ФГБОУ ВПО «Воронежский государственный
технический университет»

Кафедра систем информационной безопасности

256-2015

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к курсовой работе по дисциплине
«Математические основы управления рисками»
для студентов специальности
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Воронеж 2015

Составитель д-р техн. наук О. Н. Чопоров

УДК 004.056

Методические указания к курсовой работе по дисциплине «Математические основы управления рисками» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. О. Н. Чопоров. Воронеж, 2015. 36 с.

В данных методических указаниях приведены краткие теоретические сведения и задание для выполнения курсовой работы по дисциплине «Математические основы управления рисками». Издание предполагает углубленное изучение лекционного материала и приобретение навыков по разработке системы менеджмента информационной безопасности предприятия и использованию различных методов принятия решений для выбора адекватных мер контроля и управления, направленных на снижение риска.

Методические указания подготовлены в электронном виде в текстовом редакторе MS Word 2007 и содержатся в файле Чопоров_КР_МОУР.pdf.

Табл. 8. Ил. 1. Библиогр.: 22 назв.

Рецензент д-р техн. наук, проф. А.Г. Остапенко

Ответственный за выпуск зав. кафедрой д-р техн. наук, проф. А.Г. Остапенко

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

ВВЕДЕНИЕ

Управление рисками нарушения информационной безопасности является одним из базовых составляющих системы менеджмента информационной безопасности. Данному вопросу посвящен ряд отечественных и зарубежных публикаций [2, 3, 5, 12-19, 21-22], а также стандартов ИСО, среди которых ГОСТ Р ИСО 31000–2010 «Менеджмент риска. Принципы и руководство» [6], ГОСТ Р ИСО 31010–2011 «Менеджмент риска. Методы оценки риска» [7], ГОСТ Р ИСО/МЭК 27000–2012 «Информационная технология «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» [8], ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [9], ГОСТ Р ИСО/МЭК 27002–2012 «Информационная технология «Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [10], ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология «Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [11].

В данных стандартах рассматриваются общие вопросы управления рисками в целом и менеджмента риска информационной безопасности. Однако, отсутствуют конкретные рекомендации для использования в реальной практике. Недостаточно представлен вопрос оценки рисков и выбора адекватных мер контроля и управления. Достаточно эффективным при решении данной задачи является использование математических методов и моделей, в частности, элементов теории принятия решений и оптимизации.

Данная курсовая предлагает самостоятельную разработку системы менеджмента риска информационной безопасности в соответствии со стандартом ГОСТ Р ИСО/МЭК

27005–2010 и использованием различных методов принятия решений и оптимизационных моделей при выборе адекватных мер контроля и управления направленных на снижение информационных рисков.

Данные методические указания по написанию курсовой работы содержат теоретические сведения, задание, требования к работе, а также сроки ее выполнения.

1. ЦЕЛИ И ЗАДАЧИ КУРСОВОЙ РАБОТЫ

Целью курсовой работы является разработка, на примере выбранного предприятия, системы управления информационными рисками (в соответствии со стандартом ГОСТ Р ИСО/МЭК 27005-2010), построении математической модели выбора эффективных защитных мероприятий, направленных на снижение риска информационной безопасности.

При выполнении курсовой работы студенты должны изучить современные стандарты в области менеджмента риска информационной безопасности, основные этапы процесса менеджмента риска информационной безопасности, разновидности активов предприятия, типовые угрозы, уязвимости и способы их описания, методику построения реестра рисков информационной безопасности, методы принятия решений при управлении информационными рисками в детерминированных системах, условиях неопределенности и наличия противоборствующей стороны.

Практическая часть курсовой работы ориентирована на разработку системы менеджмента рисков информационной безопасности предприятия, разработку математических моделей выбора оптимальных мер контроля и управления на этапе снижения риска.

Студентам рекомендуется использовать современные инструментальные средства при создании моделей и алгоритма управления рисками, и подготовке отчета в частности, текстовый редактор MS Word, электронные таблицы MS Excel, систему MATCAD.

2. ТРЕБОВАНИЯ К СОДЕРЖАНИЮ И ОБЪЁМУ КУРСОВОЙ РАБОТЫ

Основные требования к курсовой работе (КР) установлены стандартом предприятия СТП ВГТУ 62-2007. КР состоит из расчетно-пояснительной записки (РПЗ) объёмом от 30 до 50 страниц печатного текста с иллюстративным графическим материалом, размещенным по разделам работы.

Пояснительная записка содержит следующие разделы:

а) титульный лист;

б) задание на курсовую работу;

в) лист «Замечания руководителя»;

г) содержание включает введение, наименование всех разделов, подразделов, пунктов (если они имеют наименование), заключение, список литературы, наименование приложений с указанием номеров страниц, с которых начинаются эти элементы пояснительной записки;

д) введение;

е) основную часть (исследовательскую) содержащую:

- описание организации (установление контекста);
- реестр активов;
- методику анализа и оценки рисков;
- реестр рисков;
- реестр мер контроля и управления;
- описание методики обработки и принятия рисков;
- реализацию одного из методов принятия решений или оптимизационную модель для выбора мер и средств контроля и управления;
- контрольные примеры.

ж) заключение;

з) список литературы;

и) приложения (при необходимости).

Также к КР прилагается диск с электронным вариантом курсовой работы.

2.1. График выполнения курсовой работы

Таблица 1

График выполнения курсовой работы

Срок выполнения	Содержание работы
1 – 2-я недели семестра	Выбор задания курсовой работы. Ознакомление с постановкой задачи
3 – 8-я недели семестра	Осмысление задания, изучение подхода к его выполнению, разработка системы управления информационными рисками (в соответствии со стандартом ГОСТ Р ИСО/МЭК 27005-2010).
9 – 12-я недели семестра	Реализация одного из методов принятия решений или оптимизационную модель для выбора мер и средств контроля и управления
13 – 16-я недели семестра	Разработка примеров решения задачи выбора. Оформление пояснительной записки.
17 – 18-я недели семестра	Сдача пояснительной записки. Защита курсовой работы

2.2. Последовательность выполнения

Последовательность выполнения, рекомендации по выполнению разделов проекта:

1. Содержательный анализ задачи.

