ФГБОУ ВПО «Воронежский государственный
технический университет»

Кафедра систем информационной безопасности

147-2015

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению научно-исследовательской работы
«Риск-анализ атакуемых информационных
технологий и систем»
для студентов специальностей
090301 «Компьютерная безопасность»,
090302 «Информационная безопасность
телекоммуникационных систем»,
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Воронеж 2015

Составители: д-р техн. наук А. Г. Остапенко, Р. К. Бабаджанов, Н. Н Корнеева

УДК 004.056

Методические указания к выполнению научно-исследовательской работы «Риск-анализ атакуемых информационных технологий и систем» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. А. Г. Остапенко, Р. К. Бабаджанов, Н. Н. Корнеева. Воронеж, 2015. 40 с.

Методические указания к выполнению научно-исследовательской работы содержат материал, направленный на углубленное изучение лекционного материала и приобретение практических навыков при решении различных задач по риск-оценке.

Методические указания подготовлены в электронном виде в текстовом редакторе и содержатся в файле Остапенко_УИР_Риск-анализ.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

ЦЕЛЬ РАБОТЫ

Целью проведения на 4-ом курсе научно-исследовательской работы является закрепление и развитие знаний и навыков, полученных на кафедре, а также подготовка к предстоящему дипломному проектированию и созданию качественной выпускной квалификационной работы.

1. РАЗВИТИЕ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ОЦЕНКИ ОЖИДАЕМОЙ ЭФФЕКТИВНОСТИ ЗАЩИТЫ СИСТЕМЫ

1.1. Основы методики расчета

Аналитическое выражение для оценки ожидаемой эффективности в момент вероятной гибели атакуемой системы t_0имеет следующий вид:

$$\mathrm{E}(t_0)=\frac{V[0,t_0][1-F(t_0)]}{U[t_0;T_{\text{ср}}]f(t_0)(\Delta t)}, \quad (1)$$

где :

V $[0,t_0]=\int_0^{t_0}\omega(t)dt$ – польза, полученная по функции полезности w (производительности) за период от 0 до t_0;

$U[t_0;T_{\text{ср}}]=\int_{t_0}^{T_{\text{ср}}}\omega(t)dt$ – ущерб (как недополученная польза), возникающая за период от t_0 до средней продолжительности жизни систем рассматриваемого класса систем $T_{\text{ср}}$;

$f(t_0)$ – значение плотности вероятности гибели атакуемой системы в момент t_0;

$F(t_0)$ – накопленная вероятность того, что система не доживет до момента t_0;

$\Delta t \le \frac{1}{kf_{max}}$ – шаг дискретизации времени;

f_{max}- пик плотности вероятности *f(t)*;

n – количество отсчетов при дискретизации времени на интервале от 0 до$T_{\text{ср}}$

k– степень дискретизации.

Следует заметить, что *f(t)*, *F(t)*, f_{max} обычно заданы видом избранного непрерывного распределения (см. теорию вероятности) и имеют вполне определенное аналитическое выражение.

Традиционно функции распределения находят на основе статистических данных путем доказательства гипотез по критериям Пирсона, Колмогорова и др.

Таким образом, при дискретизации имеем выражение мгновенной эффективности, равное:

$$\mathrm{E}\left(\frac{k_0}{n}\right)=\frac{V\left[0,\frac{k_0}{n}\right][1-\sum_{k=0}^{k_0} f\left(\frac{k_0}{n}\right)(\overline{\Delta t})]}{U\left[\frac{k_0}{n};1\right]f\left(\frac{k_0}{n}\right)(\overline{\Delta t})}, \quad (2)$$

где $k_0=\left[\frac{t_0}{T_{cp}}n\right]$ – целая часть нормированного момента времени $(\frac{t_0}{T_{cp}})$, помноженного на количество дискрет n (фактически ось времени пронормирована по средней продолжительности жизни $T_{\text{ср}}$ и укладывается в отрезок от 0 до 1); $\overline{\Delta t}=\frac{1}{n}$ – нормированный шаг дискретизации.

