ФГБОУ ВПО «Воронежский государственный
технический университет»

Кафедра систем информационной безопасности

214-2015

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к самостоятельным работам по дисциплине
«Управление рисками в распределенных
информационных системах»
для студентов специальности
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Воронеж 2015

Составители: аспирант Е. С. Соколова, д-р техн. наук А. Г. Остапенко

УДК 004.05

Методические указания к самостоятельным работам по дисциплине «Управление рисками в распределенных информационных системах» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. Е. С. Соколова, А. Г. Остапенко. Воронеж, 2015. 27 с.

Методические указания к самостоятельным работам содержат указания и рекомендации, направленные на системное изучение информационных технологий и систем поддержки управленческих решений в распределенных информационных системах.

Методические указания подготовлены в электронном виде в текстовом редакторе MW-2013 и содержатся в файле Соколова_СР_Риски в РИС.pdf.

Табл. 1. Библиогр.: 109 назв.

Рецензент д-р техн. наук, проф. О. Н. Чопоров

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

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

ВВЕДЕНИЕ

Во многих организациях распределенные системы стали основным средством обработки и хранения информационных ресурсов и нередко содержат конфиденциальную информацию.

Создание распределенной системы в организации, или внедрение новых информационных средств в существующие системы, должны сопровождаться проведением тщательного анализа с точки зрения оценки состояния информационной безопасности.

Под информационной безопасностью понимается «состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз». Таким образом, оценка состояния информационной безопасности распределенной системы заключается в оценке защищенности ее информационных ресурсов.

Методические указания посвящены исследованию вопросов управления информационной безопасностью через регулирование информационных рисков распределенных систем.

Как известно, информационные атаки на системы, а также сбои их компонентов вызывают разнообразные отказы, наносящие ущерб и обуславливающие соответствующие риски.

Высокоуровневая оценка риска информационной безопасности дает возможность определять приоритеты и хронологию действий.

1. ЦЕЛИ И ЗАДАЧИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Целью самостоятельной работы студентов (СРС) является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

– систематизация и закрепление полученных теоретических знаний и практических умений студентов;

– углубление и расширение теоретических знаний;

– формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;

– развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

– формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

– развитие исследовательских умений;

– использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических занятиях, для эффективной подготовки к итоговому зачету.

2. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Выделяется два вида самостоятельной работы – аудиторная, под руководством преподавателя, и внеаудиторная. Тесная взаимосвязь этих видов работ предусматривает дифференциацию и эффективность результатов ее выполнения и зависит от организации, содержания, логики учебного процесса (межпредметных связей, перспективных знаний и др.):

– аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

– внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Основными видами самостоятельной работы студентов без участия преподавателей являются:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- подготовка к семинарам и практическим работам, их оформление;
- работа с учебно-методической литературой;
- оформление конспектов лекций;
- подготовка к курсовому проектированию;
- подготовка к зачету.

3. ТЕМАТИКА САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Виды самостоятельной работы и способы контроля

Наименование разделов и тем	**Содержание самостоятельной работы**	**Вид контроля и отчетность по результатам самостоятельной работы**
Раздел 1 Основные понятия и задачи	**Теоретический материал:**	
	1. Основные понятия	Подготовка конспекта лекций
	2. Обзор процесса управления рисками информационной безопасности	Подготовка конспекта лекций
	3. Основные критерии в управлении рисками	Подготовка конспекта лекций, подготовка к письменной проверочной работе по пройденному материалу
Раздел 2 Оценка риска информационной безопасности	**Теоретический материал:**	
	1. Общее описание оценки риска информационной безопасности	Подготовка конспекта лекций
	2. Анализ риска	Подготовка конспекта лекций
	3. Оценивание рисков	Подготовка конспекта лекций
	4. Измерение рисков	Подготовка конспекта лекций
	5. Установление значений уровня рисков	Подготовка конспекта лекций, подготовка к письменной проверочной работе по пройденному материалу

Наименование разделов и тем	Содержание самостоятельной работы	Вид контроля и отчетность по результатам самостоятельной работы
Раздел 3 Методы оценки информационных рисков	**Теоретический материал:**	
	1. Высокоуровневая оценка риска информационной безопасности	Подготовка конспекта лекций
	2. Детальная оценка риска информационной безопасности	Составление отчета о проделанной работе
Раздел 4 Обработка риска информационной безопасности	**Теоретический материал:**	
	1. Общее описание обработки риска	Подготовка конспекта лекций
	2. Снижение риска	Подготовка конспекта лекций
	3. Сохранение риска	Подготовка конспекта лекций
	4. Предотвращение риска	Подготовка конспекта лекций
	5. Принятие риска информационной безопасности	Подготовка конспекта лекций, подготовка к письменной проверочной работе по пройденному материалу
Раздел 5 Основные понятия и задачи системного анализа	**Теоретический материал:**	
	1. Системный анализ, системный подход, теория систем	Подготовка конспекта лекций
	2. Система. Цель. Структура. Классификация систем	Подготовка конспекта лекций

