ОГЛАВЛЕНИЕ

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.

В настоящее время все более актуальной становится задача защитыинформационных ресурсов компьютерных сетей от атак со стороны внешних ивнутренних нарушителей. Методика взлома компьютерных сетей совершенствуется практически с той же скоростью, с которой создаются средства защиты информации, наиболее популярными из которых являются: межсетевое экранирование, разграничение доступа, шифрование, идентификация и аутентификация. Новые технологии и программные продукты останавливают злоумышленников лишь на время, так как имеют один существенный недостаток: все они схожи со своими предшественниками по принципу работы: общие алгоритмы мало чем отличаются друг от друга у различных производителей, новые функциональные особенности содержат ошибки и т.п. Все это только на время останавливаетнарушителя, заставляя искать очередную уязвимость в продукте, зачастую унаследованную от прошлых версий. Ярким примером вышесказанному могут послужить частые случаи взлома компьютерных сетей крупных международных компаний, нарушение правильной работы фондовых бирж, утечка служебной информации из различных государственных структур [1-3].

Применительно к противодействию информационно-технологическим атакам на информационные ресурсы АС необходимо отметить, что в настоящее время разработаны методы противодействия указанным угрозам, которые, однако, носят пассивный характер (прекращение передачи информации, закрытие канала связи, изменение маршрутизации и т.п.), что предоставляет злоумышленнику информацию о том, что его воздействие обнаружено, и оставляет в его руках инициативу выбора места, времени и способа повторных атак.

Современные автоматизированные системы носят распределенный характер, из-за чего невозможно гарантировать абсолютную защиту от НСД. Вследствие этого для повышения эффективности защиты информации требуется создание и использование принципиально новых, специфических средств скрытого активного

противодействия вторжениям в автоматизированную систему. В настоящее время ведутся работы по созданию подобных механизмов защиты, одним из которых является ложная информационная система [7,8,11,14,24,28].

Главный отличием данного средства защиты от других является сокрытие его присутствия в системе и направленность на обман злоумышленника, в отличие от классического блокирования доступа, свойственного другим средствам защиты. Это позволяет не только защитить хранимую в компьютерных сетях информацию, но и проанализировать действия злоумышленника, используя полученные сведения для дальнейшего совершенствования системы защиты информации. В этом заключается особенность данного средства защиты – расчет не только на программно-аппаратный набор компонентов системы защиты и использование технических методов и средств, но и «игра в прятки» со злоумышленником в попытке заманить его на данную ложную систему [17-19, 32-36].

Принцип работы ложной информационной системы довольно простой – любому субъекту, желающему получить доступ к объекту, предлагается пройти процедуру идентификации (к примеру, ввести пароль). Если проверка проходит успешно, то субъект получает доступ. Если проверка прошла неудачно или у системы безопасности «возникли подозрения», то субъект автоматически переводиться на ложную систему, которая в достаточной степени эмулирует объект. Таким образом, если субъект пытался получить незаконный доступ к объекту, то для него создается впечатление, что попытка взлома прошла успешно [43-45].

Ложные информационные системы позволяют в режиме реального времени выявлять атаки и направлять их по ложному следу. То есть злоумышленник тратит на ловушки и ложные целивремя, которое администраторы безопасности могут использовать для сбора необходимых сведений об атаках или для идентификации злоумышленника. Благодаря использованию ЛИС сокращаются издержки на администрирование системы, в результате защита становится более гибкой и эффективной [52,60,62].

Еще одной особенностью данного средства защиты является возможность отследить злоумышленника. Большинство нарушителей пытаются скрыть свое местоположение с использованием различных ухищрений. Одним из наиболее распространенных методов является использование цепочки прокси-серверов, через которые злоумышленник пытается подключиться к объекту. Как только нарушитель понимает, что система защиты зафиксировала попытку взлома, он отключается от объекта, а попытки отследить конечное положение злоумышленника оказываются невозможными из-за большого количества прокси-серверов. Ложные информационные системы позволяют решить эту проблему – злоумышленник считает, что он не обнаружен и продолжает работу, в то время как ответственный персонал (к примеру, администратор безопасности сети) проводит мероприятия по определению положения злоумышленника путем вычисления конечного IP-адреса подключения.

