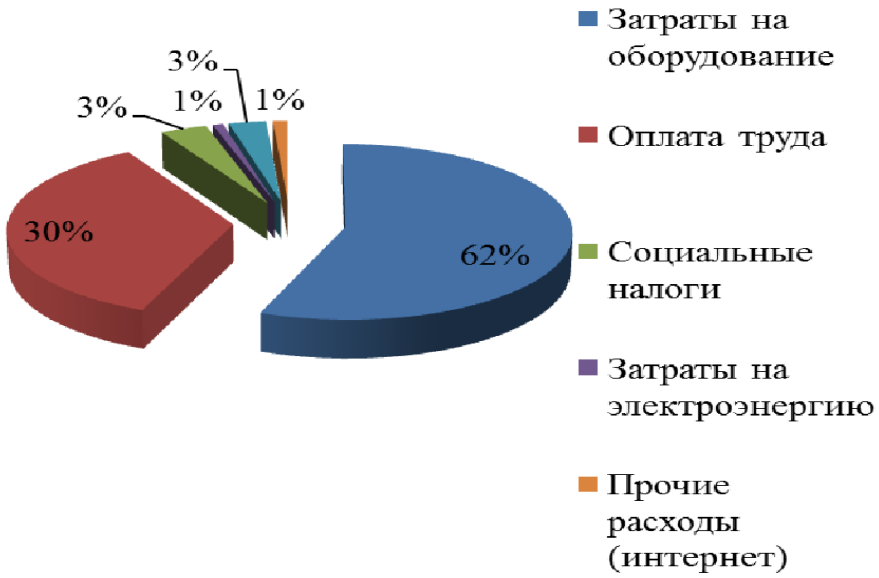


Рисунок 4.1 – Диаграмма структуры эксплуатационных затрат

4.3 Социальный эффект

Положительный эффект от внедрения разработанного комплекса лабораторных работ по информационной безопасности на тему

«Исследование уязвимостей серверов»:

- повышение уровня знании об уязвимостях серверного ПО, а так-же об типах серверного ПО;
- позволяет практически проверить данные уязвимости и сделать анализ самой атаки и возможности обезопасить себя от данных угроз;
- практическая польза для кафедры радиотехники и информационной безопасности.

Разработанный комплекс решает поставленные задачи поставленные кафедрой для получение комплекса лабораторных работ.

4.4 Вывод по экономической части

В данной главе, было рассмотрено экономическое обоснование для выполнения дипломного проекта.

В данной главе был произведён расчет всех необходимых расходов на покупку материальных средств, затрат на энергопотребление, на пенсионные отчисления, выплата налогов и амортизационных отчислений.

Данный проект был направлен на научно-исследовательские нужды кафедры радиотехники и информационной безопасности, что в последствие привело к разработке данного комплекса лабораторных работ.

5 Безопасность жизнедеятельности

5.1 Анализ условий труда при разработке комплекса мероприятий по обеспечению информационной безопасности компании

Данный комплекс лабораторных работ на тему «Исследование уязвимостей серверов». Данный комплекс лабораторных работ осуществлен на базе Windows 7/8, и включает в себя:

- применение методик и стандартов ISO 27001
- применение утилитов security tools , rick assessments;
- применение программных продуктов

Серверное оборудование размещено в офисном помещении, которое имеет следующие размеры: 6x4x3,2.

Высота рабочей поверхности над уровнем пола составляет 0,8 м, окна начинаются с высоты 0,8 м, высота окон составляет 2,4 м. Рядом стоящее здание находится на расстоянии 8 м, высотой 12 м, с других трех сторон затеняющих зданий нет.

Согласно «Временным санитарным нормам и правилам для работников вычислительных центров» при вводе данных, редактировании программ, чтении информации с экрана непрерывная продолжительность работы с монитором не должна превышать четырех часов (с учетом восьми часового рабочего дня). Для снижения напряженности труда рекомендуется равномерно распределять нагрузку и по возможности чередовать характер деятельности.

По прошествии часа работы, рекомендуется сделать перерыв на 5–10 минут, а через каждые два часа перерыв можно увеличить до 15 минут. Один или несколько раз за час желательно выполнить серию легких упражнений для снижения напряжения (растягивание), которое накапливается в мышцах при длительной работе за персональным компьютером. Данная категория работ относится к 1а.