Наименование разделов и тем	Содержание самостоятельной работы	Вид контроля и отчетность по результатам самостоятельной работы
	3. Методика и методологические принципы системного анализа	Подготовка конспекта лекций
	4. Основные понятия и обобщенная классификация задач принятия решений	Подготовка конспекта лекций, подготовка к зачету
Раздел 6. Экспертные оценки	**Теоретический материал:**	
	1. Методологические основы и предпосылки применения методов экспертного оценивания	Подготовка конспекта лекций
	2. Основные типы шкал и методы проведения экспертизы	Подготовка конспекта лекций
	3. Качественные экспертные оценки и их особенности	Подготовка конспекта лекций
	4. Этапы работ по организации экспертного оценивания	Подготовка конспекта лекций
	5. Поиск и исключение противоречий и ошибок в ответах эксперта	Подготовка конспекта лекций, подготовка к письменной проверочной работе по пройденному материалу

Наименование разделов и тем	Содержание самостоятельной работы	Вид контроля и отчетность по результатам самостоятельной работы
Раздел 7. Детерминированные модели и методы принятия решений	**Теоретический материал:**	
	1. Постановки многокритериальных задач принятия решений	Подготовка конспекта лекций
	2. Характеристики приоритета критериев	Подготовка конспекта лекций
	3. Нормализация критериев	Подготовка конспекта лекций
	4. Принципы оптимальности в задачах принятия решений	Подготовка конспекта лекций
	5. Постановка задач оптимизации на основе комбинирования принципов оптимальности	Подготовка конспекта лекций, подготовка к письменной проверочной работе по пройденному материалу
Раздел 8. Статистическая модель одно--критериального принятия решений в условиях неопределенности. Построение критериев оценки и выбора решений для первой ситуации априорной информированности ЛПР	**Теоретический материал**:	
	1. Критерий Байеса-Лапласа	Подготовка конспекта лекций
	2. Критерий минимума среднего квадратического отклонения функции полезности или функции потерь	Подготовка конспекта лекций
	3. Объединение критериев Байеса-Лапласа и среднего квадратического отклонения функции полезности	Подготовка конспекта лекций

Наименование разделов и тем	Содержание самостоятельной работы	Вид контроля и отчетность по результатам самостоятельной работы
	4. Критерий максимизации вероятности распределения функции полезности	Подготовка конспекта лекций
	5. Модальный критерий	Подготовка конспекта лекций, подготовка к письменной проверочной работе по пройденному материалу
Раздел 9. Построение критериев оценки и выбора решений для второй ситуации априорной информированности ЛПР	**Теоретический материал:**	
	1. Максиминный критерий Вальда	Подготовка конспекта лекций
	2. Критерии минимаксного риска Сэвиджа	Подготовка конспекта лекций подготовка к письменной проверочной работе по пройденному материалу
Раздел 10. Построение критериев оценки и выбора решений для третьей ситуации априорной информированности ЛПР	**Теоретический материал:**	
	1. Критерий Гурвица.	Подготовка конспекта лекций
	2. Критерий Ходжеса-Лемана	Подготовка конспекта лекций
	3. Построение универсального комбинированного критерия оценки и выбора решений для разных ситуаций априорной информированности ЛПР	Подготовка конспекта лекций подготовка к зачету

Наименование разделов и тем	Содержание самостоятельной работы	Вид контроля и отчетность по результатам самостоятельной работы
Раздел 11. Задачи и алгоритмы принятия коллективных решений	**Теоретический материал:**	
	1. Принятие коллективных решений на основе голосования	Подготовка конспекта лекций
	2. Задача принятия группового решения	Подготовка конспекта лекций
	3. Аксиомы и парадокс Эрроу	Подготовка конспекта лекций
	4. Правила большинства	Подготовка конспекта лекций
	5. Правило суммы мест альтернатив. Основные процедуры голосования	Подготовка конспекта лекций подготовка к письменной проверочной работе по пройденному материалу
Раздел 12. Задачи и методы нечеткой оптимизации и принятия решений при нечетких состояниях среды	**Теоретический материал:**	
	1. Основные понятия и элементы теории нечетких множеств	Подготовка конспекта лекций
	2. Задачи нечеткого математического программирования при одном критерии и нескольких ограничениях	Подготовка конспекта лекций
	3. Задачи нечеткого математического программирования при нескольких критериях. Подходы к формализации нечеткости	Подготовка конспекта лекций подготовка к письменной проверочной работе по пройденному материалу

Наименование разделов и тем	Содержание самостоятельной работы	Вид контроля и отчетность по результатам самостоятельной работы
Раздел 13. Задачи и методы однокритериальной оптимизации	**Теоретический материал:**	
	1. Вопросы оптимизации	Подготовка конспекта лекций
	2. Методы безусловной минимизации гладких функций	Подготовка конспекта лекций
	3. Методы первого порядка	Подготовка конспекта лекций
	4. Градиентные методы	Подготовка конспекта лекций
	5. Гладкие функции. Конечно-разностная аппроксимация производных	Подготовка конспекта лекций
	6. Методы одномерной минимизации	Подготовка конспекта лекций подготовка к экзамену

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Батаронов, И. Л. Оценка и регулирование рисков обнаружение и предупреждение компьютерных атак на инновационные проекты [Текст] / И. Л. Батаронов, А. В. Паринов, К. В. Симонов // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 243–246.