Системы анализа защищенности компьютерных сетей, базирующиеся на использовании ЛИС, позволяют проектировщику и (или) системному администратору сети определять не только известные уязвимости в используемом программном и аппаратном обеспечении, но и определять трасы возможных атак (последовательности выполняемых нарушителем атакующих действий), выявлять «узкие» места в безопасности компьютерной сети, моделировать поведение нарушителей, определяемых множеством параметров (например, внешних и внутренних нарушителей), принимать обоснованные решения по составу используемых (или планируемых к использованию) средств обеспечения безопасности [57,63,65,69].

ЛИС не могут полностью заменить существующие технологии организации защиты, однако, с их помощью можно добиться более эффективного использования уже имеющихся механизмов защиты и архитектур систем защиты.

С учетом изложенного тема данной дипломной работы, направленной наразвитие существующих методов и алгоритмов применения ЛИС с целью повышения эффективности управления рисками в интересах защиты от НСД информации, обрабатываемой в компьютерных сетях, является актуальной.

Цель и задачи исследования.Целью настоящей работы являетсяразработка требований и путей построения перспективной ложной информационной системы, в интересах защиты компьютерных сетей от удаленных атак, а также разработка подхода для оценки эффективности от ее применения.

Для достижения поставленной цели в работе решались задачи:

1. исследование основных особенностей примененияложных информационных систем,как средства защиты от НСД к информации, обрабатываемой в КС;
2. создание вербальной модели ложной информационной системы, как средства защиты от НСД к информации, обрабатываемой в КС;
3. оценка результатов применения ложных информационных систем, как средства защиты от НСД к информации, обрабатываемой в КС, для различных типов атак;
4. практическая оценка эффективности применения ЛИС, как средства управления рисками в интересах защиты от НСД информации, обрабатываемой в КС;
5. оценка экономических показателей ложной информационной системы, как средства защиты от НСД к информации, обрабатываемой в КС;
6. рассмотрение исследуемой проблематики с точки зрения обеспечения безопасности жизнедеятельности.

Объект исследования. Объектом исследования является ложная информационная система, как средство защиты от НСД к информации, обрабатываемой в КС.

Предмет исследования. Предметом исследования является оценка эффективности применения ложных информационных систем, как средства защиты от НСД к информации, обрабатываемой в КС.

Методы исследования.Для реализации намеченной цели исследования и решения поставленных задач используются методы построения систем защиты информации, теории рисков, теории вероятности, математической статистики и системного анализа, теории информации,методы имитационного моделирования.

Научная новизна. В данной работе было проведено исследование существующих методов и алгоритмов построения ложных информационных систем, в интересах защиты компьютерных сетей от удаленных атак, в результате которого были выявлены новые уязвимости.

Учитывая результаты исследования, была построена вербальная модель перспективной ложной информационной системы, отличающаяся от существующих.

Впервые был предложен механизм для оценки эффективности применения ложных информационных систем, как средства защиты компьютерных сетей от удаленных атак.

Показаны способы и пути практической реализации ЛИС в целях защиты от несанкционированного доступа информации, обрабатываемой в компьютерных сетях. Представлена описательная модель типовой ЛИС, а также создан макет типовой ЛИС.

На защиту выносятся следующие основные результаты работы:

1. Результаты исследования существующих методови алгоритмов построенияложных информационных систем,как средства защиты компьютерных сетей от удаленных атак;
2. Вербальная модель ложной информационной системы, как средства защиты компьютерных сетей от удаленных атак;
3. Алгоритм для оценки эффективности применения ложных информационных систем, как средства защиты компьютерных сетей от удаленных атак.
4. Обоснование структуры макета ЛИС;

Практическая ценность работы заключается в разработке модели ложной информационной системы, которая может быть применена для защиты компьютерных сетей, для которых недостаточно использование традиционных механизмов защиты.

Разработанный алгоритм оценки эффективности применения ЛИС может быть использован для принятия управленческого решения о целесообразности

использования ложных информационных систем, для защиты компьютерных сетей от удаленных атак.