Одним из важнейших элементов рационального планирования рабочего места оператора является учет его индивидуальных антропометрических и психофизиологических данных.

В санитарных правилах и нормах «СанПиН 2.2.2.542-96» описываются общие требования к организации и оборудованию рабочих мест работающего при использовании персональной электронно-вычислительной машины (ПЭВМ).

Конструкция рабочего стола обеспечивает оптимальное размещение за рабочей поверхностью, как рабочего, так и используемого оборудования, а так же обеспечивает удобство размещения с учётом количества и конструктивных особенностей оборудования и характера выполняемой работы. Высота рабочей поверхности стола регулируется от 680 до 800 мм. Рабочий стол

должен иметь пространство для без препятственного размещения ног: высота

– не менее 600 мм, ширина – не менее 500 мм, глубина – не менее 450 - 650мм.

Наиболее оптимальным считается размещение оборудования оператора, которое представлено на рисунке 5.1.

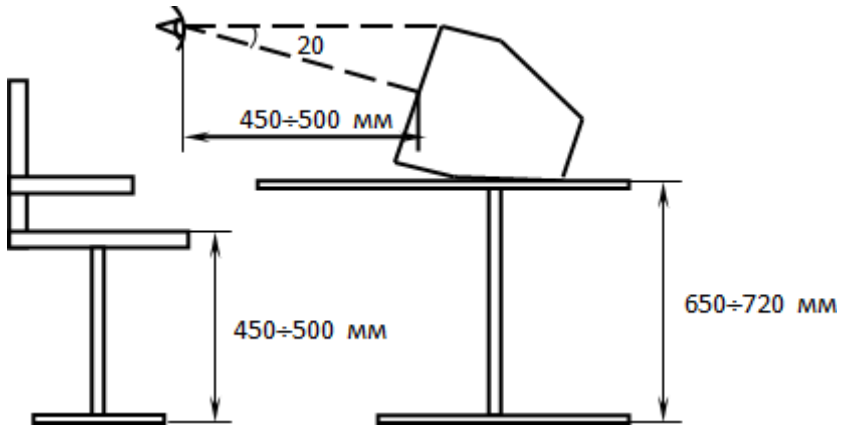
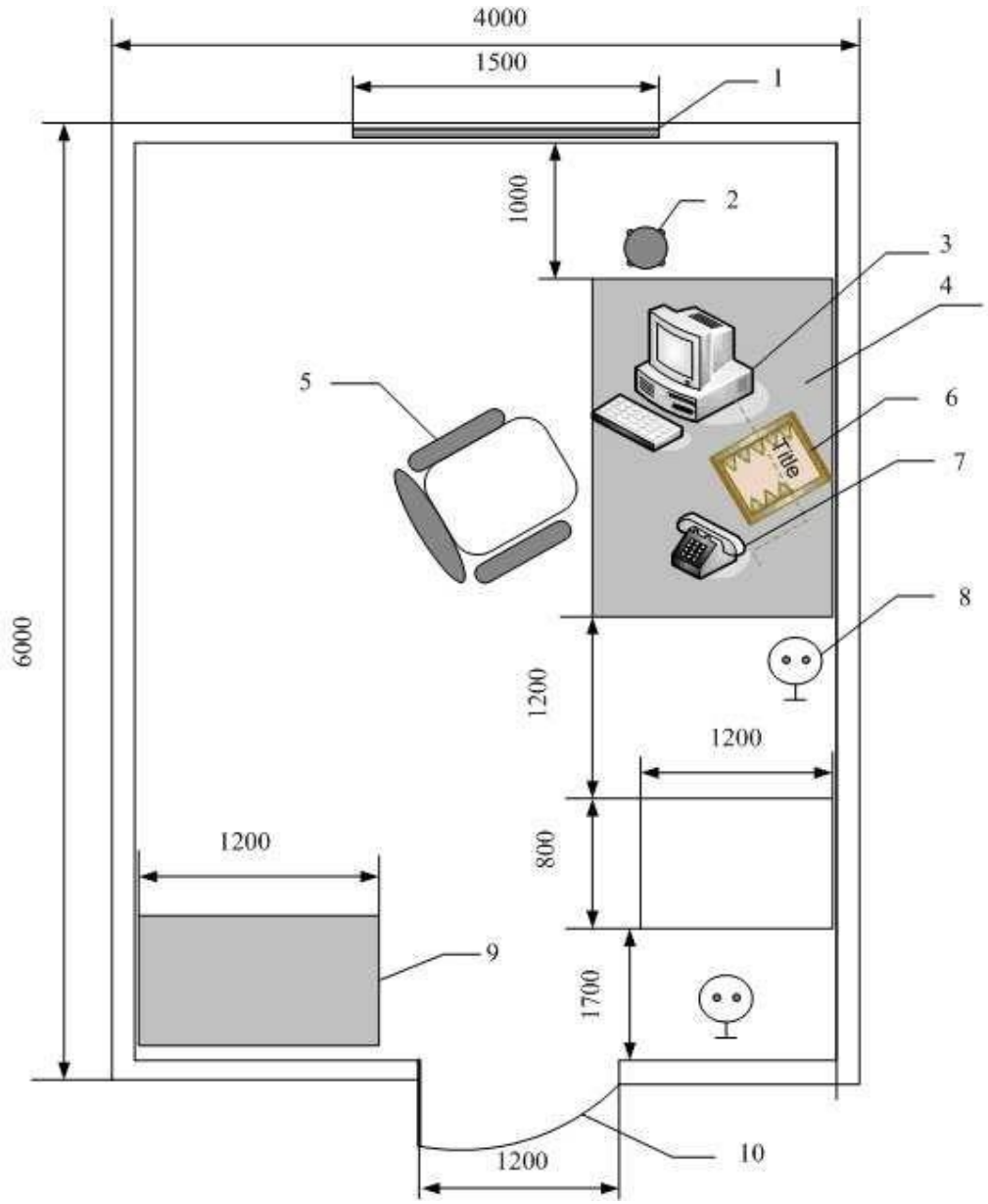