Упрощая, имеем

$$\mathrm{E}\left(\frac{k_0}{n}\right)=\frac{V\left[0,\frac{k_0}{n}\right][n-\sum_{k=0}^{k_0} f\left(\frac{k_0}{n}\right)]}{U\left[\frac{k_0}{n};1\right]f\left(\frac{k_0}{n}\right)}. \quad (3)$$

Для интегральной оценки эффективности анализируемой системы, очевидно следует воспользоваться следующим выражением:

$$E_{\Sigma}=\frac{\sum_{k_0=0}^{n} V\left[0,\frac{k_0}{n}\right][1-\sum_{k=0}^{k_0} f\left(\frac{k_0}{n}\right)(\overline{\Delta t})]}{\sum_{k_0=0}^{n} U\left[\frac{k_0}{n};1\right]f\left(\frac{k_0}{n}\right)(\overline{\Delta t})} \quad (4)$$

или

$$E_{\Sigma}=\frac{\sum_{k_0=0}^{n} V\left[0,\frac{k_0}{n}\right][1-\sum_{k=0}^{k_0} f\left(\frac{k_0}{n}\right)]}{\sum_{k_0=0}^{n} U\left[\frac{k_0}{n};1\right]f\left(\frac{k_0}{n}\right)}. \quad (5)$$

В этом случае сумма шансов относится к сумме рисков на протяжении всего жизненного цикла системы.

К примеру, для прямоугольной аппроксимации функции полезности

$$\omega\left(\frac{k_0}{n}\right)=\begin{cases}\omega_{0\ \text{при}\ \frac{k_0}{n}\le 1;}\\ 0_{\ \text{при}\ \frac{k_0}{n}>1}\end{cases}.$$

Польза будет равна

$$V\left[0,\frac{k_0}{n}\right]=\omega_0\frac{k_0}{n},$$

а ущерб соответственно составит

$$U\left[\frac{k_0}{n};1\right]=\omega_0\left(1-\frac{k_0}{n}\right).$$

Отсюда имеем

$$\mathrm{E}\left(\frac{k_0}{n}\right)=\frac{w_0\frac{k_0}{n}[1-\sum_{k=0}^{k_0}f\left(\frac{k}{n}\right)]}{w_0\left(1-\frac{k_0}{n}\right)f\left(\frac{k_0}{n}\right)}=\frac{k_0}{n-k_0}*\frac{1-\sum_{k=0}^{k_0}f\left(\frac{k}{n}\right)}{f\left(\frac{k_0}{n}\right)}. \quad (6)$$

По аналогии интегральная эффективность будет равна

$$E_{\Sigma}\ =\frac{n\sum_{k_0=0}^{n}k_0[1-\sum_{k=0}^{k_0}f\left(\frac{k}{n}\right)]}{\sum_{k_0=0}^{n}(n-k_0)f\left(\frac{k_0}{n}\right)}. \quad (7)$$

В случае дискретных распределений, когда дискретизация, очевидно не требуется, расчет эффективности упрощается:

$$\mathrm{E}\left(\frac{k_0}{n}\right)=\frac{V\left[0,\frac{k_0}{n}\right][1-\sum_{k=0}^{k_0}P\left(\frac{k}{n}\right)]}{U\left[\frac{k_0}{n};1\right]P\left(\frac{k_0}{n}\right)} \quad (8)$$

и

$$E_{\Sigma}\ =\frac{\sum_{k_0=0}^{n}V\left[0,\frac{k_0}{n}\right][1-\sum_{k=0}^{k_0}P\left(\frac{k}{n}\right)]}{\sum_{k_0=0}^{n}U\left[\frac{k_0}{n};1\right]P\left(\frac{k_0}{n}\right)}. \quad (9)$$

При этом для обоих классов распределений реальный теоретический и практический интерес представляют не

столько инструкции по подстановке в вышеуказанные выражения $f\left(\frac{k_0}{n}\right)$ или $P\left(\frac{k_0}{n}\right)$, сколько существенное аналитическое упрощение итоговых выражений для их последующего инженерного применения и алгоритмизации, т.е. удобства численных расчетов и оптимизации.

1.2. Область применения рекомендуемой методики

Относительно области применения рекомендуемой методики (1)-(9) следует заметить, что она достаточно широка и сегодня особенно актуальна эта тема для информационных технологий и систем, где возникает масса проблем управления их эффективностью в условиях атак и сбоев для стремительно усложняющегося аппаратно-программного обеспечения. Рассмотрим их подробнее.