2. Бекетнова, Ю. М. Решение задачи раннего выявления рисков нарушения финансовой и информационной безопасности юридического лица в терминах теории распознавания образов [Текст] / Ю. М. Бекетнова, И. Я. Львович // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 191–194.

3. Вероятностные аналитические модели сетевой атаки с внедрением вредоносного программного обеспечения [Текст] / В. И. Борисов, Н. М. Радько, А. А. Голозубов, И. Л. Батаронов, Е. В. Ермилов // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 5–30.

4. Разработка методологии оценки эффективности средств защиты беспроводных сетей группы стандартов IEEE 802.11 [Текст] / В. И. Борисов, В. Б. Щербаков, С. А. Ермаков, И. Л. Батаронов // Информация и безопасность. – 2011. – Т. 14. – Вып. 3. – С. 317–336.

5. Бурса, М. В. DDOS–атаки на информационно–телекоммуникационные системы: управление рисками [Текст] / М. В. Бурса, Ю. Г. Пастернак // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 255–256.

6. Бурса, М. В. Оценка риска релизации распределенных атак типа «HTTP-флуд» на многокомпонентные информационно-телекоммуникационные системы [Текст] / М. В. Бурса, Г. А. Остапенко // Информация и безопасность. – 2014. – Т. 17. – Вып. 3. – С. 424-427.

7. Бутузов, В. В. К вопросу обоснования функции ущерба атакуемых систем [Текст] / В. В. Бутузов, А. В. Заряев // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 47–54.

8. Бутузов, В. В. Моделирование процесса реализации атаки, с помощью sms, e-mail флудов, на канал связи автоматизированной информационной системы [Текст] / В. В. Бутузов, А. В. Завальский, А. В. Заряев // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 220-223.

9. Бутузов, В. В. Риск–анализ в интервале времени: некоторые приложения [Текст] / В. В. Бутузов, Л. Г. Попова // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 137–138.

10. Васильев, Б. В. Оценка стоимости объектов информационной безопасности в проектных организациях нефтегазового комплекса [Текст] / Б. В. Васильев, Н. И. Баранников, Д. Г. Плотников // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 204-207.

11. Васильев, Б. В. Учет и идентификация объектов информационной безопасности в проектных организациях нефтегазового комплекса [Текст] / Б. В. Васильев, Н. И. Баранников, Д. Г. Плотников // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 224-227.

12. Воронов, А. А. Применение методологического анализа в исследовании безопасности [Текст] / А. А. Воронов, И. Я. Львович // Информация и безопасность. – 2011. – Т. 14. – Вып. 3. – С. 469–470.

13. Риск-моделирование процесса заражения автоматизированных информационных систем, построенных в сетях топологии «звезда», посредством вирусов-спутников [Текст] / А. А. Голозубов, Н. В. Филатов, О. Ю. Макаров, Е. А. Москалева // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 200-203.

14. Дешина, А. Е. Инновационные технологии регулирования рисков мультисерверных систем в условиях атак комплексного типа [Текст] / А. Е. Дешина, О. Н. Чопоров, К. А. Разинкин // Информация и безопасность. – 2013. – Т. 16. – Вып. 3. – С. 371-374.

15. Дешина, А. Е. Интегральная оценка общего риска при синтезе ИТКС на основе параметров риска ее компонентов

[Текст] / А. Е. Дешина, И. А. Ушкин, О. Н. Чопоров // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 510-513.

16. Дешина, А. Е. Информационные риски в мультисерверных системах: атаки комплексного типа [Текст] / А. Е. Дешина, В. И. Белоножкин // Информация и безопасность. – 2013. – Т. 16. – Вып. 3. – С. 335-344.

17. Дешина, А. Е. Информационные риски в мультисерверных системах: выбор параметров системы защиты [Текст] / А. Е. Дешина, О. Н. Чопоров, К. А. Разинкин // Информация и безопасность. – 2013. – Т. 16. – Вып. 3. – С. 365-370.

18. Дешина, А. Е. Информационные риски мультисерверных систем: получение параметров компонентов системы по заданным параметрам общего риска [Текст] / А. Е. Дешина, И. Я. Львович // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 604-611.

19. Дешина, А. Е. Управление рисками мультисерверных систем в случае синхронных DDOS-атак на их компоненты [Текст] / А. Е. Дешина, И. Я. Львович // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 324-327.

20. Ермаков, С. А. Применение теории массового обслуживания для моделирования сетей LTE [Текст] / С. А. Ермаков, Н. И. Баранников, И. Л. Батаронов // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 538-545.

