Содержание

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

ВВЕДЕНИЕ

Актуальность исследования

С развитием в России информационных технологий широкое распространение получила всемирная сеть - интернет, зарекомендовавшая себя в качестве удобного информационного источника. В стране с каждым днем увеличивается количество пользователей интернета, в любых организациях и предприятиях присутствует доступ во всемирную сеть[1,3,7].

Однако ситуация связанная с распространенностью сети интернет характеризуется и рядом негативных признаков. Наряду с информатизацией наблюдается и возрастание интереса к сети со стороны криминальных кругов[34, 41]. По мере увеличения количества пользователей интернета и все большей циркуляции информации в сети возникает опасность хищения этой информации заинтересованными лицами. Анализ динамики видов преступлений позволяет сделать вывод о росте числа правонарушений в сфере компьютерной информации, который идет не менее быстрыми темпами, чем компьютеризация в России. Одновременно непрекращающееся увеличение числа пользователей персональных компьютеров и сети интернет в последние годы породило множество незаконных явлений, атаки хакеров на web-рессурсы, распространение программно-математических средств, «троянских» программ, интернет-мошенничество, спам, распространение детской порнографии, и кибертерроизм[44, 55, 104].

В современном обществе роль глобальной информационной сети интернет - немаловажна. Для многих людей пользование интернетом стало привычным делом, наряду с чтением газет, просмотром телевизионных передач. Многие уже не могут представить свою жизнь без социальных сетей, веб-форумов, новостных лент, различных сайтов «тумблеров», содержащих фото и видео подборки тематического материала[1-7]. Популярность и доступность интернета приводит к тому, что с каждым днем все большее и большее количество пользователей привязываются к данному источнику информации. Внимание огромнейшей массы людей приковано к относительно небольшому количеству веб-ресурсов, которые они посещают

регулярно. Для поддержки такого рода ресурсов используют специальное оборудование, позволяющее сразу обслуживать множество пользователей. Остальные редко посещаемые или узкоспециализированные ресурсы не нуждаются в таком дорогостоящем оборудовании, ведь работают одновременно с небольшим количеством пользователей. Случается такие события, что популярные ресурсы размещают в своих новостных лентах ссылки на другие сайты, которые не рассчитаны на столь множественные запросы, и это приводит к перегрузке последних[3, 5-9, 76]. Работа сервера становится невозможной, все запросы пользователей не выполняются. Собственник сайта при этом терпит ущерб от упущенной прибыли, затраты на восстановление нормальной работы сайта и ликвидации последствий атаки, но с другой стороны это является своеобразной рекламой сайта, и повышение его рейтинга в поисковых системах. Эта ситуация аналогична атаке в отказе в обслуживании, только без участия злоумышленников, она называется слэшдот-эффект[1, 3-7]. Это проблема особенно актуальна в развитых странах Европы и Америки, где процент пользователей сети интернет от общего числа населения велик. На данный момент населением России все еще происходит освоение всемирной паутины. В России около 43% от общего числа людей имеют доступ к сети, когда в большинстве развитых стран эта цифра приближается к 80%, а в наиболее развитых более 90% (данные веб-ресурса wikipedia.org). Отсюда следует, что для Российских веб-ресурсов проблема слэшдот-эффекта вскоре также станет актуальна[6].

В связи с этим, рассмотрение риск-анализаслэшдот атак – крайне актуальная задача. Она является сложной и многогранной, так как требует исследования множества факторов[56, 89, 106]. Одним из таких факторов является математическое моделирование атак, которое позволит оценить, во-первых, возможный ущерб от успешной атаки на заданную автоматизированную систему, во-вторых - эффективность используемых средств защиты.

В данном случае под математическим моделированием понимается построение риск-моделейслэшдот атак на автоматизированные системы.

Данные модели являются необходимым инструментом для изучения и анализа слэшдот атак.

Степень проработанности темы

Атаки «слэшдот» эффект достаточно новое явление для современного информационного общества. На данный момент «слэшдот» эффект изучен не полностью, что затрудняет оценку рисков, уровень которых, как известно, определяет степень защищенности (безопасности) систем.