Рисунок 5.1 – Оптимальные размещение оборудования оператора рабочего места

Монитор размещается на рабочем столе или подставке таким образом, чтобы расстояние наблюдения информации на его экране не превышало 700 мм от глаз работающего. Для букв и цифр рекомендуемое значения составляет 15-18 мм. Экран монитора располагается под углом 20 градусов чтобы по высоте данный угол находился между нормалью к центру экрана и горизонтальной линией взгляда. В горизонтальной плоскости угол наблюдения экрана не должен превышать значения в 60 градусов.

Клавиатура размещается на рабочем столе или подставке таким образом, чтобы высота клавиатуры по отношению к полу составляла порядка 650-720 мм, а положение рук работающего находилось параллельно поверхности стола, и кисти были расположены над столом на высоте 20-35 мм при работе на клавиатуре. Данное положение позволяет снять напряжение с рук в перерывах между печатанием и расслабляет кисти и предплечья.

Для ввода работающим любых данных, рекомендуется располагать документ так, чтобы расстояние не превышало 500 мм от глаза оператора, и располагалось желательно слева. При данном расположении угол между экраном дисплея и документом в горизонтальной плоскости составляет 30-40 градусов. Угол наклона клавиатуры рекомендуется устанавливать в 15 градусов. Экран дисплея, документы и клавиатуру необходимо расположить таким образом, чтобы перепад яркостей поверхностей, зависящий от их расположения относительно источника света, и не превышал масштаба 1:10.



1 - окно, 2 - урна, 3 - персональный компьютер, 4 - Стол письменный, 5 - кресло, 6 - журнал регистрации неисправностей, 7 - телефон, 8 – розетка (евростандарт), 9 - шкаф, 10 - дверь.

Рисунок 5.2 – План размещения в рабочей комнате оператора

5.2 Требования к микроклимату

В производственных помещениях с эксплуатацией персональных компьютеров климатические параметры, такие как температура, относительная влажность и скорость движения воздуха на рабочем месте соответствуют действующим нормам микроклимата (таблица 5.1).