21. Риск–анализ распределенных систем на основе параметров рисков их компонентов [Текст] / Е. В. Ермилов, Е. А. Попов, М. М. Жуков, О. Н. Чопоров // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 123–126.

22. Есин, В. И. Защита данных в базе данных с универсальной структурой [Текст] / В. И. Есин, В. Г. Юрасов // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 180-187.

23. Построение динамической риск–модели для компонентов распределенной системы на основе заданного

закона распределения ущерба [Текст] / М. М. Жуков, Е. В. Ермилов, О. Н. Чопоров, А. В. Бабурин // Информация и безопасность. – 2012. – Т. 15. – Вып. 4. – С. 449–460.

24. Специфика построения многокомпонентных систем с заданными параметрами общего риска [Текст] / М. М. Жуков, Е. В. Ермилов, Н. И. Баранников, И. П. Нестеровский // Информация и безопасность. – 2012. – Т. 15. – Вып. 4. – С. 567–570.

25. Моделирование атак на беспроводные сети WI-FI [Текст] / А. С. Заворыкин, Н. Н. Корнеева, Н. Н. Толстых, В. Г. Юрасов, В. И. Белоножкин // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 486-489.

26. Матричное представление функционального описания угроз проникновения на охраняемые объекты в результате искажения информации систем централизованного наблюдения [Текст] / В. С. Зарубин, Е. М. Абросимова, М. Ф. Сизинцев, Т. Б. Ходырев // Информация и безопасность. – 2014. – Т. 17. – Вып. 1. – С. 134-139.

27. Структурные модели как основа формализованного представления механизмов защиты информационных процессов в автоматизированных комплексах физической защиты [Текст] / В. С. Зарубин, С. В. Зарубин, А. А. Никитин, В. А. Половинкин // Информация и безопасность. – 2012. – Т. 15. – Вып. 4. – С. 555–560.

28. Иванкин, Е. Ф. Аналитическая оценка информационных рисков вирусноатакуемых автоматизированных систем [Текст] / Е. Ф. Иванкин, С. В. Машин, Н. И. Баранников // Информация и безопасность. – 2013. – Т. 16. – Вып. 3. – С. 463-465.

29. Иванкин, Е. Ф. Вирусные атаки на информационные ресурсы инновационных проектов: управление рисками [Текст] / Е. Ф. Иванкин, С. В. Машин, О. А. Лосева // Информация и безопасность. – 2012. – Т. 15. – Вып. 3. – С. 401–406.

30. Иванкин, Е. Ф. Инновационные платежные системы на основе банковских карт: методы снижения

информационных рисков [Текст] / Е. Ф. Иванкин, М. М. Жуков, Р. В. Менжулин // Информация и безопасность. – 2012. – Т. 15. – Вып. 3. – С. 299–312.

31. Распределенные платежные системы: состояние и перспективы развития в контексте обеспечения их безопасности [Текст] / Е. Ф. Иванкин, М. М. Жуков, Р. В. Менжулин, М. В. Бурса, А. В. Заряев // Информация и безопасность. – 2011. – Т. 14. – Вып. 4. – С. 481–506.

32. Иванкин, М. П. Атаки на распределенную корпоративную сеть, ориентированные на «внедрение доверенного ложного объекта» [Текст] / М. П. Иванкин, Е. А. Шварцкопф, А. В. Заряев // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 514-517.

33. Иванкин, М. П. Оценка остаточного риска в условиях атаки типа «анализ сетевого трафика» [Текст] / М. П. Иванкин, Е. Ф. Иванкин // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 249–250.

34. Иванкин, М. П. Управление риском информационно безопасности в условиях атаки типа «анализ сетевого трафика» [Текст] / М. П. Иванкин, А. В. Заряев // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 494-495.

35. Канин, Д. М. Информационные технологии как инструментарий интеллектуализации управления устойчивым развитием территории [Текст] / Д. М. Канин, Л. В. Паринова, И. Я. Львович // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 31–38.

36. Идентификация параметров нечетких моделей оценки информационных рисков информационных систем [Текст] / Д. О. Карпеев, А. Ю. Татаринцев, Д. С. Яковлев, А. В. Заряев // Информация и безопасность. – 2010. – Т. 13. – Вып. 1. – С. 37–42.

37. Риск–анализ распределенных вычислительных систем на основе модели Белла Ла–Падулы с применением экспертной оценки [Текст] / Д. О. Карпеев, Д. С. Яковлев,

А. Ю. Татаринцев, А. В. Заряев // Информация и безопасность. – 2010. – Т. 13. – Вып. 1. – С. 43–46.

38. Социально–информационные системы: деструктивные воздействия на их пользователей и риск модели последствий подобных операций [Текст] / Д. М. Коваленко, Г. А. Остапенко, М. А. Баленко, Н. Н. Толстых // Информация и безопасность. – 2011. – Т. 14. – Вып. 3. – С. 381–390.