Вместе с тем, довольно успешно [48-50] сейчас развивается методология риск-анализа, широко применимая в теории и практике обеспечения информационной безопасности. Ее совершенствование в контексте повышения защищенности высоконагруженных автоматизированных систем общего доступа, имеющие подключение к сети интернет, на основе оценки и регулирования рисков представляется весьма актуальным.

Учитывая актуальность явления и недостаточную эффективность решений для регулирования рисков высоконагруженных автоматизированных систем общего доступа, имеющих подключение к сети интернет, подвергшихся атаке слэшдот эффект, возникает необходимость в более глубоком и детальном изучении данной проблемы. Изучив существующие научные исследования и экспериментальные работы в области атак отказа в обслуживания, такие как - отслеживание источника атаки,ограничение допустимого предела, фильтрация не подписанных пакетов, возникает противоречие в частом возникновении атак и отсутствии действительно эффективных решений для избегания сильных отрицательного последствий. Из противоречия следует явная проблемав отсутствии регулирующих механизмов, которые позволят владельцам интернет ресурсов сократить материальные потери в результате неблагоприятного исхода. Для разрешения проблемы предложим инновационный и актуальный на сегодняшний день метод решения, отраженный в цели данной выпускной квалификационной работе.

Цель работы: состоит в оценивание рисков высоконагруженных автоматизированных систем общего доступа, обусловленных атакой

слэшдот-эффект. Для достижения поставленной цели необходимо решить следующие задачи:

1. Произвести анализ, рассмотреть сущность, условие возникновения и деструктивное воздействие атаки слэшдот-эффект, на высоконагруженные автоматизированные системы общего доступа, имеющие подключение к сети интернет, собрать статистику для данных атак и найти закономерности которым она подчиняется.
2. Построение риск-модели, на основе закономерностей справедливых для атак слэшдот эффект, которая позволит рассчитать риски для деструктивных воздействий на высоконагруженные автоматизированные системы общего доступа, имеющие подключение к сети интернет, оценить условия при которых возможно регулирование рисков.
3. Произвести изучение распределенных атак типа слэшдот эффект, на высоконагруженные автоматизированные системы общего доступа, имеющие подключение к сети интернет, рассмотреть управление рисками предложить инновационное эффективное решение.

Объектом исследования являются высоконагруженные автоматизированные систем общего доступа, имеющие подключение к сети интернет, подверженные атаке слэшдот эффект.

Предметом исследования являются риски реализации деструктивных воздействий в сетях общего пользования, и явления в автоматизированных системах при реализации информационных атак.

В исследовании используются методы теории графов, системного анализа, методы экспертных оценок и математического моделирования, численные методы расчета и анализа, методы теории рисков, теории вероятности, математической статистики, системного анализа, интегральных оценок, применения функций чувствительности.

Научная новизна. В данной работеиспользована теория оценки рисков для высоконагруженных систем общего доступ имеющих подключение к сети интернет, обусловленных атакой слэшдот эффект. Ранее данный вопрос не был должным образом рассмотрен в теории оценки рисков для

распределенных атак на автоматизированные системы. Проблема отказа в обслуживании не решалась по представленному алгоритму управления рисками, из-за недостаточной исследовательской базы.

1. Выбранное для изучение распределение впервые рассматривается в теории риск-анализа, главным отличием от ранее изученных аналогов является наличие новых зависимостей значения риска от реализуемых атак, от параметров q-экспоненциального распределения.

2. Исследования в отличие от аналогичных проводились для распределенных автоматизированных систем общего доступа имеющих подключение к сети интернет, обусловленных атакой слэшдот эффект.

3. В отличие от аналогов предложен алгоритм управления рисками основанный на регулировании мощности сервера, ранее с этой стороны вопрос не рассматривался, введенный метод является инновационным.

4. В отличие от раннее представленных алгоритмов, данная разработка является практически применима для организаций предоставляющих хостингдля сайтов, и полностью автоматизирована.

На защиту выносятся следующие основные результаты работы:

- описательная модель высоконагруженных автоматизированных систем общего доступа, обусловленных атакой слэшдотэффект;

- алгоритм построение риск-модели автоматизированной системы при реализации слэшдот атак, исследование распределения и расчет оновных параметров риска

- Организация управления рисками при реализации слэшдот атак в случае асинхронных атак при определении риска с помощью интегральной оценки;

- результаты сравнения программных средств, реализующих технологию аппаратной виртуализации, приДИВ, направленных на нарушение доступности защищаемой информации в КС.