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

projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT

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

projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT projectIT

ЗАКЛЮЧЕНИЕ

Работа посвящена исследованию возможности управления рисками автоматизированных систем на основе использования ложных информационных систем.В ходе её выполнения были получены следующие основные результаты:

1. Проведено исследование основных особенностей применения ЛИС, как средства защиты от НСД к информации, обрабатываемой в КС. Приведено описание ЛИС, выявлены достоинства и недостатки их применения для защиты КС от удаленных атак. Проведена классификация ЛИС по различным признакам, описаны входящие в них компоненты.

2. Построена вербальная модель ЛИС,как средства защиты от НСД к информации, обрабатываемой в КС. Проанализированы и разработаны основные требования, предъявляемые к функциональным возможностям и архитектуре ЛИС и ее компонентов, после чего проведено моделирование ее архитектуры.

3. Проведена оценка результатов применения ложных информационных систем, как средства защиты от НСД к информации, обрабатываемой в КС, для различных типов атак. Разработан подход для оценки степени подобия ЛИС целевой системе, основанный на методе экспертных оценок. Описана динамика возникновения угроз связанных с несанкционированным доступом к информации в компьютерной сети, с использованием аппарата марковских процессов, в результате чего построена марковская модель для некоторых типов сетевых атак.

4. Выбран способ реализации ЛИС. Описаны основные элементы схемы компьютерной сети с использованием ЛИС. Описан минимальный набор программно-аппаратных средств, необходимых для функционирования ЛИС.

5. Описана схема воздействия на защищаемый объект. Разработан подход для оценки ущерба целостности, доступности и конфиденциальности информации.Предложен вариант расчета рисков нанесения ущерба безопасности информации в результате реализации угроз целостности, доступности и конфиденциальности.Оценена эффективность применения ЛИС, как средства защиты от НСД к информации, хранимой и обрабатываемой в КС.

СПИСОК ЛИТЕРАТУРЫ

1 Анин Б., Защита компьютерной информации, BHV-Санкт-Петербург, 2000 г.

2 Бармен Скотт Разработка правил информационной безопасности. изд. Вильямс, 2002 г.

3 Богатырев В.А. Надежность и эффективность резервированных компьютерных сетей//Информационные технологии. -2006 -№ 9. -С. 25-30.

4 Борисов В.И., Радько Н.М., Скобелев И.О., Науменко Н.С. Оценка рисков информационно-телекоммуникационных систем, подвергающихся НСД-атакам. Информация и безопасность, №1, 2011.

5 Боровков А.А. Математическая статистика. – М.: Наука, 1984.

6 Бородин А.Н. Элементарный курс теории вероятностей и математической статистики. – С.-П: 1999.

7 Борохов С.В., Синицын И.Н., Рыков А.С. Экспертная оценка эффективности построения системы безопасности информационно-телекоммуникационных систем высокой доступности. Наукоемкие технологии. 2006, №2, с.5-29.

8 Брэг Р., Родс-Оусли М., Страсберг К. Безопасность сетей, полное руководство, ЭКОМ, 2006 г.

9 Вентцель Е.С. Теория вероятностей и ее инженерные приложения: учеб. пособие для втузов / Е.С. Вентцель, Л.А. Овчаров. – М.: Высшая школа, 2003. – 464с.

10 Вентцель Е.С. Теория вероятностей: учеб. для втузов / Е.С. Вентцель – М.: Высш. шк, 1998. – 576 с.

11 Володин А.В., Устинов Г.Н., Цибин В.В. Сеть передачи данных —модель угроз информационной безопасности // Вестник связи. 1999, № 4, 52-57.

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

13 Гаек Я., Шидак З. Теория ранговых критериев. – М.: Наука, 1971.

14 Галатенко В.А. Основы информационной безопасности, 2008 г.

15Гихман И.И., Скороход А.В., Ядренко М.И. Теория вероятностей и математическая статистика. – Киев: Вища школа, 1979.

16 Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – 12-е изд., стереотип. – М.: Высшая школа, 2005. – 479 с.

17 ГОСТ Р 50922-96 Защита информации. Основные термины и определения.