39. Колюбанов, А. А. Моделирование процесса спам-атаки, реализуемого с помощью поисковых роботов [Текст] / А. А. Колюбанов, В. А. Транин, И. Л. Батаронов // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 312-315.

40. Корнев, И. А. Риски информационной безопасности при использовании электронных денежных средств [Текст] / И. А. Корнев, Л. Г. Попова // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 253–254.

41. Куликов, С. С. Расчет общего риска информационно–телекоммуникационных систем при возникновении эффекта «unicast flooding» в нескольких компонентах [Текст] / С. С. Куликов, Г. А. Остапенко // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 199–202.

42. Любченков, А. В. Алгоритмизация оценки эффективности применения средств пассивной защиты на объектах информатизации [Текст] / А. В. Любченков, Л. В. Паринова // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 316-319.

43. Любченков, А. В. Особенности взаимодействия владельцев информационных ресурсов при передаче конфиденциальной информации [Текст] / А. В. Любченков, В. Г. Юрасов // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 185–190.

44. Макаров, О. Ю. К вопросу построения модели риск–анализа выживаемости распределенных автоматизированных информационных систем [Текст] / О. Ю. Макаров, Д. Г. Плотников, А. С. Рогозина // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 265–266.

45. Машин, С. В. Описание вирусной атаки на компьютерные системы с помощью выборочного нормального распределения [Текст] / С. В. Машин, В. Г. Юрасов, И. А. Корейщиков // Информация и безопасность. – 2012. – Т. 15. – Вып. 1. – С. 121–124.

46. Оценка рисков наступления ущербов автоматизированных систем при атаках вирусного характера [Текст] / С. В. Машин, Н. М. Тихомиров, А. Е. Киселев, А. Ю. Зацепин // Информация и безопасность. – 2011. – Т. 14. – Вып. 3. – С. 443–446.

47. Машин, С. В. Параметры риска для автоматизированных систем, атакуемых вирусами [Текст] / С. В. Машин, К. А. Разинкин, А. Ю. Зацепин // Информация и безопасность. – 2011. – Т. 14. – Вып. 3. – С. 467–468.

48. Машин, С. В. Функции чувствительности риска при вирусных атаках на автоматизированные системы [Текст] / С. В. Машин, Н. И. Баранников, А. Ю. Зацепин // Информация и безопасность. – 2011. – Т. 14. – Вып. 3. – С. 391–400.

49. Менжулин, Р. В. Оценка рисков и регулирование защищенности распределенной платежной системы, на основе банкоматов [Текст] / Р. В. Менжулин, Г. А. Остапенко, Л. В. Паринова // Информация и безопасность. – 2011. – Т. 14. – Вып. 3. – С. 359–380.

50. Менжулин, Р. В. Риск–модели мошеннических операций в распределенных платежных системах на основе банковских карт [Текст] / Р. В. Менжулин, Г. А. Остапенко, О. Ю. Макаров // Информация и безопасность. – 2011. – Т. 14. – Вып. 3. – С. 337–358.

51. Мещеряков, В. А. Об отнесении информационной системы к категории «государственных информационных систем» [Текст] / В. А. Мещеряков, В. П. Железняк, О. А. Остапенко // Информация и безопасность. – 2014. – Т. 17. – Вып. 3. – С. 500-503.

52. Мордовин, А. И. Методика оценки рисков в процессе реализации атаки Каминского [Текст] / А. И.

Мордовин, О. А. Остапенко // Информация и безопасность. – 2014. – Т. 17. – Вып. 3. – С. 432-435.

53. Инновационные тренды в организации учебного процесса подготовки специалистов по защите информации: формирование компетенций в области управления информационными рисками и обеспечении безопасности инфокоммуникационных технологий [Текст] / Д. А. Новиков, В. И. Борисов, А. Г. Остапенко, А. О. Калашников, Г. А. Остапенко, Е. С. Соколова, Н. Н. Корнеева // Информация и безопасность. – 2014. – Т. 17. – Вып. 3. – С. 360-365.

54. Остапенко, А. Г. Исследование возможностей регулирования рисков автоматизированных систем при защите от атак типа «отказ в обслуживании» [Текст] / А. Г. Остапенко, С. А. Тишков // Информация и безопасность. – 2009. – Т. 12. – Вып. 1. – С. 25–38.

55. Логлогистическое распределение ущерба: расчёт риска ИТКС на основе параметров риска её компонентов [Текст] / А. Г. Остапенко, Д. Г. Плотников, О. А. Остапенко, П. А. Маслихов // Информация и безопасность. – 2012. – Т. 15. – Вып. 3. – С. 425–428.

56. Остапенко, А. Г. Основы риск-анализа и управления эффективностью флуд-атакуемых информационных систем [Текст] / А. Г. Остапенко, В. В. Бутузов, И. В. Шевченко // Информация и безопасность. – 2014. – Т. 17. – Вып. 1. – С. 88-91.