Практическая ценность работы заключается в оценивание рисков высоконагруженных автоматизированных систем общего доступа,

обусловленных атакой слэшдот-эффект, важным критерием функционирования которой является обеспечение доступности информации.

Построенная риск-модель может применяться для оценки рисков осуществления атак типа слэшдот эффект, для любых интернет ресурсов, которые имеют ограниченный по количеству запросов доступ к серверу, а также построения систем, устойчивых к воздействию стремительного наплыва посетителей. Полученные выражения для интегрального риска данных систем и его экстремумов позволяют оценить защищенность системы в целом, а также выявить наиболее уязвимые компоненты.

Подход к регулированию риска в случае реализации асинхронных атак может применяться для снижения риска осуществления атак типа слэшдот эффект, в частности, он позволяет снизить среднее значение ущерба, наносимого владельцу интернет ресурсавцелом, путем регулирования параметров в компонентах системы. Это позволяет проводить мероприятия по управлению рисками выборочно, уделяя внимание защите лишь в тех случаях, когда существует реальная угроза экономических потерь организации-владельцу ресурса, что уменьшает затраты на защиту.

Структура и объем работы. Работа состоит из введения, пяти глав, заключения и списка литературы, включающего 112 наименований.

Заключение

Работа посвящена оцениванию рисков высоконагруженных автоматизированных систем общего доступа, обусловленных атакой слэшдот-эффект. В ходе еѐ выполнения были получены следующие основные результаты:

1. В проделанной работе изучен процесс осуществления атаки, изучены существующие научные исследования и экспериментально наработанные данные в представленной проблеме.Приведено описание протекания атаки, причины ее возникновения, построена математическая описательная риск-модель приведены и возможные способы уменьшения ущерба от ее негативных последствий.

2. Разработана методика оценивание рисков, с помощью интегральных оценок риска, рассмотрен вариант ассинхронной распределенной атаки на высоконагруженные автоматизированные системы общего доступа, обусловленных атакой слэшдот-эффект.

3. В работе был использован подход который ранее применялся к данной проблеме не достаточно эффективно, при этом выдвинуты гипотезы о корреляции времени отклика с ущербом от атаки и равномерное распределение коэффициентов распределения при реальной атаке. Данный подход, а именно – интегральная оценка рисков и управление рисками является нестандартной для данной проблемы – атак слэшдот эффект.

4. В работе выявлена закономерность изменения рисков от регулирования внешних параметров, наибольшей эфффективностью в регулировании является параметр q, что дает возможность широкого применения, а также перспективность данного подхода. В ходе работы был использован ранее введенный понятийные аппарат.

5. В ходе исследований была сопоставлена статистика времени отклика сервера и ущерба от проведения атаки, и определена их корреляция

близкая к единице. Что позволила импользовать данные взятые непосредственно с атакуемого сервера.

6. Применительно к проблематике работы эффективно, то есть с получением обладающих новизной результатов использовались различные общенаучные и частнонаучные методы исследования такие, как: диалектический метод, методы системного анализа, математического моделирования, численные методы расчета и анализа, методы теории рисков, теории вероятности, математической статистики и системного анализа.

7. Коценивание рисков высоконагруженных автоматизированных систем общего доступа, обусловленных атакой слэшдот-эффект данный метод исследований ранее не применялся, следовательно проведенные исследования обладают новизной результатов, также представленный алгоритм управления мощностью сервера является инновационным.

8. В данной работе выявлена тенденция уменьшения значения риска для высоконагруженных автоматизированных систем общего доступа, обусловленных атакой слэшдот-эффект при увеличении мощности сервера, также изменение значений риска с помощью регулирования внешних параметров.

9. В ходе работы было установлено, что атака протекает не в результате действий злоумышленника, а при действии простых пользователей, что является неким противоречием определению атака. Это также означает что каждая атака обладает случайными характеристиками, так как простые пользователи не будут моделировать специальные ситуации.

10. Также выявлены некоторые положительные стороны атаки – увеличение популярности интернет ресурса, но в рамках данной работы этот эффект не рассматривается, так как является следствием атаки, то есть владелец ресурса уже понес ущерб.