Таблица 5.1 – Нормы микроклимата помещений с ПК

Период года	Категория работ	Температура воздуха, °С	Относительная влажность воздуха, %	Скорость движения воздуха,
Холодный	Легкая - а	22-24	40-60	0,1
	Легкая - 16	21-23	40-60	0,1
Теплый	Легкая - а Легкая - 16	23-25 22-24	40-60 40-60	0,1 0,2

Выполняемая работа в рабочем помещении относится к категории 1а. Производственная среда, окружающая человека, обеспечивает оптимальные санитарно-гигиенические условия согласно СН 245-71 и устанавливает на одного работающего объем производственного помещения не менее 15 м3, а площадь помещения, которое выгорожено стенами или глухими перегородками составляет порядка 4,5 м2. В данном помещении минимальная площадь составляет порядка 24 м2, а объем производственного помещения составляет порядка 76,8 м3, что удовлетворяет условиям санитарных норм. Для улучшения производственной обстановки помещения необходимо рациональное решение следующих вопросов: изменение цвета в производственном интерьере, освещения, применение кондиционеров, отделки полов и потолков и др.

Микроклимат рабочего помещения оказывает значительное влияние на работника. Отклонение отдельных параметров микроклимата от рекомендованных норм могут снизить работоспособность, ухудшить самочувствие работника и приводят к профессиональным заболеваниям.

К параметрам микроклимата в производственных помещениях относится шум, освещение, кондиционирование.

Шум может нарушать условия труда, оказывая вредное действие на организм человека. Операторы, которые работают в условиях длительного шумового воздействия могут испытывать раздражительность, головные боли, головокружение, снижение памяти, повышенную утомляемость, понижение аппетита, боли в ушах и т. д. Такие нарушения в работе ряда органов и систем организма человека могут вызвать негативные изменения в эмоциональном состоянии человека вплоть до стрессовых. Воздействие шума так же снижает концентрацию внимания, что ведет к нарушению физиологических функций, появляется усталость, нервно-психическое напряжение, ухудшается речь. Все эти факторы снижают работоспособность человека и его производительность, а так-же качество и безопасность труда. Длительное воздействие интенсивного шума (выше 80 дБА) на слух человека приводит к его частичной или полной потере.

В таблице 5.2 указаны безопасные пределы уровня звука в зависимости от категории тяжести и напряженности труда.

Таблица 5.2 – Пределы уровня звука, дБ, на рабочих местах

Категория напряженности труда	Категория тяжести труда			
	I. Легкая	II. Средняя	III. Тяжелая	IV. Очень тяжелая
Мало напряженный	80	80	75	75
Умеренно напряженный	70	70	65	65
Напряженный	60	60	-	-
Очень напряженный	50	50	-	-

Уровень шума на рабочем месте оператора не должен превышать 50дБА, а в залах обработки информации на вычислительных машинах составляет порядка 65дБА. Для снижения уровня шума применяются мероприятия, к которым относится изолирование стен и потолков помещений, где установлены компьютеры, звукопоглощающим материалом. Уровень вибрации в помещениях вычислительных центров может быть снижен при помощи установки оборудования на специальных виброизоляторах.

Естественное освещение на промышленных предприятиях, оказывает большое влияние на зрительную работоспособность, а так же физическое и моральное состояние работников. Освещение в помещении оператора должно состоять из естественного и искусственного, для обеспечения комфортной работы человека с персональным компьютером и оборудованием.

Комбинированное освещение используется если существует недостаток в естественном освещении. Естественное освещение – это освещение при котором в светлое время суток используется одновременно естественный и искусственный свет. Для работы в темное время суток используется преимущественно искусственное освещение, которое создается искусственными источниками света (лампа накаливания, газоразрядные лампы). Применяется из-за отсутствия и недостатка естественного освещения. По назначению бывает: рабочим, аварийным, эвакуационным, охранным, дежурным.При проектировании освещения рабочего места оператора необходимо учитывать такие характеристики, как яркость и контраст фона.

Степень яркости зависит от индивидуальных черт и потребностей оператора. Принимается, что правильная степень освещенности находится в пределах 300-1000 люкс.

При освещении рабочего места оператора большую роль играет контраст между непосредственным полем действия оператора и смежными поверхностями. Слишком малый контраст ухудшает восприятие текста, а слишком большой - вызывает неприятные для глаз отблески. Непосредственное поле зрения оператора должно быть освещено ясно, а смежные поверхности в отношении 3/1. Поддержание рациональной цветовой гаммы достигается правильным выбором осветительных установок, обеспечивающих необходимый световой спектр. В процессе эксплуатации осветительных установок необходимо предусматривать регулярную очистку от загрязнении светильников и остекленных проемов, своевременную замену отработавшей свой срок службы лампы, контроль напряжений питания осветительной сети, регулярную и рациональную окраску стен, потолка, оборудования.