18 Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. – М.: Гостехкомиссия России, 1999. – 14 с.

19 Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ 09.09.2000.

20 Ефимова А.В. Сборник задач по математике. Теория вероятностей и математическая статистика. – М.: Наука, 1990.

21 Ефремов А. Сетевые атаки и средства борьбы с ними // ComputerWeekly № 14, 1998, с. 14-17.

22 Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей. Учебное пособие. Е.А. Карпов, И.В. Котенко, М.М. Котухов, А.С. Марков, Г.А. Парр, А.Ю. Рунеев. СПб.:ВУС, 2000. 190 с.

23 Злобина И.А. Экономика информационной безопасности: учеб. пособие / И.А. Злобина –Воронеж: Воронежский государственный технический университет, 2005. – 196 с.

24 Информационная безопасность и защита информации. Сборник терминов и определений. – М.: Гостехкомиссия России. 2001.

25 Карайчев Г.В., Нестеренко В.А. Применение весовых функций для определения локальных статистических характеристик потока пакетов в сети. Известия высших учебных заведений. Северо-Кавказский регион. Серия: Естественные науки. 2008, №1, с.10-13.

26 Карпов Ю. Имитационное моделирование систем. Введение в моделирование с Anylogic 5. -СПБ.: БВХ-Петербург, 2005. - 400 с.: ил.

27 Колмогорцев Е.Л. Модель производительности распределенной иерархической системы управления с резервированием коммуникационной подсистемы//Информационные технологии моделирования и управления. -2006 -№ 9(34). -С. 1172-1178.

28 Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: Руководящий документ. Гостехкомиссия РФ. – М.: JetInfo, 1996. – №2.

29 Концепция национальной безопасности Российской Федерации. Утверждена указом Президента РФ от 17 декабря 1997 года №1300.

30 Корн Г. Справочник по математике для научных работников и инженеров / Г. Корн. – М.: Наука, 1977. – 832 с.

31 Королюк В.С. Справочник по теории вероятностей и математической статистике / В.С. Королюк, Н.И. Портенко, А.В. Скороход. – М.: Наука. Главная редакция физико-математической литературы, 1985. – 640 с.

32 Котенко И.В., Степашкин М.В. Обманные системы для защиты информационных ресурсов в компьютерных сетях // Труды СПИИРАН, Вып.2. СПб: СПИИРАН, 2004

33 Котенко И.В., Степашкин М.В. Прототип ложной информационной системы // XI Российская научно-техническая конференция «Методы и технические средства обеспечения безопасности информации». Тезисы докладов. Санкт-Петербург. Издательство СПбГПУ. 2003

34 Котенко И.В., Степашкин М.В., Михайлов Д.Ю. Система сбора анализа и хранения данных аудита работы пользователей // Методы и технические средства обеспечения безопасности информации. Материалы XII общероссийской научно-технической конференции. 4-5 октября 2004 года, Санкт-Петербург. Издательство политехнического университета. 2004.

35 Котенко, И. В, Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников [Текст] И. В.

Котенко, М. В. Степашкин, В. Богданов Проблемы информационной безонасности. Компьютерные системы. СПб., 2006.

36 Котенко, И. В. Анализ защищенности компьютерных сетей на этапах проектирования и эксплуатации [Текст] И. В. Котенко, М. В. Степашкин, В. Богданов Изв. вузов. Приборостроение. СПб., 2006. Т. 49, 5.

37 Котенко, И. В. Модели и методика интеллектуальной оценки уровня защищенности компьютерных сетей [Текст] И. В. Котенко, М. В. Степашкин, В. Богданов Труды Международных научно-технических конференций «Интеллектуальные системы (AIS-06)» и «Интеллектуальные САПР (CAD-2006)». М Физматлит, 2006.

38 Котенко, И. В. Модель атак для имитации действий злоумышленника в системе анализа защищенности компьютерных сетей [Текст] И. В. Котенко, М. В. Степашкин, В. Богданов Труды IV Межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2005)». СПб.