11. Расчет интегральной оценки рисков состоящей изn компонент, для определения момента увеличения мощности сервера ранее не проводилось.

12. Для дальнейшего развития темы может послужить более точная оценка корреляции времени отклика сервера и ущерба от проведения атаки, также в итоговой оценке рисков может быть определена и учтена «положительная» сторона данной атаки, но данное утверждения нуждается в дополнительном глубоком изучении, так как положительная сторона эффекта имеет специфическое проявление

13. Идея данной проблемы была взята из практики использования интернет ресурсов, при прекращении работы с ресурсом в результате большого времени отклика сервера.

14. Дынная работа не имеет источников, с которыми можно было бы осуществить сравнения, так как данный подход к оцениванию рисков высоконагруженных автоматизированных систем общего доступа, обусловленных атакой слэшдот-эффект, используется впервые. Также использование q-экспоненциального распределения является инновационным шагом.

15. Оценка достоверности результатов исследования основана на открытой статистике отечественных и зарубежных социальных информационных систем, а также известных топологических схемах СИС. Идея работы базируется на использовании адаптационного подхода, анализа и практики передового опыта в области исследования процессов, протекающих в автоматизированных системах.

16. В результате сравнения разработанной модели и моделей, рассмотренных в литературных источниках отражающих в основном физическую составляющую атак, была выявлена большая эффективность применения авторской модели.

17. В работе использованы результаты применения современных систем сбора и обработки исходной информации, в частности, – статистических данных. Применялись методы их анализа и предварительной обработки.

18. Личный вклад состоит в непосредственном участии в нахождении и анализе исходных данных, проведении научных исследований, обработке и интерпретации полученных экспериментальных данных, идеи регулирования рисков путем изменения мощности сервера.

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

Список литературы

1 AmyJoKim. Community building on the Web, 2011 – 178c.

2 Bettina Rehmann Deliberative Nerdocracy. The Online Public Sphere of Slashdot and Digg, 2009 –321c.

3 Chromatic,BrianAker,DaveKrieger.Running weblogs with Slash, 2010 – 289 c.

4 Halavais, Alexander M. Campbell. The Slashdot effect: analysis of a large-scale public conversation on the World Wide Web, 2011 – 248 c.

5 Lambert M. Surhone, Miriam T. Timpledon, Susan F. Marseken. Slashdot, 2010 – 289 c.

6 Markus Schumacher. Security engineering with patterns: origins, theoretical model, and new applications, 2009. -156 c.

7 Rob Malda, Anonymous Coward, Jon Katz. Slashdot, 2011. – 345 c.

8 Stuff That Matters. Slashdot and the Emergence of Open News, 2010. – 278 c.

9 АлексейОвчаров.Диссертация«Определениесвойствфрагментасетивусловиях, близкихкпредельным (загрузканауровне 70-100%)», 2000. – 120 с.

10 Андреев Д.А., Брянский А.Е. Вирусы и риски заражения систем: Обзор и построение обобщенных вероятностных моделей // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2009. – Том. 12. – Часть. 4. - С. 519 – 536.

11 Андреев Д.А., Котрахов В.В., Остапенко А.Г. Компьютерные вирусы: классификация и статистический анализ // Информация и безопасность: Регион. науч.-техн. журнал. – Воронеж. 2010. – Том. 13. – Часть. 2. - С. 295 – 296.

12 Балдин К.В. Управление рисками: Учеб. пособие / К.В. Балдин, С.Н. Воробьев. – М.: ЮНИТИ-ДАНА, 2005. – 511с.

13 Бартон Т. Комплексный подход к безопасности сетей / Т. Бартон, У. Шенкир, П. Уокер. – М.: Издательский дом "Вильямс", 2003. – 208 с.

14 Безруков Н.Н. Компьютерная вирусология / Безруков Н.Н. - Киев: УРЕ, 1991. – 88 с.

15 Бендат Дж., Пирсол А. Прикладной анализ случайных данных. М.: Мир, 1989.– 540 с.

16 Боровиков А.А. Теория вероятностей /А.А. Боровиков – М.: Наука, 1986. – 432 с.

17 Бостанджиян В.А. Пособие по статистическим распределениям/ В.А. Бостанджиян. - Черноголовка: ИПХФ, 2000. – 1006 с.