57. Остапенко, А. Г. Перспективы развития методологии риск–анализа систем [Текст] / А. Г. Остапенко, Д. О. Карпеев, Д. Г. Плотников // Информация и безопасность. – 2009. – Т. 12. – Вып. 3. – С. 419–424.

58. Предупреждение и минимизация последствий компьютерных атак на элементы критической информационной инфраструктуры и автоматизированные информационные системы критически важных объектов: риск–анализ и оценка эффективности защиты [Текст] / А. Г. Остапенко, Е. В. Ермилов, А. Н. Шершень, Е. С. Соколова,

И. В. Шевченко // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 167–178.

59. Остапенко, А. Г. Риски ущербности, шансы полезности и жизнестойкость компонент автоматизированных систем в условиях воздействия на них информационных угроз [Текст] / А. Г. Остапенко, Е. В. Ермилов, А. О. Калашников // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 215–218.

60. Формализация процесса управления рисками в информационно-технологической инфраструктуре критически важного объекта [Текст] / А. Г. Остапенко, А. О. Калашников, Е. В. Ермилов, Н. Н. Корнеева // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 164-179.

61. Остапенко, А. Г. Функция возможности в оценке рисков, шансов и эффективности систем [Текст] / А. Г. Остапенко // Информация и безопасность. – 2010. – Т. 13. – Вып. 1. – С. 17–20.

62. Алгоритмизация оценки живучести сетевых информационных структур [Текст] / Г. А. Остапенко, Я. С. Мишина, В. И. Белоножкин, И. В. Шевченко // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 304-307.

63. Остапенко, Г. А. Аналитическое моделирование процесса реализации DDOS–атаки типа HTTP–flood [Текст] / Г. А. Остапенко, М. В. Бурса, Е. Ф. Иванкин // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 107–110.

64. Остапенко, Г. А. Жизнестойкость элементов критической информационной инфраструктуры: аналитическая оценка с учетом возможных ущербов [Текст] / Г. А. Остапенко, Д. Г. Плотников, А. С. Рогозина // Информация и безопасность. – 2013. – Т. 16. – Вып. 3. – С. 353-364.

65. Информационные ресурсы инновационных проектов: риск–моделирование в условиях DDoS–атак [Текст] / Г. А. Остапенко, М. В. Бурса, Е. А. Попов, С. С. Вяхирева // Информация и безопасность. – 2012. – Т. 15. – Вып. 3. – С. 345–352.

66. К вопросу об оценке ущерба и жизнестойкости атакуемых распределенных информационных систем: развитие методического обеспечения [Текст] / Г. А. Остапенко, Д. Г. Плотников, Н. Ю. Щербакова, В. С. Зарубин // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 141–142.

67. Остапенко, Г. А. Концептуальный подход к расчету и регулированию рисков нарушения актуальности информации в элементах критической информационной структуры [Текст] / Г. А. Остапенко, А. Н. Шершень, А. О. Калашников // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 239–242.

68. Методика риск–анализа систем, атаки на которые предусматривают внедрение вредоносного программного обеспечения: экспоненциальные модели [Текст] / Г. А. Остапенко, Н. М. Радько, Д. Г. Плотников, А. А. Голозубов, А. Н. Шершень // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 99–102.

69. Остапенко, Г. А. Методическое и алгоритмическое обеспечение расчета параметров рисков для компонентов распределенных систем [Текст] / Г. А. Остапенко, Д. Г. Плотников, Е. А. Мешкова // Информация и безопасность. – 2010. – Т. 13. – Вып. 3. – С. 335–350.

70. Остапенко, Г. А. Методическое и алгоритмическое обеспечение расчета распределенных систем на основе параметров рисков их компонент [Текст] / Г. А. Остапенко, Д. О. Карпеев // Информация и безопасность. – 2010. – Т. 13. – Вып. 3. – С. 373–380.

71. Модели выживаемости атакуемой распределенной информационной системы: риск–формализация с учетом возможного ущерба [Текст] / Г. А. Остапенко, Д. Г. Плотников, Н. Ю. Щербакова, Н. И. Баранников // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 63–68.

72. Оценка защищенности ресурсов информационно-телекоммуникационных систем, подвергающимся DDOS-атакам [Текст] / Г. А. Остапенко, М. В. Бурса, Н. И.

Баранников, И. Л. Батаронов // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 496-497.

73. Остапенко, Г. А. Построение функций ущерба и риска для компьютерных атак, приводящих к нарушению доступности к информации [Текст] / Г. А. Остапенко, Е. В. Ермилов, А. О. Калашников // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 207–210.

74. Программная реализация алгоритмов риск–анализа распределенных систем [Текст] / Г. А. Остапенко, С. С. Куликов, Д. Г. Плотников, Ю. С. Науменко // Информация и безопасность. – 2011. – Т. 14. – Вып. 1. – С. 53–60.