1) CALS-технологии

CALS-технологии (англ. Continuous Acquisition and Lifecycle Support – непрерывная информационная поддержка поставок и жизненного цикла) – современный подход к проектированию и производству высокотехнологичной и наукоёмкой продукции, заключающийся в использовании компьютерной техники и современных информационных технологий на всех стадиях жизненного цикла изделия. За счет непрерывной информационной поддержки обеспечиваются единообразные способы управления процессами и взаимодействия всех участников этого цикла: заказчиков продукции, поставщиков/производителей продукции, эксплуатационного и ремонтного персонала. Информационная поддержка реализуется в соответствии с требованиями системы международных стандартов, регламентирующих правила указанного взаимодействия преимущественно посредством электронного обмена данными.

Применение CALS-технологий позволяет существенно сократить объёмы проектных работ, так как описания многих

составных частей оборудования, машин и систем, проектировавшихся ранее, хранятся в унифицированных форматах данных сетевых серверов, доступных любому пользователю технологий CALS. Существенно облегчается решение проблем ремонтопригодности, интеграции продукции в различного рода системы и среды, адаптации к меняющимся условиям эксплуатации, специализации проектных организаций и т.п. Предполагается, что успех на рынке сложной технической продукции будет немыслим вне технологий CALS.

Развитие CALS-технологий должно привести к появлению так называемых виртуальных производств, в которых процесс создания спецификаций с информацией для программно-управляемого технологического оборудования, достаточной для изготовления изделия, может быть распределён во времени и пространстве между многими организационно-автономными проектными студиями. Среди несомненных достижений CALS-технологий следует отметить лёгкость распространения передовых проектных решений, возможность многократного воспроизведения частей проекта в новых разработках и др.

Построение открытых распределённых автоматизированных систем для проектирования и управления в промышленности составляет основу современных CALS-технологий. Главная проблема их построения — обеспечение единообразного описания и интерпретации данных, независимо от места и времени их получения в общей системе, имеющей масштабы вплоть до глобальных. Структура проектной, технологической и эксплуатационной документации, языки её представления должны быть стандартизированными. Тогда становится реальной успешная работа над общим проектом разных коллективов, разделённых во времени и пространстве и использующих разные CAD/CAM/CAE-системы. Одна и та же конструкторская документация может быть использована многократно в разных проектах, а одна и та же технологическая документация —

адаптирована к разным производственным условиям, что позволяет существенно сократить и удешевить общий цикл проектирования и производства. Кроме того, упрощается эксплуатация систем.

Для обеспечения информационной интеграции CALS использует стандарты IGES и STEP в качестве форматов данных. В CALS входят также стандарты электронного обмена данными, электронной технической документации и руководства для усовершенствования процессов. В последние годы работа по созданию национальных CALS-стандартов проводится в России под эгидой ФСТЭК России. С этой целью создан Технический Комитет ТК431 «CALS-технологии», силами которого разработан ряд стандартов серии ГОСТ Р ИСО 10303, являющихся аутентичными переводами соответствующих международных стандартов (STEP).

2) GRID-технологии

Грид-технологии (англ. Grid – решётка, сеть) – это форма распределённых вычислений, в которой «виртуальный суперкомпьютер» представлен в виде кластеров соединённых с помощью сети, слабосвязанных, гетерогенных компьютеров, работающих вместе для выполнения огромного количества заданий (операций, работ). Эта технология применяется для решения научных, математических задач, требующих значительных вычислительных ресурсов. Грид-технологии используются также в коммерческой инфраструктуре для решения таких трудоёмких задач, как экономическое прогнозирование, сейсмоанализ, разработка и изучение свойств новых лекарств.

Грид с точки зрения сетевой организации представляет собой согласованную, открытую и стандартизованную среду, которая обеспечивает гибкое, безопасное, скоординированное разделение вычислительных ресурсов и ресурсов хранения информации, которые являются частью этой среды, в рамках одной виртуальной организации.

Типы грид-технологий:

1. Добровольные гриды – гриды на основе использования добровольно предоставляемого свободного ресурса персональных компьютеров;
2. Научные гриды – хорошо распараллеливаемые приложения программируются специальным образом (например, с использованием Globus Toolkit);
3. Гриды на основе выделения вычислительных ресурсов по требованию (коммерческий грид, англ. enterprise grid) – обычные коммерческие приложения работают на виртуальном компьютере, который, в свою очередь, состоит из нескольких физических компьютеров, объединённых с помощью грид-технологий.