18 Буянов В.П., Уфимцев Ю.С. Методика информационной безопасности. М.: «Экзамен», 2004. – 148 с.Вадзинский Р.Н. Справочник по вероятностным распределениям – Санкт-Петербург.: «Наука», 2001. – 149 с.

19 Вентцель Е.С. Теория вероятностей и ее инженерные приложения. Учеб. пособие для втузов. / Е.С. Вентцель, Л.А. Овчаров. – М.: Высш. шк, 2003. – 464 с.

20 Вентцель Е.С. Теория случайных процессов и ее инженерные приложения. Учеб. пособие для втузов. / Е.С. Вентцель, Л.А. Овчаров. – М.: Высш. шк, 2000. – 383 с.

21 Воронцовский А.В. Управление рисками: Учеб. пособие. 2-ое изд., испр. и доп / А.В. Воронцовский – СПб: Изд-во С.-Петерб. ун-та, 2000; ОЦЭиМ, 2004. – 458 с.

22 Выгодский М.Я. Справочник по высшей математике / М.Я. Выгодский – М.: Наука, 1973. – 872 с.

23 Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 84 с.

24 Герик Т. Информационная база для оценки риска / Т. Герик //LAN: журнал сетевых решений, 2006. – №9. – С. 22-25.

25 Гмурман В. Е. Теория вероятностей и математическая статистика.– М.: Высшая школа, 2004.– 148 с.

26 Гнеденко Б.В. Математические методы в теории надежности. / Б.В. Гнеденко, Ю.К. Беляев, А.Д. Соловьев. – М.: Наука, 1965. – 333 с.

27 Гончаренко Л.П. Риск-менеджмент: учебное пособие / Под ред. д-ра тех. наук. проф., засл. деятеля науки РФ Е.А. Олейникова; Л.П. Гончаренко, С.А. Филин. – М.: КНОРУС, 2006. – 216 с.

28 ГОСТ 12.1.003-83. Шум. Общие требования безопасности. — М.: Изд-во стандартов, 1986. — 9 с.

29 ГОСТ 12.1.005-88. Воздух рабочей зоны. Общие санитарно-гигиенические требования. — М.: Изд-во стандартов, 1988. — 75 с.

30 ГОСТ 12.1.032-78. Рабочее место при выполнении работ сидя. Общие эргономические требования. — М.: Изд-во стандартов, 1992. — 9 с.

31 ГОСТ 12.1.030-81. Электробезопасность. Защитное заземление, зануление. — М.: Изд-во стандартов, 1986. — 9 с.

32 ГОСТ 12.1.019-79. Электробезопасность. Общие требования. — М.: Изд-во стандартов, 1986. — 6 с.

33 ГОСТ 12.1.004-91. Пожарная безопасность. Общие требования. — М.: Изд-во стандартов, 1991. — 77 с.

34 Громов Ю.Ю. Классификация видов атакующих воздействий на информационную систему / Ю.Ю. Громов, В.О. Драчев, В.В. Войтюк, Ю.Ф. Мартемьянов, А.Ю. Громова // Журнал «Информация и безопасность». – Воронеж: ВГТУ, 2010. – Вып. 3 – С. 413-418.

35 Грушо А.А.. Тимонина Е.Е. Теоретические основы защиты информации. - М.: Издательство Агентства «Яхтсмен». 1996. – 192 с.

36 Гусак А.А. Высшая математика: учебник для студентов вузов / А.А. Гусак. – Мн.: ТетраСистемс, - 2004. – 5-е изд. - Т.2- 448 с.

37 Естественное и искусственное освещение. СНиП 23/05-95. — М.: Стройиздат, 1995. — 48 с.

38 Зайденберг А.П. Законы распределения случайных величин / А.П. Зайденберг– Омск: Омский институт инженеров железнодорожного транспорта, 1971. – 253 с.

39 Зражевский В.В. Основные направления совершенствования системы управления рисками / В.В. Зражевский. – М.: 1999. – 465 с.

40 Зубань С.С., Иохвидова А.Е., Остапенко О.А. Методический подход к синтезу распределенных систем с заданным уровнем риска // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 2. - С. 203 – 208.