2. Изучить стандарт ГОСТ Р ИСО/МЭК 27005-2010.

3. Разработать систему управления информационными рисками.

3.1. Дать описание организации (области применения и границ процесса менеджмента риска ИБ) в соответствии с приложением А ГОСТ Р ИСО/МЭК 27005-2010.

3.2. Определить основные критерии, необходимые для менеджмента риска ИБ (критерии оценки риска, критерии влияния, критерии принятия риска).

3.3. Разработать реестр информационных активов организации.

3.4. Определить требования безопасности для активов (законодательные и нормативные требования, контрактные обязательства, требования бизнеса).

3.5. Разработать шкалу для определения ценности активов.

3.6. Идентифицировать угрозы, предложить шкалу для их оценки.

3.7. Описать профиль и жизненный цикл для одной из угроз.

3.8. Составить список идентифицированных угроз, затрагиваемых ими активов или групп активов и мер вероятности того, что угроза произойдет (на основ разработанной шкалы).

3.9. Составить список уязвимостей, связанных с идентифицированными угрозами, предложить шкалу для оценки уязвимостей.

3.10. Предложить шкалу для оценки величины рисков.

3.11. Составить реестр информационных рисков.

3.12. Сформировать перечень мер контроля и управления, направленных на снижение информационных рисков.

3.13. Привести примеры расчетов ценности активов, уровня угроз, уязвимостей, эффективности мер контроля и управления с использованием экспертных оценок, обработанных с использованием соответствующих методов.

3.14. Описать методику обработки и принятия рисков.

4. Реализовать один из методов принятия решений или оптимизационную модель для выбора мер и средств контроля и управления.

5. Разработать пример решения задачи выбора.

6. Оформить отчет по курсовой работе.

2.3. Критерии оценки курсовой работы

Оценка за курсовую работу складывается из оценки за предоставленный отчет, полноту выполненной работы, защиту (ответы на вопросы по теме проекта) и составляет от 2 до 5 («неудовлетворительно», «удовлетворительно», «хорошо», «отлично»).

3. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Согласно ***ГОСТ Р ИСО/МЭК 27005–2010*** «Информационная технология «Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [11], процесс менеджмента риска ИБ состоит из установления контекста, оценки риска, обработки риска, принятия риска, коммуникаций риска, а также мониторинга и переоценки риска ИБ (рисунок) [14, 15].

Установление контекста включает определение основных критериев, необходимых для менеджмента риска ИБ, определение области применения и границ, а также создание соответствующей организационной структуры, занимающейся менеджментом риска ИБ. Подробная информация об определении области применения и границ процесса менеджмента риска ИБ приведена в приложении А ГОСТ Р ИСО/МЭК 27005-2010.

Процесс ***оценки риска*** состоит из: ***анализа риска,*** включающего идентификацию риска и установление значения риска, и оценивания риска.

Идентификация риска представляет собой процесс нахождения, составления перечня и описания элементов риска и включает следующие этапы:

1) определение (идентификация) активов;

2) определение угроз;

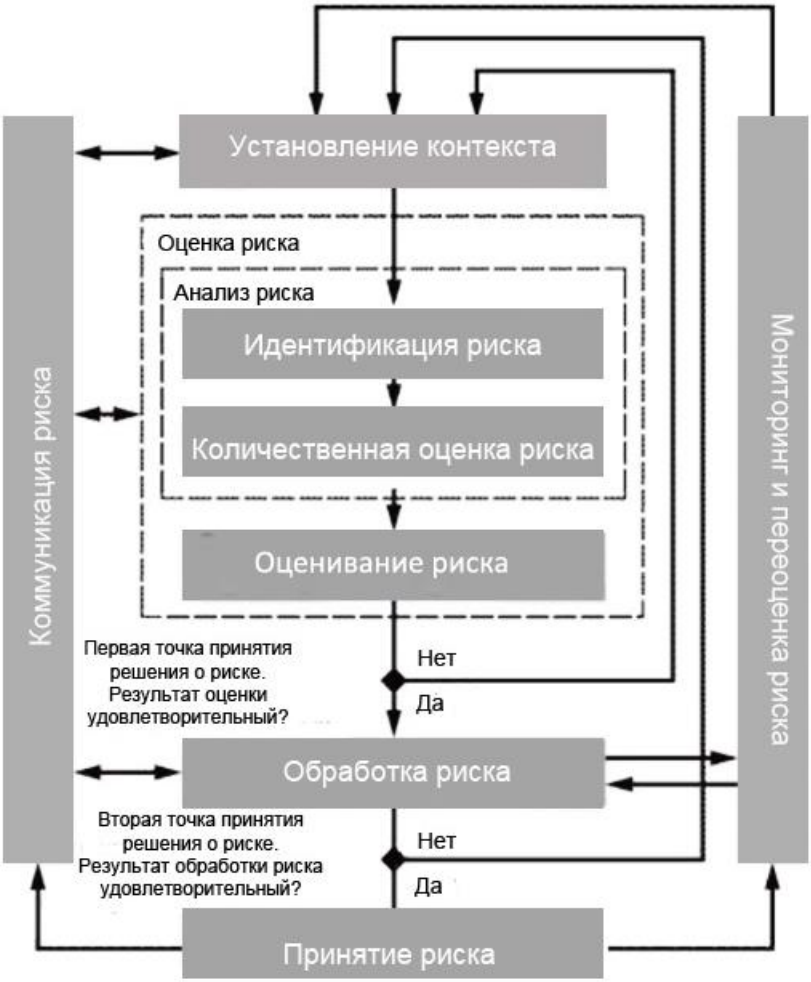
3) определение существующих мер и средств контроля и управления;

4) выявление уязвимостей;

5) определение последствий.

Идентификация активов включает в себя: формирование модели бизнес-процессов (табл. 2); инвентаризацию активов; формирование реестра активов (табл. 3); определение взаимосвязей между реестрами активов; построение модели активов; определение владельцев активов и их обязанностей; делегирование обязанностей по обеспечению безопасности

активов; классификацию и категорирование активов; определение правил допустимого использования активов [2, 5, 14].