5.3 Расчет искусственного освещения

Для удовлетворения вышеперечисленным требованиям осуществляют расчет по одному из предложенных методов, т. к. помещение еще не оборудовано системой освещения, то воспользуемся методом коэффициента использования.

Исходные данные для расчета:

длина помещения – 6 м;

ширина помещения – 4 м;

высота помещения – 3,2 м;

высота рабочей поверхности h - 0,8 м;

категория зрительной работы – III (высокой точности), E= 300 лк (СНип РК 2.04-05-2002).

Помещение офиса свежепобелено, с окнами без штор, цвет пола – светлый, поэтому соответствующие коэфф. отражения примем равными: рпот=70%; рст = 50%; рпол = 30%.

Для офиса используем люминесцентные лампы ЛБ40 (белого цвета), мощностью 40 Вт, световым потоком 3120 лм, диаметром 40 мм и длиной со штырьками 1213,6 мм. Они имеют высокий срок службы (до 14 000 часов) и оптимальную световую отдачу. При их использовании не происходит утомление зрительных анализаторов, не вызывает слепимости и нарушений функций глаза.

Определим число светильников:

$$N = E \cdot K \cdot S \cdot Z / n \cdot \Phi \cdot n \qquad (5.1)$$

где E - заданная минимальная освещенность светильника. Для персонала работающего с ЭВМ E = 300 лк;

K - коэффициент запаса, учитывающий запыление и износ источников света в процессе эксплуатации. K = 1,5;

S – освещаемая площадь, S = 4 · 6 = 24 м2;

K - коэффициент неравномерности освещения, = 1,1 1,2;

N - коэффициент использования;

Ф – световой поток одной лампы, ФЛ = 3000 лм.

n– число ламп в светильнике, n=1.

$$N = E \cdot K \cdot S \cdot Z / \Phi \cdot n = 300 \cdot 1.5 \cdot 24 \cdot 1,1 \cdot 3000 \cdot 0,74 = 6 \text{ шт}$$

Определим оптимальное расстояние между светильниками по ширине:

$$Z = \lambda \cdot h, \text{ m} \qquad (5.2)$$

λ - где выбирается как в диапазоне от 1 до 1,4;

$$h = H - h_p = 3,2 - 0,8 = 2,4\text{м}$$

По этим данным находим, что оптимальное расстояние между светильниками равно:

$$Z = \lambda \cdot h = 1 \cdot 2,4 = 2,4\text{м}$$

Рассчитаем число рядов светильников по ширине:

где B – ширина помещения, B = 4 м;

Z – расстояние между светильниками, Z = 2,4 м.

Следовательно, светильники располагаются в два ряда по ширине. Рассчитаем число рядов светильников по длине:

Z – расстояние между светильниками, Z = 2,4 м.

Следовательно, светильники располагаются в три ряда по длине.

Оптимальное расстояние l от крайнего ряда светильников вдоль до стены рекомендуется принимать равным Z/4, следовательно, расстояние l = 0,6м, а по ширине равным Z/3 =0,8м.

Таким образом, необходимо 6 светильников расположенных в два ряда, в каждом ряду по три светильника, в каждом светильнике по две лампы.

По размерам помещения S = A·B и высоте подвеса h_p светильника определяем показатель помещения i:

$$S_i = 6 \cdot 4 \cdot h_p \cdot (a + b) = 24 / 3{,}2 \cdot (6 + 4) = 32{,}75$$

Показатель помещения 0,75 соответствует коэффициенту использования светового потока светильников выбранного типа с люминесцентными лампами η=74%. Наиболее оптимальный вариант расположения светильников представлен на рисунке 5.3, где расстояние между светильниками по ширине рассчитывается исходя из габаритов выбранных ламп и рассчитанного расстояния между ними[14].