41 Кадлоф А. Вирусы / А. Кадлоф. // Компьютер. -1990. - №1. – с. 44-47.

42 Карпеев Д.О., Плотников Д.Г., Дуплищева А.Ю. Расчет рисков атакуемых компонент информационно-вычислительных систем для дискретных законов распределения вероятности наступления ущербов // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 2. - С. 195 – 202.

43 Карпеев Д.О., Татаринцев А.Ю., Яковлев Д.С., Заряев А.В. Идентификация параметров нечетких моделей оценки информационных рисков информационных систем // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 1. - С. 37 – 42.

44 Касперски К. Записки исследователя компьютерных вирусов / К. Касперски - Издательство: Питер, 2005. – 316 с.

45 Кейт Дж. Джонс, Майк Шема, Бредли С. Джонсон. Анти-хакер. Средства защиты компьютерных сетей. - Издательство СП ЭКОМ, 2004. – 700 с.

46 Кендалл М. Теория распределений/ М. Кендалл, А. Стьюарт. – М.: Наука, 1966. – 590 с.

47 Кокс Д. Статистический анализ последовательностей событий / Д. Кокс, Льюис П. – М.: Издательство "МИР", 1969. – 312 с.

48 КоролюкВ.С., ПортенкоН.И., СкороходА.В., ТурбинА.Ф.Справочник по теории вероятностей и математической статистике/ – М.: Наука. Главная редакция физико-математической литературы, 1985. – 640с.

49 Куликов Е.И. Методы измерения случайных процессов/ Е.И. Куликов – М.: Радио и связь, 1986. – 272 с.

50 Куликов Е.И. Прикладной статистический анализ: Учеб.пособие для вузов/ Е.И. Куликов. – М.: Радио и связь, 2003. – 376 с.

51 Курило А.П. О проблеме компьютерной безопасности // Научно-техническая информация. Сер. 1. Орг. и методика информ. работы. – 1993. - №8. - 412 с.

52 Куринной Г.Ч. Математика: справочник. М.: Фолио, 2000.– 464 с.

53 Курносов Ю.В., Конотопов П.Ю. Аналитика: метрология, технология и организация информационно-аналитической работы / Ю.В.Курносов, П.Ю.Конотопов– М.: РУСАК, 2004. – 512с.

54 Лагунов В.С. Безопасность и экологичность в дипломном проекте: Учеб. пособие по дипломному проектированию. — Воронеж: Воронеж. гос. техн. ун-т, 2003. — 124 с.

55 Левин М. Как стать хакером / М. Левин– Издательство Новый издательский Дом, 2004. – 320 с.

56 Левин М. Руководство для хакеров 2. Электронные корсары / М. Левин– Издательство Новый издательский дом, 2005. – 208 с.

57 Линч Ф. Уильям, Стив Манзуик, РайянПемех и др. Защита от хакеров корпоративных сетей. – Издательство ДМК Пресс, 2005. – 864 с.

58 Липаев В.В. Анализ и сокращение рисков проектов сложных программных средств / В.В. Липаев– Издательство «Синтег», 2005. – 208 с.

59 Локхарт Э. Антихакинг в сети. Трюки / Э. Локхарт - Издательство: Питер, 2005. – 296 с.

60 Малошевский С.Г. Теория вероятностей: Учеб. пособие. Часть 1. Вероятностное пространство. Дискретные случайные величины / С.Г. Малошевский – СПб: Петербургский гос. ун-т путей сообщения, 1999.– 92 с.

61 Малюк А.А. Защита информации / А.А. Малюк – М.: МИФИ, 2002. – 52с.

62 Методические указания к выполнению организационно-экономической части дипломных проектов научно-исследовательского направления для студентов специальности 090102, 090105, 090106 дневного обучения / Воронеж, гос. техн. ун-т; Сост. И. А. Злобина. Воронеж, 2004. 26 с.

63 Михайлов С.Ф., Петров В.А., Тимофеев Ю. А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции: Учебное пособие. – М.: МИФИ, 1995. – 112 с.

64 Мирошников Б.Н. Борьба с преступлениями в сфере информационных технологий // Системы безопасности. 2002, №5(47). – 104 с.

65 Найт Ф.Х. Риск, неопределенность и прибыль. Пер. с англ. / Ф.Х. Найт– М.: Дело, 2003. – 360 с.