3) Scada-технологии.

SCADA (аббр. от англ. supervisory control and data acquisition, диспетчерское управление и сбор данных) – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления. SCADA может являться частью АСУ ТП, АСКУЭ, системы экологического мониторинга, научного эксперимента, автоматизации здания и т.д. SCADA-системы используются во всех отраслях хозяйства, где требуется обеспечивать операторский контроль за технологическими процессами в реальном времени. Данное программное обеспечение устанавливается на компьютеры и, для связи с объектом, использует драйверы ввода-вывода или OPC/DDE серверы. Программный код может быть, как написан на языке программирования (например, на C++), так и сгенерирован в среде проектирования.

SCADA-системы решают следующие задачи:

- Обмен данными с «устройствами связи с объектом» (то есть с промышленными контроллерами и платами ввода/вывода) в реальном времени через драйверы.
- Обработка информации в реальном времени.
- Логическое управление.

- Отображение информации на экране монитора в удобной и понятной для человека форме.
- Ведение базы данных реального времени с технологической информацией.
- Аварийная сигнализация и управление тревожными сообщениями.
- Подготовка и генерирование отчетов о ходе технологического процесса.
- Осуществление сетевого взаимодействия между SCADA ПК.
- Обеспечение связи с внешними приложениями (СУБД, электронные таблицы, текстовые процессоры и т. д.). В системе управления предприятием такими приложениями чаще всего являются приложения, относимые к уровню MES.

SCADA-системы позволяют разрабатывать АСУ ТП в клиент-серверной или в распределённой архитектуре.

4) Облачные технологии:

4.1) SaaS (Программное обеспечение как услуга)

Программное обеспечение как услуга (SaaS, англ. Software-as-a-Service) – модель, в которой потребителю предоставляется возможность использования прикладного программного обеспечения провайдера, работающего в облачной инфраструктуре и доступного из различных клиентских устройств или посредством тонкого клиента, например, из браузера (например, веб-почта) или интерфейс программы. Контроль и управление основной физической и виртуальной инфраструктурой облака, в том числе сети, серверов, операционных систем, хранения, или даже индивидуальных возможностей приложения (за исключением ограниченного набора пользовательских настроек конфигурации приложения) осуществляется облачным провайдером.

4.2) PaaS (Платформа как услуга)

Платформа как услуга (PaaS, англ. Platform-as-a-Service) – модель, когда потребителю предоставляется возможность использования облачной инфраструктуры для размещения

базового программного обеспечения для последующего размещения на нём новых или существующих приложений (собственных, разработанных на заказ или приобретённых тиражируемых приложений). В состав таких платформ входят инструментальные средства создания, тестирования и выполнения прикладного программного обеспечения – системы управления базами данных, связующее программное обеспечение, среды исполнения языков программирования – предоставляемые облачным провайдером.

Контроль и управление основной физической и виртуальной инфраструктурой облака, в том числе сети, серверов, операционных систем, хранения осуществляется облачным провайдером, за исключением разработанных или установленных приложений, а также, по возможности, параметров конфигурации среды (платформы).

4.3) IaaS (Инфраструктура как услуга)

Инфраструктура как услуга (IaaS, англ. IaaS or Infrastructure-as-a-Service) предоставляется как возможность использования облачной инфраструктуры для самостоятельного управления ресурсами обработки, хранения, сетей и другими фундаментальными вычислительными ресурсами, например, потребитель может устанавливать и запускать произвольное программное обеспечение, которое может включать в себя операционные системы, платформенное и прикладное программное обеспечение. Потребитель может контролировать операционные системы, виртуальные системы хранения данных и установленные приложения, а также ограниченный контроль набора доступных сервисов (например, межсетевой экран, DNS). Контроль и управление основной физической и виртуальной инфраструктурой облака, в том числе сети, серверов, типов используемых операционных систем, систем хранения осуществляется облачным провайдером.

На каждой из этих технологий могут базироваться определенные системы. Рассмотрим некоторые из них:

1) **Сервер рабочей группы**

Представляет собой систему начального уровня, как правило, однопроцессорный. Небольшие компании и удаленные офисы не имеют выделенного специального помещения и располагают сервер непосредственно в своем офисе. Такая система должна как можно меньше привносить шум в офисное помещение. По функциям, такая машина служит для разграничения прав доступа сотрудников к файловым ресурсам либо служит как емкость для хранения общих данных.