75. Распределенные системы: методологии оценки эффективности в условиях атак [Текст] / Г А. Остапенко, Д. Г. Плотников, Р. В. Батищев, И. В. Гончаров // Информация и безопасность. – 2010. – Т. 13. – Вып. 3. – С. 359–366.

76. Остапенко, Г. А. Риск-анализ деструктивных воздействий на информационно-телекоммуникационные системы при нерегулярном гамма распределении [Текст] / Г. А. Остапенко, Е. А. Попов, А. С. Двоенко // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 336-337.

77. Риски распределенных систем: методики и алгоритмы оценки и управления [Текст] / Г. А. Остапенко, Д. О. Карпеев, Д. Г. Плотников, Р. В. Батищев, И. В. Гончаров, П. А. Маслихов, Е. А. Мешкова, Н. М. Морозова, С. А. Рязанов, Е. В. Субботина, В. А. Транин // Информация и безопасность. – 2010. – Т. 13. – Вып. 4. – С. 485–530.

78. Остапенко, Г. А. Риск-модель инновационного проекта, функционирующего в условиях угроз реализации ddos-атак [Текст] / Г. А. Остапенко, М. В. Бурса, Н. Н. Толстых // Информация и безопасность. – 2013. – Т. 16. – Вып. 3. – С. 443-444.

79. Паринов, А. В. Риск-оценка смертности инновационных проектов: научно-методические основы [Текст] / А. В. Паринов, Л. В. Паринова, В. Г. Юрасов // Информация и безопасность. – 2013. – Т. 16. – Вып. 3. – С. 423-426.

80. К вопросу об оценке рисков атакуемых распределенных информационных систем: развитие математического обеспечения [Текст] / Л. В. Паринова, Н. М. Радько, А. Г. Остапенко, В. Л. Каркоцкий, Д. Г. Плотников // Информация и безопасность. – 2012. – Т. 15. – Вып. 4. – С. 585–586.

81. Пастернак, Ю. Г. К вопросу моделирования процесса реализации атак посредством компьютерных червей [Текст] / Ю. Г. Пастернак, Н. Н. Корнеева, К. В. Дегтярева // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 330-331.

82. Пахомова, А. С. Анализ применимости классификации шаблонов атак CAPEC для описания угроз компьютерного шпионажа [Текст] / А. С. Пахомова, О. А. Остапенко // Информация и безопасность. – 2014. – Т. 17. – Вып. 3. – С. 472-475.

83. Пахомова, А. С. К вопросу о разработке структурной модели угрозы компьютерной разведки [Текст] / А. С. Пахомова, А. П. Пахомов, К. А. Разинкин // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 115–118.

84. Пахомова, А. С. Об использовании классификации известных компьютерных атак в интересах разработки структурной модели компьютерной разведки [Текст] / А. С. Пахомова, А. П. Пахомов, В. Г. Юрасов // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 81–86.

85. Пахомова, А. С. Целенаправленные угрозы компьютерного шпионажа: признаки, принципы и технологии реализации [Текст] / А. С. Пахомова, О. Н. Чопоров, К. А. Разинкин // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 211–214.

86. Плотников, Д. Г. Алгоритмическое обеспечение риск–анализа систем в диапазоне ущербов [Текст] / Д. Г. Плотников, Д. Б. Борисов, О. Ю. Макаров // Информация и безопасность. – 2011. – Т. 14. – Вып. 4. – С. 603–606.

87. Плотников, Д. Г. Оценка рисков ИТКС в условиях синхронных и асинхронных атак в случае логлогистического распределения плотности вероятности наступления ущерба [Текст] / Д. Г. Плотников, Д. Б. Борисов, В. С. Зарубин // Информация и безопасность. – 2012. – Т. 15. – Вып. 1. – С. 141–142.

88. Пономаренко, Е. Н. Модель реализации атаки с использованием email-worm в автоматизированной информационной системе [Текст] / Е. Н. Пономаренко, В. С. Арефьев, Е. Ф. Иванкин // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 194-199.

89. Попов, Е. А. DOS-атаки на инновационные государственные распределенные информационные системы: риск-анализ при нерегулярном распределении ущерба [Текст] / Е. А. Попов, Г. А. Остапенко // Информация и безопасность. – 2014. – Т. 17. – Вып. 3. – С. 452-455.

90. Попов, Е. А. DOS-атаки на инновационные государственные распределtнные информационные системы: риск-анализ при нерегулярном распределении ущерба [Текст] / Е. А. Попов, Г. А. Остапенко // Информация и безопасность. – 2014. – Т. 17. – Вып. 3. – С. 456-459.

91. Риск–анализ атакуемых информационно–телекоммуникационных систем с использованием нерегулярного распределения [Текст] / Е. А. Попов, Н. Ю. Щербакова, Н. М. Тихомиров, А. Н. Шершень // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 39–46.

92. Риск-анализ информационно-телекоммуникационных систем при аддитивном характере параметра нерегулярности [Текст] / Е. А. Попов, Н. Н. Корнеева, О. Н. Чопоров, А. В. Заряев // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 482-485.