Процесс менеджмента риска информационной безопасности

Таблица 2

Описание бизнес-процессов и классификация информационных ресурсов

Название (информационного ресурса или группы ресурсов)	**Назначение** (краткое описание для чего используется)	**Размещение** (помещения, оборудование, носители информации)	**Приложения и сервисы**	**Пользователи и владельцы**	**Критичность** (конфиденциальность, целостность, доступность)

Подробная информация об определении и установлении ценности активов и оценке влияния приведена в приложении В ГОСТ Р ИСО/МЭК 27005-2010.

Для каждого информационного актива или группы активов определяется список угроз в отношении конфиденциальности, целостности и доступности. Подробный перечень примерных типичных угроз безопасности, рассматриваемых при оценке информационных рисков, приведен в приложении С ГОСТ Р ИСО/МЭК 27005-2010. По завершении оценки угроз составляется список идентифицированных угроз, затрагиваемых ими активов или групп активов и меры вероятности того, что угроза произойдет (табл. 4).

На третьем этапе должен быть определен перечень всех существующих и планируемых мер и средств контроля и управления, их нахождение и состояние использования.

Выявление уязвимостей включает выявление слабых мест, которые могут быть использованы источником угрозы для причинения вреда активам. Примеры уязвимостей и методы их оценки приведены в приложении D ГОСТ Р ИСО/МЭК 27005-2010.

Таблица 3

Пример реестра информационных активов компании

Реестр информационных ресурсов Компании

Конфиденциально

Дата последнего изменения 06.02.2015 г. Ценность ресурса: ОН - очень низкая, Н - низкая, С - средняя, В - высокая, ОВ - очень высокая

Категория	**Название**	**Описание**	**Размещение**	**Использование (бизнес-процессы)**	**Формат**	**Конфиденциальность**	**Целостность**	**Доступность**	**Максимальные период недоступности**	**Сервисы, приложения**	**Владелец**
Веб-сайты	Корпоративный сайт Компании	http:/ компания.ru	Офисная сеть	Представительство компании в сети Интернет		-	Н	Н	1 день		ИТ
	Сайт проекта X	http:/ проект 1.ru	ЦОД	Представительство проекта в сети Интернет, коммуникации с клиентами и партнерами		-	С	С	1 час		ИТ
	Сайт проекта Y	http:/ проект2.т	ЦОД	Представительство проекта в сети Интернет, коммуникации с клиентами и партнерами		-	Н	С	1 час		ИТ
Данные по клиентам и партнерам	Коммерческие предложения		Файловый сервер	Работа с клиентами	doc	Н	-	-	1 неделя		Департамент продаж
	Электронные сообщения	Входящая и исходящая электронная почта сотрудников	Файловый сервер	Внутренние и внешние коммуникации		В	-	С	3 часа		Все
	Презентации	Презентации для клиентов и партнеров	Файловый сервер	Привлечение новых клиентов и партнеров	ppt	L	-	-	2 недели		Департамент продаж

Таблица 4

Результаты оценки угроз и уязвимостей (фрагмент)

№	Группы угроз	Уязвимости	Вероятность угроз	Уровень уязвимости	Механизмы контроля
1	НСД к ресурсам ЛВС компании со стороны внутренних злоумышленников. Маскарад, использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификационной информации	Слабые пароли, отсутствие парольной политики. Наличие внутренних уязвимостей, обусловленных несвоевременным обновлением ОС, Мониторинг действий пользователей не производится	C	B	Корректное управление доступом. Низкая квалификация пользователей для осуществления НСД
2	НСД к ресурсам ЛВС компании со стороны внешних злоумышленников. Маскарад, использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификациионной информации	Отсутствуют последние обновления на корпоративном файерволле. Единственный защитный барьер. Наличие внутренних уязвимостей, обусловленных несвоевременным обновлением ОС. Отсутствие системы обнаружения вторжений (IDS)	B	C	Хорошая защита периметра. Отсутствие известных уязвимостей

Перед оценкой риска должны быть определены последствия для активов, вызванные потерей конфиденциальности, целостности и доступности. В результате формируется перечень сценариев инцидентов с их последствиями, связанными с активами и бизнес-процессами [2, 14] (табл. 5).

Перечень критериев для оценки возможного ущерба в результате осуществления угроз в отношении активов может выглядеть следующим образом:

У1 – ущерб коммерческим интересам партнеров и третьих лиц;

У2 – санкции со стороны правоохранительных и регулирующих органов (штрафы, административная и уголовная ответственность)

У3 – ущерб коммерческим интересам организации;

У4 – финансовые потерн;

У5 – ущерб репутации организации;

У6 – дезорганизация деятельности, ухудшение морального климата в коллективе, снижение эффективности работы.

Анализ риска может быть выполнен с различной степенью детализации в зависимости от критичности активов, распространенности известных уязвимостей и прежних инцидентов, касавшихся организации.

Методология ***установления значения риска*** может быть качественной, количественной или комбинированной, в зависимости от обстоятельств. Форма анализа должна согласовываться с критериями оценки риска, разработанными как часть установления контекста.

Для установления качественного значения используется шкала квалификации атрибутов, с помощью которой описываются величины возможных последствий (например, «низкий», «средний» и «высокий») и вероятности возникновения этих последствий.

Для установления количественной оценки используется шкала с числовыми значениями как последствий, так и вероятности, с применением данных из различных источников (табл. 6).

Таблица 5

Оценка величины возможного ущерба и ценности активов

Название актива	**Последствие угрозы**	**Требование безопасности**	**Тип ущерба**	**Ценность актива (величина ущерба)**	**Примечание (описание возможных последствий угрозы и ущерба)**
Корпоративный веб-сайт	К		–	–	
	Ц		У5	1	Незначительные затруднения в установлении отношений с новыми партнерами
	Д		У5	0	Посещаемость сайта незначительна
Сайт проекта Х	К		–	–	
	Ц		У5	3	Существенный ущерб имиджу компании, потеря доверия со стороны значительной части клиентов
	д		У5	3	Невозможность получения информации клиентами При недоступности сайта более 1 часа, репутации компании может быть нанесен серьезный ущерб
Персональные данные клиентов	к		У2.У5	3	В случае несанкционированного раскрытия информации из базы персональных данных возможна потеря значительной части клиентов
	ц		У2	2	Возможен срыв маркетинговых мероприятий в случае несанкционированного изменения персональных данных клиентов (email, почтовый адрес, SMS)
			У6	3	В случае недоступности базы персональных данных более 1 дня

Примечание: последствия угрозы оцениваются с точки зрения утраты конфиденциальности (К), целостности (Ц) и доступности (Д) актива; среди требований безопасности выделяют законодательные и нормативные требования (Т1), контрактные обязательства (Т2), требования бизнеса (Т3).