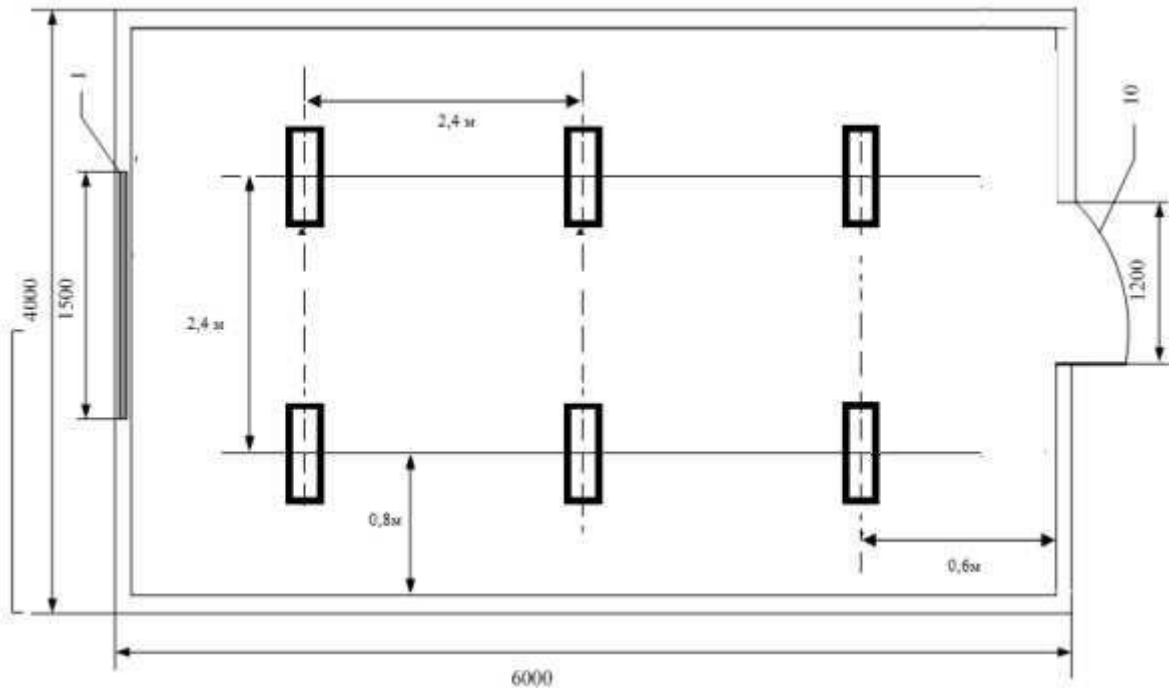


Рисунок 5.3 – Схема размещения светильников

5.4 Выводы по разделу БЖД

В ходе выполнения дипломного проекта по разработке комплекса лабораторных работ на тему «Исследование уязвимостей серверов» были рассмотрены вопросы реализации атак на серверное ПО такие как: FTP, SSH и MSSQL – сервера, с использованием операционной системы Kali Linux.

В соответствии теме дипломного проекта был произведен анализ условий труда при организации комплекса лабораторных работ, который включает в себя определение основных требований к микроклимату, шуму и вибрации в помещении, где расположено серверное оборудование. Был произведен расчет искусственного освещения в помещении. В результате чего

для обеспечения нормируемого освещения при $E_н$ = 300 лк требуется 6 ламп типа ЛБ40 (белого цвета).

В Санитарных нормах и правилах – СанПиН 2.2.2.542-96 даются общие требования к организации и оборудованию рабочих мест с персонально электронно-вычислительной машины ПЭВМ.

Заключение

В дипломной работе выполнены исследования, которые использованы при разработке эффективных САОРИБ по предложенной методологии синтеза, основанной на созданных в работе методах и составленной модели КМР риска. В ходе решения поставленных задач были получены следующие результаты:

1) На основании проведенного анализа САОР и его базовых понятий, разработана кортежная модель базовых характеристик риска, которая за счет обобщения базовых характеристик, отображенных шестикомпонентным кортежем, позволяет формировать необходимые множества данных для обеспечения гибкости и требуемой функциональности разрабатываемых САОР.

2) Предложены методы анализа и оценивания рисков ИБ, которые на основе использования обобщенной модели КМР и логико-лингвистического подхода, позволяют создавать соответствующие средства оценивания с интегрированными возможностями, использующие в качестве входных данных динамически изменяемые наборы детерминированных и нечетко определенных базовых характеристик с учетом периода времени, отрасли, экономической и управленческой специфики объекта защиты и др.