39 Котенко, И. В. Прототип имитатора информационной системы: архитектура и сценарии проведения экспериментов [Текст] И. В. Котенко, М. В. Степащкин Труды конференции «Информационная безопасность регионов России (ИБРР-2003)». СПб.: Издательство Политехника, 2003. 68-

40 Ларичев О.И. Теория и методы принятия решений / О.И. Ларичев М.: Логос, 2002.-392 с.: ил.

41 Ликеш И., Ляга И. Основные таблицы математической статистики. – М.: Финансы и статистика, 1985.

42 Ллойд. Э., Ледерман У. Справочник по прикладной статистике, т.т. 1,2. – М.: Финансы и статистика. 1989.

43 Лукацкий А.В. Атаки на информационные системы. «Электроника. Наука. Технологии и Бизнес». 2000, 1, с.42-44.

44 Лукацкий А.В. Обнаружение атак — СПб.: БХВ-Петербург, 2001.-624 с.

45 Магауенов Р.Г. Основные задачи и способы обеспечения безопасности автоматизированных систем обработки информации. / Р.Г. Магауенов. – М.: Мир и безопасность, 1997 – №1. – С. 118-126.

46 Малошевский С.Г. Теория вероятностей: учеб. пособие. Часть 1. Вероятностное пространство. Дискретные случайные величины / С.Г. Малошевский. – СПб.: Петербургский государственный университет путей сообщения, 1999. – 92 с.

47 Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов / А.А. Малюк М.: Горячая линия – Телеком, 2004. – 280 с.: ил.

48 Матвеевский В.Р. Надежность технических систем. Учебное пособие – Московский государственный институт электроники и математики. М., 2002 г. – 113 с.

49 Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры: Руководящий документ ФСТЭК России от 18.05.2007.

50 Мишин К.Н. Имитационное моделирование аномальных явлений в компьютерных сетях. Записки научных семинаров Санкт-Петербургского отделения математического института им. В.А. Стеклова РАН. 2007, с. 120-128.

51 Новейший словарь иностранных слов и выражений. — М.: АСТ, 2002.

52 Общие требования безопасности информации в ключевых системах информационной инфраструктуры: Руководящий документ ФСТЭК России от 18.05.2007.

53 Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. - СПБ.: Питер, 2010. -944 с.: ил.

54 Остапенко А.Г. Комплексная оценка эффективности защиты от угроз безопасности с использованием аппарата теории нечетких множеств / А.Г. Остапенко, Ю.К. Язов, Р.В. Батищев, О.А. Середа // Информация и безопасность. – 2001. – №2. – С. 4-11.

55 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.

56 Павлов А.А. Основы системного анализа и проектирования автоматизированных систем управления: учеб. пособие / А.А. Павлов. – Киев: Выща школа, 1991. – 364 с.

57 Парфенов В.И. Защита информации (Словарь). – Воронеж: НП РЦИБ "Факел", 2003.– 293 с.

58 Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.

59 Прангишвили И.В. Системные закономерности и системная оптимизация / И.В. Прангишвили, В.Н. Бурков. – М.: Синтег, 2004. – 208 с.

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

61 Пугачев В.С. Теория вероятностей и математическая статистика: учеб. пособие. – 2-е изд., исправл. и дополн. – М.: ФИЗМАТЛИТ, 2002. – 496 с.

62 Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры: Руководящий документ ФСТЭК России от 19.11.2007.

63 Риндле К. Динамические инфраструктуры. Журнал сетевых решений/LAN. 2010, №7+8.

64 Романовский В. Математическая статистика. – М.: Гостехиздат, 1938.

65 Руднев М. Хранение данных и, резервное копирование в сетях. Компьютер-Пресс, 2000, № 7 (Тематический выпуск: хранение и защита данных), с.40-43.

66 Сабо Ю.И. Применение сетей Петри с марковскими свойствами для анализа отказоустойчивости систем с резервированием. // Изв. вузов. Приборостроение. 2004. Т.47. №12.

67 Селезнев А.В. Организация резервного копирования в локальных и корпоративных сетях. Сети и системы связи. 1996, № 10, с. 110.

68 Смирнов Н.В., Дунин-Барковский И.В. Краткий курс математической статистики для технических приложений. – М.: Физмагиз, 1959.