2) Сервер контроллер домена, Domain Controller server

Необходим в организации с количеством сотрудников более 20 рабочих мест, позволяет централизованно управлять сетевыми и файловыми ресурсами компании, также обычно выполняет роль сервера печати. DC server должен быть уже на порядок качественнее и надежнее в отличии от сервера рабочей группы, иметь возможность масштабирования при росте количества пользователей локальной сети. Производительность его зависит от масштаба компании, обычно это одно- двухпроцессорный узел, под управлением MS Windows Server 2003-2008 с настроенной службой каталогов Active Directory.

3) Прокси Сервер

Прокси Сервер – шлюз в Интернет. В этой роли серверная машина обеспечивает общий доступ в интернет всем (или определенным компьютерам офиса) безопасную работу сотрудников в Интернете. В случае если бизнес компании жестко связан с работой сотрудников во внешней сети, такой шлюз должен быть не только отказоустойчивым, но и достаточно производительным: работа специального программного обеспечения (антивирусных программ, анализ и учет трафика, анализаторы атак и т.п.) может требовать большого количества системных ресурсов и высокоскоростных интерфейсов связи.

4) Сервер электронной почты. (Mail Server)

Выделенный узел для обработки почтовых приложений может иметь потребность у организации с численностью сотрудников 30-40 человек и позволяет централизованно управлять внешней корреспонденцией, внутренней перепиской и документооборотом. Серверные версии антивирусных программ и грамотно настроенные фильтры снизят риск потери или утечки конфиденциальной информации и уменьшат объемы нежелательной почты.

5) Веб сервер, сервер WEB-приложений

Многие современные компании и организации имеют свой виртуальный офис или магазин в сети Интернет WEB-сайт. Сайт может быть простым и служить лишь визитной карточкой компании, либо более сложным – порталом, онлайн каталогом с возможностью оформления заказов от клиентов. Бизнес-процесс многих компаний в современном мире полностью зависим от работы WEB служб, а в нашем случае от веб-сервера, его доступность и отказоустойчивость, возможность противостоять внешним негативным воздействиям, атакам и попыткам взлома, достаточной производительностью для сотни или тысячи одновременно принимаемых запросов из сети. Выделенный узел для веб-приложений позволит обеспечить доступ большому количеству посетителей, гарантировать работу сложных, критически важных веб-приложений компании.

6) Терминальный сервер

Работу удаленных офисов, мобильных пользователей и сотрудников, часто работающих из дома или в командировке, с обеспечением привычного доступа к рабочим ресурсам посредством сети Интернет или выделенных каналов связи способен обеспечить терминальный сервер. Шифрование передаваемых данных обеспечивает безопасность такого вида связи. Пользователь соединяется через канал связи с сервером, вводит свои учетные данные и попадает на свой виртуальный рабочий стол, или документам. Эта служба удобна тем что важные данные хранятся непосредственно на сервере, и доступ

к ним можно получить из любой точки мира, был бы там лишь доступ в Интернет! Также позволяет использовать программу 1С удаленно из любой точки планеты, при наличии Интернет канала.

7) Сервер баз данных (Database server)

Следующая роль следует из названия – обработка данных, организованных и структурированных согласно определенным правилам и хранимых совместно. Наиболее часто используемые средства управления данными это MS SQL Server, Oracle, Apache, MySql. В случае потребности бизнес процессов компании в подготовке и обработке данных необходим выделенный вычислительный ресурс. Как правило, параметры такого узла напрямую зависят от масштаба базы данных, количества пользователей, динамики и характера обращений к данным. Важность бизнес приложения связанного с обработкой данных в жизни компании определяет необходимый уровень доступности данных, т.е. отказоустойчивости и надежности такой системы.

8) Файловый сервер

Предназначен для организации и структурированного хранения данных пользователей с учетом политик безопасности и доступа. Количество пользователей и объем хранимых данных являются определяющими моментами при определении состава такой системы

9) Серверы приложений

Для сервера приложений характерны расширенные возможности обработки информации, а взаимодействие с клиентом становится подобным работе приложения. В маркетинге термином «сервер приложений» обычно обозначают предлагаемое продавцами комплексное решение, которое содержит все требуемые компоненты технологий. Для некоторых организаций такой комплексный подход к построению сервера приложений облегчает разработку благодаря унификации разрабатываемых моделей и централизации поддержки.

10) «Беспроводной» сервер

В своей простейшей интерпретации такой компьютер может представлять собой типичный Web-сервер или сервер приложений, который просто знает, как передавать документы, составленные на стандартном для беспроводных устройств языке. Часто в качестве такого языка выступает Wireless Markup Language (WML). Адаптация Web-сервера для работы в качестве беспроводного сервера, способного обрабатывать документы WML-типа, обычно сводится просто к тому, чтобы обучить сервер распознаванию этих документов. Web-серверу требуется только сообщить клиенту, что документ составлен в формате для беспроводных устройств, и на этом его работа заканчивается.

11) Брандмауэры (межсетевые экраны**)**, файрволлы

Это защитный экран от вредоносных воздействий из интернета, стена в одну строну пропускает исходящие данные, а в обратную (на прием) уже анализирует что именно поступает в сеть, определяя вредоносные данные, отсеивает их из общего потока входящей информации, что в настоящем времени является очень актуальной защитой от вирусов и атак из интернета. Прокси-серверы можно сконфигурировать так, что они будут принимать или отвергать определенные типы сетевых запросов, поступающие как из локальной сети, так и из Интернета. В такой конфигурации прокси-сервер становится межсетевым экраном – брандмауэром. Брандмауэр, как и подразумевает его «боевое» имя, представляет собой средство обеспечения безопасности, задачи которого во многом схожи с работой пограничников: осматривать каждый фрагмент данных, который пытается пересечь границу сети.

12) Серверы DHCP

В настоящее время во многих локальных сетях (интрасетях) также используется протокол TCP/IP, но иногда применяются и оригинальные протоколы обмена, такие, как NetBEUI или AppleTalk. IP-адрес компьютерам можно присваивать вручную, или же на одной из машин запускается так называемый сервер DHCP (Dynamic Host Configuration

Protocol), который автоматически присваивает IP-адрес каждой локальной машине. Основное преимущество сервера DHCP – свобода изменения конфигурации локальной сети при ее расширении, добавлении или удалении машин (например, портативных ПК).

13) Серверы FTP

Подобные серверы, работающие на основе протокола File Transfer Protocol, уже много десятилетий назад стали стандартом де-факто при перемещении файлов в Интернете. FTP-серверы поддерживают работу простых файловых менеджеров – клиентов. Сложные FTP-серверы обеспечивают администратору большие возможности управления в том, что касается прав на подключение и совместного использования файлов, типов разделяемых файлов и их размещения. Конфигурируемые ресурсы, выделяемые ряду соединений с сервером, ограничения на количество передаваемых данных и минимальную скорость передачи и т.п., становятся все более популярными средствами, помогающими повысить безопасность FTP-серверов.

14) Принт-серверы

Такие серверы позволяют всем подключенным к сети компьютерам распечатывать документы на одном или нескольких общих принтерах. В этом случае отпадает необходимость комплектовать каждый компьютер собственным печатающим устройством. Кроме того, принимая на себя все заботы о выводе документов на печать, принт-сервер освобождает компьютеры для другой работы. Например, принт-сервер хранит посланные на печать документы на своем жестком диске, выстраивает их в очередь и выводит на принтер в порядке очередности.

15) Маршрутизатор

Маршрутизатор – специализированный сетевой компьютер, имеющий минимум два сетевых интерфейса и пересылающий пакеты данных между различными сегментами сети, принимающий решения о пересылке на основании

информации о топологии сети и определённых правил, заданных администратором.

16) Домашний сервер

В связи с тем, что компьютерная техника имеет очень доступную цену, и проникает повсюду, а также современные операционные системы имеют серверные возможности. С их помощью можно предоставлять пользователям других (соседних) компьютеров доступ к данным на жестком диске или к принтеру, а также «делиться» каналом интернета. Кроме того, домашний сервер можно использовать для резервного хранения данных или, сделав его доступным через Интернет, работать с документами на нем с любого ПК, подключенного к глобальной Сети. «Поднять» домашний сервер для хранения файлов и разделения доступа к Интернету не так сложно, как может показаться неискушенному пользователю. Для этой цели можно использовать обычный компьютер, даже без монитора. Для файлового или простого веб-сервера достаточно компьютера с процессором не слабее Intell Pentium 4 или AMD Sempron, оперативной памятью объемом 512 Мб и приводом CD-ROM. Если же на компьютере планируется запуск игрового сервера (весьма популярная инициатива в небольших локальных сетях), потребуется машина помощнее.

В задании предполагается оценки эффективности обеспечения информационной безопасности вышеуказанных объектов.

1.3. Содержание задания и отчета

Необходимо последовательно:

1. Получить аналитические выражения функций ущерба и пользы из функции полезности.
2. Выбрать из таблиц выражения плотности вероятности и накопленной вероятности для заданного вида распределения.
3. На основе результатов пп. 1.1 и 1.2 получить аналитическое выражение ожидаемой эффективности атакуемой системы.
4. Модифицировать последнее выражение с учетом дискретизации по времени.
5. Построить выражение для интегральной оценки ожидаемой эффективности.
6. Упростить полученные выражения.
7. Обосновать выбор объекта (раздел 1.2) исследования для заданного закона распределения плотности вероятности отказа (на основе найденной статистика и доказательства статистической гипотезы).
8. Подобрать реальные параметры распределения для исследуемого объекта и осуществить численное моделирование оценки эффективности в динамике параметров.

1.4. Варианты индивидуальных заданий

Непрерывные распределения	**Вид функции полезности**	
	Экспоненциальная	**Показательная**
Бета-распределение	1 вариант	2 вариант
Гамма-распределение	3 вариант	4 вариант
Гиперэкспоненциальное	5 вариант	6 вариант
Логистическое	7 вариант	8 вариант
Логнормальное	9 вариант	10 вариант
Парето	11 вариант	12 вариант
Райса	13 вариант	14 вариант
Рэллея	15 вариант	16 вариант
Стьюдента	17 вариант	18 вариант
Фишера	19 вариант	20 вариант
Хи-квадрат	21 вариант	22 вариант
Вейбулла	23 вариант	24 вариант
Гомпертца	25 вариант	26 вариант
Дирихле	27 вариант	28 вариант
Колмогорова	29 вариант	30 вариант
Коши	31 вариант	32 вариант
Лапласа	33 вариант	34 вариант
Максвелла	35 вариант	36 вариант
Накагами	37 вариант	38 вариант
Эрланга	39 вариант	40 вариант
Дискретные распределения	**Вид функции полезности**	
	Экспоненциальная	**Показательная**
Биномиальное	41 вариант	42 вариант
Геометрическое	43 вариант	44 вариант
Гипергеометрическое	45 вариант	46 вариант
Логарифмическое	47 вариант	48 вариант
Пуассона	49 вариант	50 вариант

2. РАЗВИТИЕ АЛГОРИТМИЧЕСКОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КАК ИНСТРУМЕНТАРИЯ РИСК-АНАЛИЗА

2.1. Содержание заданий комплексных научно-исследовательский работ

2.1.1. Совершенствование и/или разработка алгоритмического и программного обеспечения риск-оценки и регулирования живучести и инфостойкости инновационных проектов различных типов и классов в контексте их выживания в условиях наличия разнообразных информационных рисков для всевозможных (п. 1.4) законов распределения плотности вероятности их отказов.

Для возможных непрерывных законов распределения получить и упростить аналитические выражения для риск-оценки живучести инновационных кибер-систем на основе отношения Милла:

$$\frac{1}{\mu} = \frac{1 - F(t)}{f(t)\,dt},$$

где:

$1 - F(t)$ – это вероятность того, что система доживет до возраста t;

$F(t)$ – это накопленная вероятность гибели системы в диапазоне времени [0, t];

$f(t)$ – плотность вероятности гибели системы в момент времени t;

$f(t)\,dt$ – вероятность гибели в возрасте $t \pm \frac{dt}{2}$;

dt – шаг дискретизации времени $dt = 1/k \cdot f_{max}$;

k – степень дискретизации $k \geq 2$.

Создать программное обеспечение автоматизированного численного расчета отношения Милла, включая

возможности управления этим параметром. Провести всестороннее имитационное моделирование в динамике управления риском.

Адаптация различных законов распределения к определенным классам и типам исследуемых объектов.

2.1.2. Решение аналогичной задачи для дискретных законов распределения.

2.1.3. Совершенствование и/или разработка элементов инструментария автоматизации анализа для всевозможных законов распределения плотности вероятности *f(x)* (п. 1.4) наступления ущерба *u* или получения пользы *v*

$$v(x) = \int_{0}^{x_0} \omega(x)dx;$$

$$u(x) = \int_{x_0}^{x_{\text{ср}}} \omega(x)dx,$$

для случайной переменной состояния *x*, заданной функцией полезности $\omega(x)$ и непрерывным законом распределения вероятности *F(x)*, в том числе в точке ожидаемого отказа.

Аналитически риск и шанс определяются следующим образом:

$$Risk(x_0) = \frac{u(x_0)f(x_0)}{k \cdot f_{max}};$$

$$Chance(x_0) = v(x_0) \cdot [1 - F(x_0)],$$

где f_{max} – пик плотности вероятности *f(x)*;

k – степень дискретизации.

2.1.4. Решение аналогичной задачи для дискретных законов распределения.

2.1.5. Разработка и/или совершенствование программного обеспечения (ПО) имитационного

моделирования актуальных корпоративных и/или безмасштабных сетей (конкретизируется базовым предприятием).

2.1.6. Web-программирование для риск-анализа социальных информационных сетей в целях противодействия проявлениям экстремизма (конкретизируется базовым предприятием).

2.1.7. Программирование в целях повышения привлекательности и защищенности Интернет-ресурсов кафедры (конкретизируется выпускающей кафедрой).

2.2. Содержание отчетов о работе

2.2.1. Формулировка задания.

2.2.2. Описание методического обеспечения.

2.2.3. Обоснование алгоритмического обеспечения и выбора версии языка программирования.

2.2.4. Описание формата представления данных.

2.2.5. Листинг программы.

2.2.6. Тестовые примеры.

2.2.7. Результаты контрольных расчетов.

2.2.8. Документы, подтверждающие регистрацию ПО в фонде алгоритмов и программ.

2.2.9. Проекты публикаций в изданиях кафедры.

3. ПОИСКОВЫЕ ИССЛЕДОВАНИЯ В ОБЛАСТИ РИСК-АНАЛИЗА

3.1. Тематика комплексных научно-исследовательских работ

Подготовка по ГОСТ обзорного материала и презентации (не менее 20 слайдов) по следующим проблемам:

3.1.1. Антология сетевых войн: цели, задачи, сценарии и средства их проведения, практические примеры и оценка перспектив развития и противодействия в контексте обеспечения информационной безопасности государства.

3.1.2. Социальные информационные сети как инструмент организации протестов и «цветных революций»: способы и средства возмущения социума, сценарий ослабления и свержения власти, меры противодействия в контексте обеспечения информационной безопасности государства.

3.1.3. Статистический риск-анализ всевозможных классов и типов атак на информационные кибер-системы: цели, частота атак и величина ущербов от их реализации, соответствующая оценка рисков в динамике развития сферы информационной безопасности за последние пять лет, выводы относительно опасности и возможностей противодействия.

3.1.4. Анализ и подготовка обзора научно-технических материалов по безмасштабным сетям в контексте обеспечения их безопасности.

3.1.5. Развитие научно-методического обеспечения теории ветвящихся процессов на риск-анализ распространения вредоносного программного обеспечения в сетевых структурах.

3.1.6. Развитие научно-методического обеспечения теории случайных графов на риск-анализ живучести сетевых структур.

3.1.7. Спецзадание: для студентов, состоящих в резерве аспирантуры кафедры (конкретизируется выпускающей кафедрой).

3.2. Содержание отчетов о работе

3.2.1. Постановка задач исследования.
3.2.2. Основное содержание (≈50 страниц).
3.2.3. Основные результаты работы.
3.2.4. Библиографический список (≈50 наименований)

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

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 компонент 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.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 выполнению научно-исследовательской работы
«Риск-анализ атакуемых информационных
технологий и систем»
для студентов специальностей
090301 «Компьютерная безопасность»,
090302 «Информационная безопасность
телекоммуникационных систем»,
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Составители:
Остапенко Александр Григорьевич
Бабаджанов Руслан Каландарович
Корнеева Наталья Николаевна

В авторской редакции

Подписано к изданию 06.04.2015.
Уч.-изд. л. 2,6.

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