3) Разработаны методы реализации функции n-кратного инкрементирования числа термов с использованием первого и второго частного расширения базы, в котором за счет модификации n-кратным расширением функции инкрементирования термов на один порядок, расширяется возможность формализации процесса эквивалентного трансформирования числа эталонных термов ЛП на n порядков без привлечения экспертов соответствующей предметной области.

4) Получила дальнейшее развитие методология синтеза САОР, которая позволила, за счет формализации и обобщения процесса использования сформированной модели характеристик и предложенных методов, детерминировать процесс построения инструментальных средств с гибкими возможностями использования заданных множеств величин при анализе и оценивание рисков ИБ.

5) Разработаны структуры систем САОР, которые за счет подсистем обработки базовых характеристик и формирования данных, реализующих предложенные FirstM методы, позволяют преобразовать и формировать данные, как в качественной, так и в количественной интерпретации.

Список сокращение

АС – автоматизированная система;
ЗИ – защита информации;
ИА – информационный актив;
ИБ – информационная безопасность;
ИР – информационные ресурсы;
ИС – информационная система;
ИТ – информационные технологии;
КЛ – количественная;
КМР - кортежная модель базовых характеристик риска;
КЧ – качественная;
КЭС – комплексная экспертная система;
ЛП – лингвистическая переменная;
НАО – нечеткие арифметические операции;
НД – нарушение доступности;
НК – нарушение конфиденциальности;
НМ – нечеткое множество;
НСД – несанкционированный доступ;
НСМ – несанкционированная модификация;
НЦ – нарушение целостности;
НЧ – нечеткие числа;
ОР – оценка риска;
ОУ – оценка угрозы;
ПК – персональный компьютер;
ПО – программное обеспечение;
ПС – программные средства;
ПП – проект пользователей;
РИС – ресурс информационной системы;
РП – рискообразующий потенциал;
САОР – средства анализа и оценивание рисков;
СЗИ – система защиты информации;
СМИБ – система менеджмента информационной безопасности;
ТВ – тематический вопросник;
УБХ – уровень базовой характеристики;
УР – уровень риска;
ФП – функция принадлежности;
ЦО – целевые объекты.

Список использованной литературы

1 Peltier T.R. Information security risk analysis – London: Auerbach Publications, 2001. – 281 p.

2 Информационная технология. Методы защиты. Менеджмент рисков информационной безопасности: BS ISO/IEC 27005:2008. – Киев: 2011. – 70 с.

3 ГОСТ Р ИСО/МЭК 13335-1 – 2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий: – Введ. 2007.05.31. – М.: ИПК «Издательство стандартов», 2007. – ч.1. 23 с.

4 Smith M. Commonsense Computer Security, your practical guide to information security / M. Smith // London: McGraw – Hill, 1993 – 105 p.

5 Rowe W. An anatomy of risk. / W. Rowe – NY/: John Wiley, 1997. – 488 p.

6 Information technology, Security techniques, Code of practice for information security management: ISO/IEC 27002:2005 // International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2005. – 171 p.

7 Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013 // International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2013. – 34 p.

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

9 Симонов С. В. Технологии и инструментарий для управления рисками //Информационный бюллетень JetInfo. – 2003. – № 2 (117) – С. 3 – 32.

10 Ахметов Б.Б. Использование аппарата нечеткой логики для оценки риска информационной безопасности вуза // Поиск. Серия технических и естественных наук, 2009. – №3. – С.235-240.

11 ГОСТ Р ИСО/МЭК 15026 – 2002. Информационная технология. Уровни целостности систем и программных средств: Введ. 2003.06.30. – М.: ИПК “Издательство стандартов”, 2003. – 15 с.

12 ГОСТ Р 51897–2002. Менеджмент риска. Термины и определения: – Введ. 2001.05.31. – М.: ИПК «Издательство стандартов», 2002. – 8 с.

13 Risk analysis based on IT-Grundschutz: BSI-Standard 100-3 – Boon: Bundesamtfür Sicherheit in der Information stechnik, 2008. – 23 p.

14 MEHARI – Overview / Club de la Securit ´ e de l’Information Franc¸ais – Paris: CLUSIF, 2010 – 50 p.

15 MAGERIT – version 2. Methodology for Information Systems Risk Analysis and Management. Book I –The Method / [version 2]. – Madrid: Ministerio de administra cionespúblicas, 2006. – 140 p.