69Соколов А.В., Методы информационной защиты объектов и компьютерных сетей, изд. Полигон, 2000 г.

70 Соколов Г.А., Гладких И.М. Математическая статистика: учебник для вузов. – М.: Экзамен, 2007. – 431с.

71Спитцнер Л. HoneynetProject: ловушка для хакеров // Открытые системы, № 07-08, 2003

72Степашкин М.В. Модели и методика анализа защищенности компьютерных сетей на основе построения деревьев атак / Санкт-Петербург, 196 с.

73 Строгалев В.П., Толкачева И.О. Имитационное моделирование: Учеб. пособие. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 280 с.: ил.

74 Сулицкий В.Н. Методы статистического анализа в управлении / В.Н. Сулицкий. – М.: Дело, 2002. – 520 с.

75 Таненбаум Э. Архитектура компьютера. -СПб.: Питер, 2003. -704 с.

76 Таненбаум Э. Современные операционные системы. 3-е изд. - Спб.: Питер, 2010. -1120 с.: ил.

77 Тихонов В.И., Миронов М.А. Марковские процессы. М.: Советское радио, 1977.

78 Толковый словарь по вычислительным системам / Под ред. В. Иллингуорта, Э.Л. Глейзера, И.К. Пайла / Пер. санглийского. — М.: Машиностроение, 1989.

79 Торокин А.А. Основы инженерно-технической защиты информации. – М: Ось-89, 1998. – 336 с.

80 Трайнер В.А. Информационная безопасность предприятия: учеб. пособие / В.А. Трайнер, А.А. Федулов: Международная академия наук информации, информационных процессов и технологий (МАН ИПТ). – М.: Дашков и К, 2004. – 336 с.

81 Тюрин Е.Н., Макаров А.А. Статистический анализ данных на компьютере. – М.: ИНФРА-М, 1998.

82 Ушаков И.А. Вероятностные модели надежности информационно-вычислительных систем. -М.: Радио и связь, 1991. -132 с.

83 Федеральный закон "Об информации, информационных технологиях и защите информации" №146. – 2006.

84 Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных».

85 Функциональные требования безопасности. Введ. 2002-04-04. М Изд-во стандартов, 2002. 159 с. ГОСТ Р ИСО/МЭК 15408-3-2

86 Царегородцев А.В. Информационная безопасность в распределенных управляемых системах: монография / А.В. Царегородцев. – М.: РУДН, 2003. – 217 с.

87 Ченцов Н.Н. Статистические решающие правила и оптимальные выводы. – М.: Наука, 1972.

88 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.

89 Шторм Р. Теория вероятностей. Математическая статистика. Статистический контроль качества / Р. Шторм. – М.: Издательство "МИР", 1970. – 368 с.

90 Шумский А.А. Системный анализ в защите информации: учеб. пособие / А.А. Шумский, А.А. Шелупанов. – М.: Гелиос АРВ, 2005. – 224 с.

91 Язов Ю.К. Использование аппарата теории нечетких множеств в интересах комплексной оценки эффективности технической защиты информации в распределенных компьютерных системах / Ю.К. Язов, И.М. Седых // Вестник ВИ МВД России. – 2003. – №3(15). – С 179-182.

92 Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах / Ю.К. Язов. – Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. – 274 с.

93 Язов Ю.К. Основы технологии проектирования системы защиты информации в информационно-телекоммуникационных системах: Монография / А.В. Аграновский, В.И. Мамай, И.Г. Назаров, Ю.К. Язов. – Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. – 260 с.

94 Язов Ю.К., Седых И.М. Метод количественной оценки защищенности информации в компьютерной системе. Телекоммуникации. 2006, №6, с.46-48.

95 Clark M. Virtual Honeynets (using VMware). SecurityFocus InFocus Article, Nov 2001.

96 Honeynet Project www.honeynet.org

97 Spitzner L. / Building a Honeypot. Mar 2000.

98 Spitzner L. Honeypots: Definitions and Values. May 2003.

99 Spitzner L., Honeypots: Tracking Hackers. Addision Wesley , 2002

100 Spitzner L., The Honeynet Project: Trapping the Hackers // IEEE Security & Privacy, January-February 2003.