66 «О пожарной безопасности». ФЗ № 69 от 21.12.1994 г.

67 Остапенко Г.А. Оценка рисков и защищенности атакуемых кибернетических систем на основе дискретных распределений случайных величин / Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2005. – Вып. 2. – С. 70 – 75.

68 Остапенко Г.А., Карпеев Д.О., Плотников Д.Г., Батищев Р.В., Гончаров И.В., Маслихов П.А., Мешкова Е.А., Морозова Н.М., Рязанов С.В., Субботина Е.В., Траниин В.А.Риски распределенных систем: Методики и алгоритмы оценки и управления/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 4. - С. 485 – 530.

69 Остапенко Г.А., Карпеев Д.О.Методическое и алгоритмическое обеспечение расчета параметров рисков распределенных систем на основе параметров рисков их компонентов/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 3. - С. 373 – 380.

70 Остапенко Г.А., Маслихов П.А., Субботина Е.В. Способы регулирования рисков распределенных систем/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 3. - С. 435 – 438.

71 Остапенко Г.А.,Мешкова Е.А. Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия / Г.А. Остапенко, Е.А. Мешкова; Под редакцией Ю.Н. Лаврухина. – М: Горячая линия - Телеком, 2007. - 295 с.

72 Остапенко Г.А., Плотников Д.Г., Мешкова Е.А.Методическое и алгоритмическое обеспечение расчета параметров рисков для компонентов распределенных систем/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 3. - С. 335 – 350.

73 Остапенко Г.А., Транин В.А.Алгоритмическое обеспечение риск-анализа систем в диапазоне ущербов/ Г.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2010. – Том. 13. – Часть. 3. - С. 447 – 450.

74 Остапенко О.А. Методология оценки риска и защищенности систем/ О.А. Остапенко // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2005. – Вып. 2. – С. 28 – 32.

75 Остапенко О.А., Карпеев Д.О., Асеев В.Н., Морев Д.Е., Щербаков Д.Е. Риски систем: оценка и управление. – Воронеж: МИКТ, 2007. – 261 с.

76 Партыка Т.Л. Информационная безопасность / Т.Л. Партыка– Издательство «Форум», 2005. – 290 с.

77 Парфенов В.И. Защита информации (Словарь) / Парфенов В.И.– В.: НП РЦИБ «Факел», 2003.– 293 с.

78 Петраков А.В. Основы практической защиты информации. - М.: Радио и связь, 2000. – 368 с.

79 Петренко С.А. Управление информационными рисками: Экономически оправданная безопасность. / С.А. Петренко, С.В. Симонов. – М.: АйТи - Пресс, 2004. – 381 с.

80 Петренко С.А. Метод оценивания информационных рисков организации/ С.А. Петренко // сб.статей "Проблемы управления информационной безопасностью" под ред. д.т.н., профессора Черешкина Д.С., РАН ИСА, – М., Едиториал УРСС, 2002. – С. 112 - 124.

81 Пикфорд Дж. Управление рисками / Дж. Пикфорд – М.: ООО "Вершина", 2004. – 352 с.

82 Поллард Дж. Справочник по вычислительным методам статистики / Дж Поллард. – М.: Финансы и статистика, 1982. – 575 с.

83 Приходько А.Я. Информационная безопасность в событиях и фактах / А.Я. Приходько– М.: СИНЕГ, 2001. – 260с.

84 Приходько А.Я. Словарь-справочник по информационной безопасности / А.Я. Приходько – М.: СИНТЕГ, 2001. – 124 с.

85 Просветов Г.И. Управление рисками: задачи и решения: Учебно-практическое пособие / Г.И. Просветов– М.: Альфа-Пресс, 2008. – 416 с.

86 Радько Н.М., Скобелев И.О. // Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. – М.: РадиоСофт., 2010. – 230с.

87 Розенвассер Е.Н. Методы теории чувствительности в автоматическом управлении/Р.Н. Розенвассер, Р.М. Юсупов. – Л.: «Энергия», 1971. – 260 с.

88 Розенвассер Е.Н. Чувствительность систем управления/Р.Н. Розенвассер, Р.М. Юсупов. – М.: Наука, 1981. – 464 с.