16 International standard Risk management. Principles and guidelines: ISO/FDIS 31000:2009(E) / International Organization for Standardization // JISC – 2009. – 24 p.

17 Ахметов Б.С., Корченко А.Г., Казмирчук С.В., Жекамбаева М.Н. Система оценивания рисков на базе метода FirstM //Сборник статей XV Международной научно-технической конференции «Проблемы информатикив образовании, управлении, экономике и технике». – Пенза: Приволжский дом знаний. – 2015. – 105-110 с.

18 Мушик Э., Мюллер П. Методы принятия технических решений. – М.: Мир, 1990. – 206 с.

19 Peltier T.R. Information security risk analysis – London: Auerbach Publications, 2001. – 281 p.

20 Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft: учебный курс. – Санкт-Петербург: Издательство «INTUIT», 2009. – 136 с.

Приложение А

Фрагмент текста программной системы САОР ИБ

```
#include <vcl.h>
#pragma hdrstop

#include "Unit1.h"
#include "Unit2.h"
//---------------------------------------------------------------------------
#pragma package(smart_init)
#pragma link "dxdbtree"
#pragma link "dxtree"
#pragma resource "*.dfm"
TForm1 *Form1;
//---------------------------------------------------------------------------
__fastcall TForm1::TForm1(TComponent* Owner)
        : TForm(Owner)
{
}
//---------------------------------------------------------------------------
void __fastcall TForm1::RadioGroup1Click(TObject *Sender)
{
if (RadioGroup1->ItemIndex == 0)
        {
        Edit1->Visible = true;
        ComboBox1->Visible = false;
        }

if (RadioGroup1->ItemIndex == 1)
        {
        Edit1->Visible = false;
        ComboBox1->Visible = true;
        }
}
//---------------------------------------------------------------------------
void __fastcall TForm1::Button1Click(TObject *Sender)
{
if (RadioGroup1->ItemIndex == 0)
        {
                if (Edit1->Text != "")
                        {
                        ADOQuery1->Close();
```

```
                    ADOQuery1->SQL->Clear();
                    AnsiStringtn = "CREATE TABLE " + Edit1->Text + "(id int
AUTO_INCREMENT PRIMARY KEY, resource varchar(200) NOT NULL, threat
varchar(200) NOT NULL, probability int(5) NOT NULL, frequency decimal(4,2)
NOT NULL, loss decimal(4,2) NOT NULL, danger int(5) NOT NULL, dr
decimal(4,2))";
                    ADOQuery1->SQL->Add(tn);
                    ADOQuery1->ExecSQL();

                    ADOQuery2->Close();
                    ADOQuery2->SQL->Clear();
                    tn = "CREATE TABLE " + Edit1->Text + "(id int
AUTO_INCREMENT PRIMARY KEY, resource varchar(200) NOT NULL, risk
decimal(4,2) NOT NULL, lpvarchar(100))";
                    ADOQuery2->SQL->Add(tn);
                    ADOQuery2->ExecSQL();

                    Hide();
                    Application->CreateForm(__classid(TForm2), &Form2);
                    Form2->Label1->Caption = Form2->Label1->Caption +
Edit1->Text;
                    Form2->Label2->Caption = Edit1->Text;
                    Form2->ShowModal();
                    Close();
                    }
                else
                    {
                    ShowMessage("Введитеимяпроекта");
                    }
        }

    if (RadioGroup1->ItemIndex == 1)
        {
            if (ComboBox1->ItemIndex != -1 )
                {
                Form2->ADOQuery1->Close();
                Form2->ADOQuery1->SQL->Clear();
                AnsiStringtn = "select * from " + ComboBox1->Text;
                Form2->ADOQuery1->SQL->Add(tn);
                Form2->ADOQuery1->Open();
```

```
                    Hide();
                    Application->CreateForm(__classid(TForm2), &Form2);
                    Form2->Label1->Caption = Form2->Label1->Caption +
ComboBox1->Text;
                    Form2->Label2->Caption = ComboBox1->Text;
                    Form2->ShowModal();
                    Close();
                    }
          }
     }
     //---------------------------------------------------------------------------
     void __fastcall TForm1::FormShow(TObject *Sender)
     {
     Form2->ADOres->GetTableNames(ComboBox1->Items, false);
     }
     //---------------------------------------------------------------------------
```