Таблица 6

Матрица с величиной рисков

Стоимость ресурса	**Уровень угрозы**								
	Низкий			**Средний**			**Высокий**		
	Уровень уязвимости								
	Н	**С**	**В**	**Н**	**С**	**В**	**Н**	**С**	**В**
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
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

Различные методы оценки риска приведены в ГОСТ Р ИСО 31010–2011 «Менеджмент риска. Методы оценки риска» [7], а также рассматриваются в ряде работ [3, 12, 13, 16-19, 21, 22]. В результате формируется *Реестр информационных рисков* – основной документ, описывающий текущую ситуацию с рисками в организации [2, 14] (табл. 7).

На этапе ***оценивания рисков*** выполняется сравнение установленных значений рисков с критериями оценки риска, выбранными на этапе установления контекста. В результате получается перечень рисков с назначенными приоритетами в соответствии с критериями оценки рисков, касающимися сценариев инцидентов, которые приводят к этим рискам.

Целью **обработки рисков** является их уменьшение до приемлемого уровня путем уменьшения вероятности инцидента, либо минимизации возможного ущерба.

Для обработки риска имеется четыре варианта: 1) снижение риска, 2) сохранение риска, 3) предотвращение риска и 4) перенос риска [2, 11, 14, 15]. Варианты обработки риска должны выбираться исходя из результатов оценки риска, предполагаемой стоимости реализации этих вариантов и их ожидаемой эффективности.

Таблица 7

Реестр информационных рисков

№	Группы угроз	Уязвимости	Активы	Вероятность угроз	Уровень уязвимости	Ценность актива	Уровень риска	Механизмы контроля
Риски офисной сети. Физические риски								
1	Кража компьютерного оборудования и носителей информации инсайдерами. Физический НСД помещении организации. кабинеты и серверные комнаты, к оборудованию, бумажным документам запоминающим устройствам, носителям информации и т. п.	Не производится регистрация оборудования и информационных носителей, выносимых за пределы территории организации. Отсутствуют правила работы в зонах безопасности. При приеме на работу не производится проверка истории кандидатов	Корпоративный веб-сайт	М	М	0	2	Средний уровень лояльности сотрудников. Существует политика безопасности в отношении мобильных носителей информации и использования внешних устройств. Существует политика возврата оборудования, носителей информации и документации при увольнении сотрудников. Для доступа на территорию ортаизации используются смарт-карты. Территория охраняется службой безопасности. Офисное оборудование и документация находится строго в зонах безопасности

Снижение риска – действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском. Уменьшить риски можно следующими способами: уменьшением вероятности воздействия угрозы на активы; ликвидацией имеющихся уязвимостей; уменьшением вероятности использования уязвимости; уменьшением возможного ущерба в случае осуществления риска путем обнаружения нежелательных событий, реагирования и восстановления после них.

Более подробная информация об ограничениях, сопутствующих решениям по снижению риска, приведена в приложении F ГОСТ Р ИСО/МЭК 27005-2010 [11], а в ГОСТ Р ИСО/МЭК 27002-2012 дается подробная информация по выбору мер и средств контроля и управления [10].

Сохранение риска – принятие бремени потерь или выгод от конкретного риска. Основными факторами, влияющими на решение о принятии рисков, являются: возможные последствия осуществления риска, то есть расходы организации в каждом случае, когда это происходит; ожидаемая частота подобных событий.Если уровень риска соответствует критериям принятия риска, то нет необходимости реализовывать дополнительные меры и средства контроля и управления, и риск может быть сохранен.

Предотвращение риска – решение не быть вовлеченным в рискованную ситуацию или действие, предупреждающее вовлечение в нее. Если идентифицированные риски считаются слишком высокими или расходы на реализацию других вариантов обработки риска превышают выгоду, может быть принято решение о полном предотвращении риска путем отказа от планируемой или существующей деятельности, или их совокупности, или изменения условий, при которых осуществляется деятельность.

Перенос риска – разделение с другой стороной бремени потерь или выгод от риска. Риск должен быть перенесен на сторону, которая может наиболее эффективно осуществлять менеджмент конкретного риска, в зависимости от оценки

риска. Перенос может быть осуществлен путем страхования, которое будет поддерживать последствия, или путем заключения договора субподряда с партнером, чья роль будет заключаться в проведении мониторинга информационной системы и осуществлении незамедлительных действий по прекращению атаки, прежде чем она приведет к определенному уровню ущерба.

После того как решения по обработке рисков были приняты, должны быть определены и спланированы действия по реализации этих решений. Каждое мероприятие должно быть четко определено и разбито на такое количество действий, которое необходимо для четкого распределения ответственности между исполнителями, оценки требований к выделению ресурсов, установки вех и контрольных точек, определения критериев достижения целей и мониторинга продвижения. Решения руководства по обработке рисков оформляются в виде «Плана обработки рисков» [2, 14] (табл. 8). Этот документ является производным от «Реестра информационных рисков», определяющим для каждой группы угроз и уязвимостей перечень мер по обработке риска, позволяющих уменьшить максимальный для данной группы угроз уровень риска до уровня остаточного риска, приемлемого для организации. План обработки рисков также определяет сроки реализации, выделяемые ресурсы и ответственных исполнителей.

На этапе ***принятия риска информационной безопасности*** должно быть принято решение о принятии рисков и установлена ответственность за это решение, что должно быть официально зарегистрировано. Критерии принятия риска устанавливаются на этапе анализа контекста.

Коммуникация риска представляет собой деятельность, связанную с достижением соглашения о том, как осуществлять менеджмент риска путем обмена и/или совместного использования информации о риске лицами, принимающими решения, и другими причастными сторонами. Информация включает в себя наличие, характер, форму, вероятность, серьезность, обработку и приемлемость рисков.

Таблица 8

План обработки рисков (фрагмент)

№	Угрозы	Уязвимости	Максимальный уровень риска	Меры по обработке риска	Остаточный уровень риска	Дата	Комментарии, ресурсы, ответственные
Обработка рисков офисной сети Физические риски							
1	Кража компьютерного оборудования и носителей информации инсайдерами Физический НСД в помещении организации, а кабинеты и серверные комнаты, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и т. п.	Не производится регистрация оборудования и информационных носителей, выносимых за пределы территории организации. Отсутствуют правила работы в зонах безопасности. При приеме на работу не производится проверка истории кандидатов	5	Разработать систему мер, ограничивающих неконтролируемое использование внешних носителей и мобильных устройств вне офиса. Реализовать меры по проверке кредитной истории кандидатов для критичных должностей. Разработать правила работы в зонах безопасности.	4		

Риски не являются статичными. Угрозы, уязвимости, вероятность или последствия могут изменяться неожиданно, без каких-либо признаков изменений. Поэтому необходим непрерывный ***мониторинг и переоценка рисков и их факторов*** (т.е. ценность активов, влияние, угрозы, уязвимости, вероятность возникновения) с целью определения любых изменений в контексте организации на ранней стадии, и должно поддерживаться общее представление о всей картине риска.

Подробная информация о методике управления рисками информационной безопасности с подробными комментариями, примерами шкал для оценки активов, угроз, уязвимостей и рисков, а также примерами отчетных документов, включая реестр активов, реестр рисков, план обработки рисков, приведена в учебном пособии [14].

На этапе обработки рисков основной задачей является выбор мер и средств контроля и управления из множества имеющихся альтернатив. Для решения данной задачи целесообразно использовать элементы теории принятия решений. Одним из наиболее распространенных, простых, универсальных и доступных являются методы экспертных оценок.

К наиболее распространенным методам измерений при экспертизе относятся ранжирование, непосредственная оценка, парное сравнение [14].

Задачи многокритериального принятия решений при определенности могут быть решены за счет перехода к однокритериальным задачам оптимизации на основе принципов оптимальности. Полученные таким образом задачи можно решать однокритериальными методами оптимизации.

На начальной стадии решения задачи в целях уменьшения исходного множества решений используется принцип оптимальности по Парето. Решение (альтернативу) называют оптимальным по Парето, если невозможно улучшить (увеличить) решение ни по одному из критериев без ухудшения

(уменьшения) решения хотя бы по одному из критериев. Парето-оптимальные решения (альтернативы) составляют множество Парето (множество компромиссов).

Для выбора одного оптимального решения используются следующие принципы оптимальности: принцип идеальной точки; принцип антиидеальной точки; принцип равенства; принцип квазиравенства; принцип максимина; принцип последовательного максимина; квазиоптимальный принцип последовательного максимина; принцип абсолютной уступки; принцип относительной уступки; принцип главного критерия; лексикографический принцип; лексикографический принцип квазиоптимальности [14].

Помимо принципов оптимальности для выбора наилучшей альтернативы широко используются следующие подходы: построение функции полезности, метод аналитической иерархии; метод порогов несравнимости (ЭЛЕКТРА) и др.

При построении функции полезности предполагается, что альтернативы обладают определенной полезностью и рядом свойств, на основе которых строится функция полезности. В свою очередь, по значениям функции полезности можно сравнить альтернативы, упорядочить их или выбрать лучшие.

Метод аналитической иерархии использует дерево критериев, в котором более общие критерии разделяются на критерии частного характера. Для каждой группы критериев определяются коэффициенты важности. Альтернативы сравниваются между собой по отдельным критериям в целях определения критериальной ценности каждой из них. Средством определения коэффициентов важности критериев, или критериальной ценности альтернатив, является попарное сравнение. Результат сравнения оценивается по балльной шкале (обычно от 1 до 10). На основе таких сравнении вычисляются коэффициенты важности критериев, оценки альтернатив и находится общая оценка как взвешенная сумма оценок критериев.

Методы ЭДЕКТРА представляют собой подход к решению задачи многокритериального выбора на основе попарного сравнения альтернатив по совокупности их критериальных оценок. В этих методах строится последовательность бинарных отношений, на основе которых последовательно исключаются из рассмотрения худшие альтернативы. Процедура выбора заканчивается, когда остается приемлемое для ЛПР число лучших альтернатив.

При наличии неопределенности, обусловленной случайными состояниями среды или действиями злоумышленника, первоначально решается задача снятия неопределенности и перехода к детерминированной задаче, которая затем решается описанными выше методами.

При оценивании качества альтернатив в условиях неопределенности возможна одна из следующих трех ситуаций априорной информированности ЛПР о состояниях среды для локального критерия качества z_i.

1. ЛПР известно априорное распределение вероятностей состояний среды.

2. ЛПР известно, что среда активно противодействует его целям: среда стремится к выбору таких состояний $s_{ij} \in S_i, j = 1, \dots, q_i$для которых в случае если локальный критерий или характеристика качества z_i описывается функцией полезности U_i, то среда принимает состояние, обеспечивающее наименьшее значение функции полезности из множества своих максимально возможных (по решениям) значений. В случае если локальный критерий или характеристика качества z_i описывается функцией потерь V_i то среда принимает состояние, обеспечивающее наибольшее значение функции потерь из множества своих минимально возможных (по решениям) значений.

3. ЛПР имеет приблизительную априорную информацию о состояниях среды, являющуюся промежуточной между первой и второй ситуациями априорной информированности.

Для каждой из трех ситуаций априорной информированности используются критерии оценки и выбора решений (критерии снятия неопределенности).

Для первой ситуации – критерии Байеса-Лапласа, критерий минимума среднего квадратического отклонения функции полезности или функции потерь, критерий максимизации вероятности распределения функции полезности, модальный критерий, критерий минимума энтропии математического ожидания функции полезности, критерий Гермейера, комбинированные критерии. Для второй ситуации – максиминный критерий Вальда, критерий минимаксного риска Севиджа. Для третьей ситуации – критерий Гурвица, критерий Ходжеса-Лемана.

Более подробно модели и методы принятия решений представлены в [14].

Помимо описанных методов принятия решений, выбор мер контроля и управления, направленных на снижение рисков информационной безопасности, может быть осуществлен на основе построения оптимизационной модели, в частности, сформулированной в виде «задачи о ранце».

В данном случае первоначально формируется перечень всех возможных в данной ситуации мер контроля и управления. Затем каждому защитному мероприятию ставится в соответствие альтернативная переменная x_j $(j=\overline{1,n})$, принимающая значение единица при использовании этого мероприятия и ноль в противном случае. Все мероприятия ранжируются по их предполагаемому эффекту с введением коэффициентов «ценности» a_j. Целевой функцией является получение максимального эффекта от комплекса мероприятий:

$$\sum_{j=1}^{n} a_j x_j \to \max . \qquad (1)$$

При этом должны выполняться ограничения на затраты

$$\sum_{j=1}^{n} z_j x_j \le Z, \qquad (2)$$

где z_j - затраты на использование *j*-го мероприятия;

Z - общие затраты.

Несовместимость мероприятий учитывается на основе следующих ограничений :

$$x^t_{j_1} + x^t_{j_2} \le 1; \quad j_1, j_2 = \overline{1,n}, \quad t = \overline{1,T}, \qquad (3)$$

где T - количество возможных пар несовместимых мероприятий.

Для взаимозаменяемых мероприятий, принадлежащих одной группе, вводятся ограничения

$$\sum_{\forall i \in R_a} x^a_i \le 1, \quad a = \overline{1,A}, \qquad (4)$$

где $\grave{A}$ – количество групп, содержащих несколько мероприятий-аналогов;

R_a – множество взаимозаменяемых мероприятий, принадлежащих *a*-й группе.

В случае, когда из каждой группы мероприятий-аналогов в полученное решение обязательно должен войти какое-либо мероприятий, вводятся дополнительные ограничения

$$\sum_{\forall i \in R_a} x^a_i = 1, \quad a = \overline{1,A} \qquad (5)$$

В результате построения модели получается задача дискретного программирования «о ранце», которая решается методами многоальтернативной оптимизации.

Рассмотрим алгоритм решения задачи (1) - (5) методом «ветвей и границ» с простым и эффективным способом оценки верхней границы целевой функции [1].

Заменим z_j на z_{1j}, Z на b_1, $z^t_{j_1}=1$, $z^t_{j_2}=1$ и $z^a_i=1$ на z_{ij}, $x^t_{j_1}$, $x^t_{j_2}$ и x^a_i на x_i, тогда задача (1) - (5) будет иметь вид:

$$L=\sum_{j=1}^{n} a_j x_j \to \max \quad , \tag{6}$$

$$\sum_{j=1}^{n} z_{ij} x_j \le b_i, \quad i=\overline{1,m} \ , \tag{7}$$

$$x_j \in \{0,1\}, \quad j=\overline{1,n} \quad , \tag{8}$$

где m = T+1 , $b_i=1$ для $i=\overline{2,m}$, причем $a_j \ge 0$, $z_j \ge 0$.

Обозначим U - множество переменных x_j;

S - множество фиксированных переменных, вошедших в допустимое решение ;

E_S - множество зависимых переменных, которые не могут быть включены в множество S, т.к. для них выполняется неравенство

$$z_{ij} > b_i - \sum_{X_j \in S} z_{ij} x_j \ ;$$

G_S - множество свободных переменных, из которых производится выбор для включения в S очередной переменной.

Обозначим $h_{ij}=a_i/z_{ij}$ и допустим, что $x_j \in S$ $\left(j=1,...,k<n\right)$ и выполняются условия

$$h_{ik+1} \ge h_{ik+2} \ge ... \ge h_{il}, \quad l \le n, \quad i=\overline{1,m} \ , \tag{9}$$

$$\sum_{j=k+1}^{l} z_{ij} > b_i - \sum_{x_j \in S} z_{ij}, \tag{10}$$

$$\sum_{j=k+1}^{l-1} z_{ij} \le b_i - \sum_{x_j \in S} z_{ij} x_j, \quad i=\overline{1,m} \quad . \tag{11}$$

Условия (10), (11) означают, что в множество S без нарушения неравенств (7) можно дополнительно ввести элементы $x_{k+1}, x_{k+2}, \ldots, x_{l-1}$. При введении в множество S элементов $x_{k+1}, x_{k+2}, \ldots, x_l$ неравенства (7) не выполняются.

Для определения верхней границы решения может быть использовано выражение

$$H_S = \sum_{x_j \in S} a_j x_j + L_{sM}, \qquad (12)$$

где

$$L_{sM} = \min\{L_{s1}, L_{s2}, \ldots, L_{sm}\}, \qquad (13)$$

$$L_{si} = \sum_{j=k+1}^{l-1} a_j + h_{il} \Delta b_i, \; i = \overline{1,m}, \qquad (14)$$

$$\Delta b_i = b_i - \sum_{x_j \in S} z_{ij} x_j - \sum_{j=k+1}^{l-1} z_{ij}, \; i = \overline{1,m}. \qquad (15)$$

Из условий (9) - (11) следует, что L не меньше максимального значения величины $\sum_{x_j \in S} a_j x_j$ при ограничениях

$$\sum_{x_j \in S} z_{ij} x_j \le b_i - \sum_{x_j \in S} z_{ij} x_j = b_i', \; i = \overline{1,m},$$

$$x_j \in \{0,1\}, \; x_j \in G_S.$$

Выбор очередной переменной для включения в множество S производится с помощью условия

$$h_r x_r = \max_{x_j \in G_s} h_{Mj}(x_j),$$

где

$$h_{Mj}(x_j) = a_j / z_{Mj}.$$

Для выбранной переменной x_r определяются величины $H_s(x_r)$ и $\overline{H_s}(x_r)$, т.е. в S включается $x_r = 1$ или $x_r = 0$.

Если в процессе решения окажется, что в множестве G_S нет элементов, которые могут быть введены в множество S без нарушения ограничения (7), то полученное решение

$L_s = \sum_{x_j \in S} a_j x_j$ принимается в качестве первого приближенного решения L_0.

Все вершины дерева возможных вариантов, для которых выполняются условия $H_s \le L_0$, из дальнейшего рассмотрения исключаются.

Из оставшихся ветвей выбирается ветвь с максимальным значением H_s, и процесс поиска оптимального варианта продолжается. Если в процессе решения будет найдено $L_S = \sum_{x_j \in S} a_j x_j > L_0$, то полученное решение принимается в качестве нового приближенного результата.

Вычислительная процедура заканчивается, если для всех оставшихся ветвей выполняется условие $H_s \le L_0$.

При введении дополнительных ограничений (4) после получения нового решения L_S проверяется условия (4) и в случае их невыполнения полученное решение не принимается в качестве нового приближенного результата.

4. ЗАДАНИЕ КУРСОВОЙ РАБОТЫ

4.1. Общая часть

На примере выбранного предприятия разработать систему управления информационными рисками (в соответствии со стандартом ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности). Разработать модель принятия решений или оптимизационную модель для выбора мер и средств контроля и управления.

4.2. Индивидуальные варианты заданий

Для выполнения курсовой работы необходимо выбрать объект из предложенного ниже списка.

1. Детская поликлиника «Солнце». Оказывает услуги медицинского характера; должна иметь возможность записи пациентов через Интернет, в регистратуре и получение талона у лечащего врача; результаты обследования должны заноситься в базу поликлиники и дополнительно дублироваться в карту пациента (бумажный носитель); должна предусматриваться система хранения персональных медицинских карт в поликлинике; должна предусматриваться возможность получения удаленного доступа пациента к результатам обследований; необходимо учитывать возможность перевода пациента и его данных в другое лечебное учреждение, а также получение дополнительных данных из других учреждений.

2. Туристическое агентство «Чемодан». Оказывает услуги туристического характера; должно иметь возможность оформления паспортов, виз, разрешений на вывоз несовершеннолетних детей за границу; бронирование и оплату санаториев, баз отдыха, гостиниц, экскурсий, перелета, трансфера.

3. Автошкола «Пятое колесо». Оказывает образовательные услуги; должна иметь возможность

дистанционной записи на практические и дополнительные занятия; учета промежуточных результатов обучения.

4. Агентство недвижимости «Новоселье». Оказывает услуги по покупке/продаже/обмену/съему жилья.

5. Реабилитационный центр «Силушка богатырская». Оказывает восстановительные медицинские услуги пациентам всех возрастов; должен иметь возможность доступа к данным обследований пациента в других клиниках за большой период времени; помимо всех требований, предъявляемым к детской поликлинике (см. пункт 1) необходимо предусмотреть запись пациента в другие медицинские учреждения.

6. Страховое агентство «Цунами». Оказывает услуги в сфере страхования; должна предусматриваться возможность страхования жизни, здоровья, жилья, автосредства, отпуска и т.д.

7. Негосударственный пенсионный фонд «Гарантия». Оказывает услуги по формированию пенсионных выплат; должна поддерживаться функция «горячей линии».

8. Управляющая компания «Теремок». Оказывает услуги по восстановлению и поддержке состояния жилищного фонда клиентов; должна иметь возможность взаимодействия с коммунальными службами, поставщиками услуг.

9. Центр занятости «Статус». Оказывает услуги по трудоустройству населения; должен предусматривать возможность сотрудничества с другими компаниями; проведения статистических исследований.

10. Охранное предприятие «Спокойствие». Оказывает услуги по охране различных объектов; должна поддерживаться функция оперативного внесения в базу состояние объектов охраны.

4.3. Контрольные вопросы

1. Что представляет собой менеджмент риска информационной безопасности? Перечислите задачи менеджмента риска информационной безопасности.

2. Перечислите основные этапы менеджмента риска информационной безопасности и их взаимосвязи.

3. Что включает в себя этап установление контента? Перечислите основные критерии, необходимые для менеджмента риска ИБ.

4. В чем заключается и какие этапы включает в себя оценка риска ИБ?

5. В чем заключается и какие этапы включает в себя анализ риска ИБ?

6. В чем заключается идентификация риска ИБ? Перечислите этапы идентификации риска ИБ.

7. Что включает в себя идентификация активов? Перечислите основные виды активов.

8. Что представляют собой требования безопасности для активов?

9. Что включает в себя реестр информационных активов?

10. Каким образом может быть определена ценность активов? Приведите пример критериев и соответствующих шкал для оценки возможного ущерба.

11. Что такое профиль и жизненный цикл угрозы?

12. По каким признакам классифицируются угрозы информационной безопасности?

13. Какими способами может быть выполнена оценка вероятности угроз информационной безопасности?

14. Какими способами может быть выполнена оценка уязвимостей?

15. Каким образом может быть получена количественная оценка риска информационной безопасности?

16. Что включает в себя реестр рисков информационной безопасности?

17. В чем заключается оценивание рисков информационной безопасности?

18. Какие существуют варианты обработки риской информационной безопасности?

19. В чем заключается снижение риска информационной безопасности? Перечислите способы снижения рисков. Какие типичные ограничения должны быть учтены?

20. В чем заключается сохранение риска информационной безопасности? Перечислите факторы, влияющие не решение о принятии рисков.

21. В чем заключается предотвращение риска информационной безопасности? Перечислите основные способы предотвращения риска.

22. Что такое перенос риска информационной безопасности?

23. Какие задачи решаются в процессе коммуникации риска информационной безопасности?

24. Какие факторы подлежат мониторингу в процессе переоценки риска информационной безопасности?

25.Охарактеризовать роль лица, принимающего решения, экспертов, консультантов в задачах принятия решений.

26. Привести общую схему алгоритма экспертизы.

27. Описать основные этапы экспертизы.

28. Описать основные формы опроса экспертов, взаимодействия экспертов при опросе.

29. Составить алгоритм оценивания согласованности мнений экспертов.

30. Описать методы формирования исходного множества альтернатив.

31. Что такое область компромиссов, область согласия, множество Парето, множество эффективных решений? Как выделяют область компромиссов?

32. Описать признаки и свойства методов решения многокритериальных задач принятия решений. Провести классификацию методов многокритериальной оценки

альтернатив и методов решения многокритериальных задач принятия решений.

33. Охарактеризовать аксиоматические методы многокритериальной оценки альтернатив.

34. Какие принципы оптимальности используются в прямых методах многокритериальной оценки альтернатив?

35. Каковы основные приемы нормализации критериев?

36. Как определяется важность критериев?

37. Построить структурные схемы методов порогов несравнимости. К каким решениям могут приводить данные методы?

38. Построить структурную схему метода аналитической иерархии.

38. Чем различаются задачи принятия решений при риске и при определенности? В чем состоит неопределенность задачи принятия решений при риске?

39. Описать основные особенности однокритериальной модели принятия решений при риске.

40. Описать основные особенности многокритериальной модели принятия решений при риске.

41. В чем заключается неопределенность задачи принятия решений при риске? Как преодолевается эта неопределенность?

42. С помощью каких критериев преодолевается неопределенность задач принятия решений при риске? Каковы преимущества и недостатки этих критериев?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алексеев, О. Г. Комплексное применение методов дискретной оптимизации [Текст] / О. Г. Алексеев. – М.: Наука, 1987. – 247 с.

2. Астахов, А. М. Искусство управления информационными рисками [Текст] / А. М. Астахов. – М.: ДМК Пресс, 2010. – 312 с.

3. Атаки на информационно-технологическую инфраструктуру критически важных объектов: оценка и регулирование рисков [Текст]: монография / А. О. Калашников и др. – Воронеж: Изд-во «Научная книга». – 2013. – 160 с.

4. Белецкая, С. Ю. Принятие оптимальных решений с использованием средств EXCEL [Текст]: учеб. пособие / С. Ю. Белецкая. – Воронеж: Изд-во ВГТУ, 2000. – 98 с.

5. Варфоломеев, А. А. Управление информационными рисками [Текст]: учеб. пособие / А. А. Варфоломеев. – М.: РУДН, 2008. – 158 с.

6. ГОСТ Р ИСО 31000–2010 «Менеджмент риска. Принципы и руководство». – М.: Стандартинформ. – 2012. – 28 с.

7. ГОСТ Р ИСО 31010–2011 «Менеджмент риска. Методы оценки риска». – М.: Стандартинформ. – 2012. – 74 с.

8. ГОСТ Р ИСО/МЭК 27000–2012 «Информационная технология «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология». – М.: Стандартинформ. – 2013. – 33 с.

9. ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». – М.: Стандартинформ. – 2008. – 31 с.

10. ГОСТ Р ИСО/МЭК 27002–2012 «Информационная технология «Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности». – М.: Стандартинформ. – 2013. – 210 с.

11. ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология «Методы и средства

обеспечения безопасности. Менеджмент риска информационной безопасности». – М.: Стандартинформ. – 2011. – 51 с.

12. Методическое обеспечение оценки и регулирования рисков распределенных информационных систем [Текст]: учеб. пособие / Г. А. Остапенко и др. – Воронеж: ВГТУ, 2011. – 178 с.

13. Остапенко, А. Г. Математические основы риск-анализа [Текст]: учеб. пособие [Электронный ресурс] / А. Г. Остапенко, М. В. Бурса. – Воронеж: ВГТУ, 2013. – электрон. опт. диск.

14. Остапенко, А. Г. Математические основы управления рисками нарушения информационной безопасности [Текст]: учеб. пособие [Электронный ресурс] / А. Г. Остапенко, О. Н. Чопоров. – Воронеж: ВГТУ, 2014. – электрон. опт. диск.

15. Остапенко, А. Г. Теория управления рисками информационных систем [Текст]: учеб. пособие [Электронный ресурс] / А. Г. Остапенко, С. С. Куликов. – Воронеж: ВГТУ, 2013. – электрон. опт. диск.

16. Остапенко, Г. А. Основы оценки рисков и защищенности компьютерно атакуемых информационных систем и технологий [Текст]: учеб. пособие / Г. А. Остапенко, Д. Г. Плотников, О. А. Остапенко. – Воронеж: ВГТУ, 2013. – 143 с.

17. Остапенко, Г. А. Риски систем [Текст]: учеб. пособие [Электронный ресурс] / Г. А. Остапенко, О. А. Остапенко, Е. А. Попов. – Воронеж: ВГТУ, 2013. – электрон. опт. диск.

18. Остапенко, О. А. Риски систем: оценка и управление [Текст]: учеб. пособие [Электронный ресурс] / О. А. Остапенко, Д. О. Карпеев, В. Н. Асеев. – Воронеж: ВГТУ, 2006. – электрон. опт. диск.

19. Риски распределенных систем: методики и алгоритмы оценки и управления / Г. А. Остапенко, Д. О. Карпеев, Д. Г. Плотников и др. // Информация и безопасность. – 2010. – Т. 13. – Вып. 4. – С. 485–530.

20. Рыков, А. С. Системный анализ: модели и методы принятия решений и поисковой оптимизации [Текст] / А. С. Рыков. – М.: Издательский дом МИСиС, 2009. – 608 с.

21. Щербаков, В. Б. Оценка и управление рисками информационной безопасности беспроводных телекоммуникационных систем [Текст]: учеб. пособие [Электронный ресурс] / В. Б. Щербаков, А. В. Гармонов, О. А. Остапенко. – Воронеж: ВГТУ, 2007. – электрон. опт. диск.

22. Язов, Ю. К. Анализ и управление рисками нарушения безопасности персональных данных при обработке в информационных системах [Текст]: учеб пособие [Электронный ресурс] / Ю. К. Язов; под ред. А. Г. Остапенко. – Воронеж: ВГТУ, 2008. – электрон. опт. диск.

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к курсовой работе по дисциплине
«Математические основы управления рисками»
для студентов специальности
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Составитель
Чопоров Олег Николаевич

В авторской редакции

Подписано к изданию 13.05.2015.
Уч. - изд. л. 2,2.

ФГБОУ ВПО «Воронежский государственный
технический университет»
394026 Воронеж, Московский просп., 14