93. Радько, Н. М. Задача риск–анализа атак «вредоносами» [Текст] / Н. М. Радько, А. А. Голозубов, О. Ю. Макаров // Информация и безопасность. – 2013. – Т. 16. – Вып. 1. – С. 139–140.

94. Радько, Н. М. Методический подход к определению эпистойкости автоматизированной информационной системы (АИС), атакуемой вирусами [Текст] / Н. М. Радько, В. А. Теслинов, Н. Н. Толстых // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 252-255.

95. Некоторые оценки рисков, шансов и живучести сетей в условиях информационных атак вирусного характера [Текст] / Н. М. Радько, Л. В. Паринова, Ю. Г. Пастернак, К. А. Разинкин, Н. М. Тихомиров // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 498-499.

96. Противодействие вирусным атакам на сетевые структуры на основе риск-оценки [Текст] / Н. М. Радько, Л. В. Паринова, Ю. Г. Пастернак, К. А. Разинкин, Н. М. Тихомиров // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 502-503.

97. Риска-анализ систем при множестве источников информационных инфекций [Текст] / Радько Н. М., Паринова Л. В., Пастернак Ю. Г., Разинкин К. А., Тихомиров Н. М. // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 504-505.

98. Радько, Н. М. Риски ущербности, шансы полезности и эпистойкость информационно-телекоммуникационной системы в условиях распространения информационной эпидемии по модели MSEIR [Текст] / Н. М. Радько, В. В. Дорожкин, А. Г. Остапенко // Информация и безопасность. – 2014. – Т. 17. – Вып. 1. – С. 100-103.

99. Тотальные вирусные атаки на распределенные информационные системы: обобщенные модели оценки рисков возникновения эпидемий и шансов эффективного противодействия им [Текст] / Н. М. Радько, Л. В. Паринова, Ю. Г. Пастернак, К. А. Разинкин, Н. М. Тихомиров // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 500-501.

100. Разинкин, К. А. Удаленные деструктивные воздействия на распределенные автоматизированные системы [Текст] / К. А. Разинкин, С. В. Машин, А. Е. Киселев //

Информация и безопасность. – 2011. – Т. 14. – Вып. 4. – С. 627–628.

101. Рябков, В. Е. О применении методов визуального анализа многомерных данных в области защиты информации [Текст] / В. Е. Рябков, А. П. Пахомов, Н. И. Баранников // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 259–260.

102. Аналитические вероятностные модели реализации атак на DNS-серверы [Текст] / Е. Е. Смолькина, А. Г. Остапенко, Н. И. Баранников, И. Л. Батаронов // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 596-603.

103. Тихомиров, Н. М. К вопросу о защите информации в сотовых сетях стандарта LTE с интегрированными фемтосотами [Текст] / Н. М. Тихомиров, Н. С. Коленбет // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 261–262.

104. Транин, В. А. Инновации в социальных сетях: к вопросу оценки вероятности сбора информации с использованием поддельного профиля [Текст] / В. А. Транин, Ю. А. Кутузова, Л. В. Паринова // Информация и безопасность. – 2013. – Т. 16. – Вып. 3. – С. 433-434.

105. Транин, В. А. Оценка уровня реальной защищенности элементов критической информационной инфраструктуры, включая обнаружение и предупреждение компьютерных атак при помощи поисковых средств в социальных сетях [Текст] / В. А. Транин, Ю. А. Кутузова, А. В. Заряев // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 223–226.

106. Чопоров, О. Н. Анализ затухания радиоволн беспроводной связи внутри зданий на основе сравнения теоретических и экспериментальных данных [Текст] / О. Н. Чопоров, А. П. Преображенский, А. А. Хромых // Информация и безопасность. – 2013. – Т. 16. – Вып. 4. – С. 584-587.

107. Чукова, Д. И. Проблемы обеспечения информационной безопасности международного центра обмена

информации подразделений финансовых разведок [Текст] / Д. И. Чукова, Л. В. Паринова // Информация и безопасность. – 2013. – Т. 16. – Вып. 2. – С. 263–264.

108. Щербаков, В. Б. К вопросу о классификации основных видов атак в сотовых сетях стандарта LTE [Текст] / В. Б. Щербаков, Н. С. Коленбет, Н. М. Тихомиров // Информация и безопасность. – 2014. – Т. 17. – Вып. 2. – С. 334-335.

109. Построение матрицы чувствительности рисков для субъектов социальной информационной сети [Текст] / В. Г. Юрасов, Д. М. Коваленко, Г. А. Остапенко, М. А. Баленко // Информация и безопасность. – 2011. – Т. 14. – Вып. 3. – С. 401–408.

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к самостоятельным работам по дисциплине
«Управление рисками в распределенных
информационных системах»
для студентов специальности
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Составители:
Соколова Елена Сергеевна
Остапенко Александр Григорьевич

В авторской редакции

Подписано к изданию 27.04.2015.
Уч.-изд. л. 1,7.

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