89 Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. Шаньгина В.Ф. М.: Радио и связь, 1999. - 328 с.

90 Саати Т. Математические модели конфликтных ситуаций: Пер. с англ. / Т.Саати – М.: Сов. Радио, 1977. – 304 с.

91 Сачков В.Н. Введение в комбинаторные методы дискретной математики/ В.Н.Сачков. - М.: МЦНМО, 2004. – 421 с.

92 Севастьянов Б.А. Вероятностные модели / Б.А. Севастьянов. – М.: Наука, 1992. – 176 с.

93 Симонов С.В. Анализ рисков, управление рисками / С. В. Симонов //JetInfo. Информационный бюллетень, 1999. – № 1. – С. 2-28.

94 Таненбаум Э., ванСтеен М. Распределенные системы/ Э.Таненбаум, М. ванСтеен- Спб: Питер, 2003 – 877 с.

95 Томович Р. Общая теория чувствительности / Р. Томович, М. Вукобратович. Пер. с сербск. и с англ., под ред. Я.З. Цыпкина. – М.: Советское радио, 1972. – 240 с.

96 Унсельд И. Управление рисками и выполнение правил / И. Унсельд // LAN: журнал сетевых решений, 2006. – №8. – С. 86-88.

97 Феллер В. Введение в теорию вероятностей и ее приложения. В 2-х томах. Т.1: Пер. с англ / В. Феллер – М.: Мир. 1984. – С. 137-139.

98 Фомичев А.Н. Риск-менеджмент: Учебное пособие / А.Н. Фомичев – М.: Зорин В.А. Элементы теории процессов риска. / В.А. Зорин, В.И. Мухин. – Н. Новгород: ННГУ.2003. – 25 с.

99 Фурсов С.В., Рудаков Е.В., Толстых Н.Н. Обзор и исследование троянских программ в контексте оценки их опасности для информационно-телекоммуникационных систем на основе статистического риск-анализа // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2009. – Том. 12. – Часть. 3. - С. 363 – 378.

100 Фурсов С.В., Рудаков Е.В. Описание динамики рисков информационно-телекоммуникационных систем, подвергающихся троянским атакам // Информация и безопасность: Регион. науч.-техн. журнал. - Воронеж. 2009. – Том. 12. – Часть. 4. - С. 538 – 548.

101 Хастингс Н. Справочник по статистическим распределениям/ Н. Хастингс, Дж. Пикок. Пер. с англ. А.К. Звонкина. – М.: Статистика, 1980. – 95 с.

102 Хенли Э. Дж. Надежность технических систем и оценка риска / Э. Дж. Хенли, Х. Кумамото – М.: Машиностроение, 1984. – 528 с.

103 Хохлов Н.В. Управление риском: Учеб. Пособие для вузов / Н.В. Хохлов – М.: ЮНИТИ-ДАНА, 1999. – 239 с.

104 Черешкин Д.С. Оценка эффективности систем защиты информационных ресурсов / Д.С. Черешкин. – М.: Институт системного анализа РАН, 1998. – 455 с.

105 Чернова Г.В. Управление рисками: Учебное пособие / Г.В. Чернова, А.А. Кудрявцев. – М.: ТК Велби, Изд-во Проспект, 2003. – 160 с.

106 Шаньгин В.Ф. Защита компьютерной информации / В.Ф. Шаньгин– М.: ДМК пресс, 2008. – 544 с.

107 Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин– М.: Форум, Инфра-М, 2008. – 416 с.

108 Шилов И.А. Экология. — М.: Высшая школа. 1997. — 512 с.

109 Шиверский А. Защита информации: проблемы теории и практики / А.Шиверский – М.: Юристь, 1996. – 112 с.

110 Шоломицкий А.Г. Теория риска. Выбор при неопределенности и моделирование риска: учеб. пособие для вузов/ А.Г. Шоломицкий – М.: Изд. дом ГУ ВШЭ, 2005. – 400 с.

111 Язов Ю.К. Основы методологии количественной оценки защищенности и эффективности защиты информации в компьютерных системах / Ю.К. Язов – Ростов-на-Дону: Издательство СКНЦ ВШ, 2006. – 274 с.

112 Ярочкин В.И. Информационная безопасность / В.И. Ярочкин – М.: Летописец, 2000.– 399

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT