ФГБОУ ВПО «Воронежский государственный
технический университет»

Кафедра систем информационной безопасности

359-2015

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к преддипломной практике
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, А. М. Горобцов, А. А. Грачёв

УДК 004.056

Методические указания к преддипломной практике 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, А. М. Горобцов, А. А. Грачёв. Воронеж, 2015. 68 с.

Методические указания призваны помочь студентам в проведении преддипломной практики. На обозрение вынесены основные этапы проведения преддипломной практики, рекомендации по её выполнению, а также предлагаемая методология проведения исследования.

Методические указания подготовлены в электронном виде в текстовом редакторе MS Word 2013 и содержатся в файле Остапенко_Преддипломная практика.pdf.

Табл. 7. Ил. 22. Библиогр.: 10 назв.

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

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

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

ВВЕДЕНИЕ. ОБЩИЕ РЕКОМЕНДАЦИИ

Преддипломная практика (ПДП) является важнейшим подготовительным этапом для написания выпускной квалификационной работы (ВКР).

Учитывая научно-исследовательский характер (ВКР) на этапе ПДП предлагается прежде всего концептуально определиться со следующими её параметрами:

1. Обоснование актуальности темы исследования (на основе анализа степени её проработанности по открытым информационным источникам).
2. Уточнение объекта и предмета исследования.
3. Формулировка целей и задач исследования.

Именно такие разделы рекомендуется иметь в отчёте по ПДП.

Первая процедура предусматривает анализ широко известных источников. Однако не следует увлекаться литературой по проблеме информационной безопасности вообще, акцентируя своё внимание источникам, посвященным исключительно теме исследования. А в этой связи может быть рекомендован перечень публикаций Воронежского научно-образовательного центра управления информационными рисками (ВНОЦ).

Вторая процедура вытекает из первой. Именно анализ литературы и выявленные противоречия позволяют наиболее точно определиться с объектом и предметом исследования. При этом следует избегать огульных формулировок и использования ненормативных терминов, что всегда весьма уязвимо для критики.

Третья процедура прежде всего предусматривает формулировку цели исследования. Она должна быть измерима, т.е. по результатам работы можно было конкретно и численно определить улучшение тех или иных показателей и/или характеристик безопасности объекта. Из цели вытекает 3-5 задач, её характеризующих. Однако и в их формулировках следует избегать «лозунгов» и общих фраз в одну строчку. Задачи должны быть конкретными и понятными, так как именно их решение выносится на защиты.

Только при выполнении вышеперечисленных рекомендаций может быть в дальнейшем получена качественная ВКР.

При проектировании концептуально следует исходить из того, что риск – это возможность наступления ущерба определённой величины, а безопасность – есть состояние системы, при котором риск не превышает допустимых значений. Поэтому исключительно вероятностные (без учёта ущерба) оценки нельзя считать полноценными с точки зрения процесса обеспечения безопасности, который на сегодня обязательно включает риск-анализ и даже управление рисками, имея в виду достижение заданной защищенности и живучести атакуемых объектов.

При этом, именно по сетям распространяются самые опасные вредоносы и реализуются наиболее ущербные атаки, что позволяет говорить о масштабных сетевых угрозах и объективной необходимости управления информационными рисками в сети.

Развитие сетевых технологий объективно тормозят следующие противоречия между:

– существующими оценками безопасности атакуемых по сети объектов и необходимостью выработки методологии их регулирования;

– предпринимаемыми попытками управлять параметрами сетевой безопасности и необходимостью выработки методологии их регулирования;

– отсутствием комплекса научно-обоснованных методов и острой необходимостью их применения на практике для снижения смертности и повышения эффективности атакуемых по сети объектов.

В разрешении вышеперечисленных противоречий, обобщённо, видится предмет исследований.

В результате пресса информационных угроз прогресс в сфере сетевых объектов и недостаточной эффективностью их функционирования. При этом, объектом исследования обобщённо выступают компьютерные сети (КС), информационно-телекоммуникационные сети (ИТКС) и прочие авторизированные информационные сети (АИС) корпоративного, безмасштабного и иного характера.

В целом проблему представляется возможным сформулировать следующим образом: создание теоритических основ и их практическое внедрение для оценки и регулирования ожидаемой эффективности защиты и живучести атакуемых по сети объектов в условиях структурной разнородности и параметрической многоплановости воздействующих на них сетевых угроз.

Отсюда целью исследования можно считать снижение смертности и повышение эффективности защиты вышеуказанных объектов за счёт разработки и внедрения соответствующей методологии, ориентированной на обеспечение их сетевой безопасности.

Из вышеизложенного следуют задачи исследования:

1. Идентификация сетевых инцидентов, поиск и всестороннее исследование статистики гибели объектов, атакуемых по сети, от разнообразных угроз информационного характера. Формулировка и доказательство статистических гипотез для как можно более полного множества атакуемых объектов.

2. Получение и развитие комплекса аналитических выражений: оценки смертности атакуемых объектов для всевозможных законов распределения плотности вероятности их гибели; ущербов и пользы для различных аппроксимаций функции производительности и разнообразных атакуемых объектов; ожидаемой эффективности для различных законов распределения гибели атакуемого по сети объекта. На основе полученных аналитических выражений создание прикладного программного обеспечения для численного расчёта и оптимизации ожидаемой эффективности защиты и живучести атакуемых объектов.

3. Разработка и алгоритмизация методологии параметрического регулирования эффективности и живучести объектов. Выработка рекомендаций и программная реализация алгоритмов по управлению эффективностью и жизнестойкостью объектов и их практическая реализация для реальных процессов в условиях воздействия различных сетевых угроз.

Настоящий подход не претендует на абсолютную полноту и каждой отдельной ВКР может быть конкретизирован.

1. РЕКОМЕНДУЕМЫЕ ОБЪЕКТЫ И ПРЕДМЕТЫ ИССЛЕДОВАНИЯ

Потребность классификации вредоносного программного обеспечения возникла одновременно с появлением первой антивирусной программы. Несмотря на то, что вирусов первоначально было мало, их всё равно необходимо было как-то отличать друг от друга по названиям.

Обычно использовали самую простую классификацию, состоящую из уникального имени вируса и размера детектируемого файла. Однако из-за того, что один и тот же вирус в разных антивирусных программах мог именоваться по-разному, началась путаница.

Попытки упорядочить процесс классификации были предприняты еще в начале 90-х годов прошлого века, в рамках альянса антивирусных специалистов CARO (Computer AntiVirus Researcher's Organization). Альянсом был создан документ «CARO malware naming scheme», который на какой-то период стал стандартом для индустрии.

Стремительное развитие вредоносных программ, появление новых платформ и рост числа антивирусных компаний привели к тому, что эта схема фактически перестала использоваться. Ещё более важной причиной отказа от неё стали существенные отличия в технологиях детектирования каждой антивирусной компании и, как следствие, невозможность унификации результатов проверки разными антивирусными программами.

Продолжаются попытки выработать новую общую классификацию детектируемых антивирусными программами объектов, однако они, по большей части, остаются малоуспешными. Наиболее значительным проектом подобного рода было создание организации CME (Common Malware Enumeration), которая присваивает одинаковым детектируемым объектам единый уникальный идентификатор.

Предложенная в «Лаборатории Касперского» система классификации детектируемых объектов [1] является одной из наиболее широко используемой в индустрии, и послужила

основой для классификаций некоторых других антивирусных компаний. В настоящее время классификация «Лаборатории Касперского» включает в себя весь объём детектируемых Антивирусом Касперского вредоносных или потенциально нежелательных объектов, и основана на разделении объектов по типу совершаемых ими на компьютере пользователей действий.

Типы детектируемых объектов

Вредоносные программы

Вредоносные программы создаются специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей. К данной категории относятся вирусы и черви, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников (инструменты для взлома, конструкторы полиморфного вредоносного кода и т. д.).

Вирусы и черви

Подобные вредоносные программы обладают способностью к несанкционированному пользователем саморазмножению в компьютерах или компьютерных сетях, при этом полученные копии также обладают этой возможностью.

К вирусам и червям не относятся:

– троянские программы, распространяющие свои копии по сети и заражающие удалённые машины по команде «хозяина» вредоносной программы (целый ряд представителей Backdoor);

– прочие троянские программы, создающие свои многочисленные копии в системе или даже «цепляющиеся» к каким-либо файлам, уже присутствующим в системе. Отличие от вирусов и червей состоит в невозможности дальнейшего самовоспроизведения копий.

Основным признаком, по которому различают типы (поведения) вирусов и червей, является способ их

распространения, т. е. как вредоносная программа передает свою копию по локальным или сетевым ресурсам.

Подобные вредоносные программы обладают способностью к несанкционированному пользователем саморазмножению в компьютерах или компьютерных сетях, при этом полученные копии также обладают этой возможностью.

К данной категории вредоносных программ относятся следующие поведения (табл. 1.1).

Троянские программы

Эти вредоносные программы созданы для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей. В отличие от вирусов и червей, представители данной категории не имеют способности создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения.

Основным признаком, по которому различают типы троянских программ, являются их несанкционированные пользователем действия — те, которые они производят на заражённом компьютере (табл. 1.2).

Таблица 1.1

Типы вирусов и червей

Название	Описание
Email-Worm	Вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по каналам электронной почты. В процессе размножения червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (например, URL на зараженный файл, расположенный на взломанном или хакерском веб-сайте). В первом случае код червя активизируется при открытии (запуске) заражённого вложения, во втором — при открытии ссылки на заражённый файл. В обоих случаях эффект одинаков — активизируется код червя. Для отправки зараженных сообщений почтовые черви используют различные способы. Наиболее распространены: – прямое подключение к SMTP-серверу, используя встроенную в код червя почтовую библиотеку; – использование сервисов MS Outlook; – использование функций Windows MAPI. Различные методы используются почтовыми червями для поиска почтовых адресов, на которые будут рассылаться зараженные письма. Почтовые черви: – рассылают себя по всем адресам, обнаруженным в адресной книге MS Outlook; – считывают адреса из адресной базы WAB; – сканируют «подходящие» файлы на диске и выделяют в них строки, являющиеся адресами электронной почты; – отсылают себя по всем адресам, обнаруженным в письмах в почтовом ящике (при этом некоторые почтовые черви «отвечают» на обнаруженные в ящике письма). Многие черви используют сразу несколько из перечисленных методов. Встречаются также и другие способы поиска адресов электронной почты
P2P-Worm	Вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по каналам файлообменных пиринговых сетей (например, Kazaa, Grokster, eDonkey, FastTrack, Gnutella и др.). Механизм работы большинства подобных червей достаточно прост — для внедрения в P2P-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению вируса P2P-сеть берет на себя — при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера. Существуют более сложные P2P-черви, которые имитируют сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечают положительно — при этом червь предлагает для скачивания свою копию
IM-Worm	Вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по каналам систем мгновенного обмена сообщениями (например, ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype и др.). Для этих целей черви, как правило, рассылают на обнаруженные контакты (из контакт-листа) сообщения, содержащие URL на файл с телом червя, расположенный на каком-либо сетевом ресурсе. Данный прием практически полностью повторяет аналогичный способ рассылки, использующийся почтовыми червями

Продолжение табл. 1.1

Название	Описание
Virus	Вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по локальным ресурсам компьютера. В отличие от червей, вирусы не используют сетевых сервисов для своего распространения и проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если заражённый объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например: – при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе; – вирус скопировал себя на съёмный носитель или заразил файлы на нем; – пользователь отослал электронное письмо с зараженным вложением
IRC-Worm	Вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению через Internet Relay Chats. У этого типа червей существует два способа распространения по IRC-каналам, напоминающие способы распространения почтовых червей. Первый способ заключается в отсылке URL на копию червя. Второй способ — отсылка зараженного файла какому-либо пользователю IRC-канала. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть (запустить на выполнение)
Worm	Вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению в компьютерных сетях через сетевые ресурсы. В отличие от Net-Worm для активации Worm пользователю необходимо запустить его. Черви этого типа ищут в сети удаленные компьютеры и копируют себя в каталоги, открытые на чтение и запись (если таковые обнаружены). При этом черви данного типа перебирают доступные сетевые каталоги, используя функции операционной системы, и случайным образом ищут компьютеры в глобальной сети, подключаются к ним и пытаются открыть их диски на полный доступ. Также к данному типу червей относятся черви, которые по тем или иным причинам не обладают ни одним из других поведений (например, «мобильные» черви)
Net-Worm	Вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению в компьютерных сетях. Отличительной особенностью данного типа червей является отсутствие необходимости в пользователе как в звене в цепочке распространения (т.е. непосредственно для активации вредоносной программы). Зачастую при распространении такой червь ищет в сети компьютеры, на которых используется программное обеспечение, содержащее критические уязвимости. Для заражения уязвимых компьютеров червь посылает специально сформированный сетевой пакет (эксплойт), в результате чего код (или часть кода) червя проникает на компьютер-жертву и активируется. Если сетевой пакет содержит только часть кода червя, то после проникновения в уязвимый компьютер он скачивает основной файл червя и запускает его на исполнение. Можно встретить сетевых червей данного типа, использующих сразу несколько эксплойтов для своего распространения, что увеличивает скорость нахождения ими компьютера-жертвы

Таблица 1.2

Типы троянских программ

Название	Описание
Backdoor	Вредоносная программа, предназначенная для скрытого удалённого управления злоумышленником пораженным компьютером. По своей функциональности бэкдоры во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами-производителями программных продуктов. Эти вредоносные программы позволяют делать с компьютером все, что в них заложил автор: принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т.д. Представители этого типа вредоносных программ очень часто используются для объединения компьютеров-жертв в так называемые «ботнеты», централизованно управляемые злоумышленниками в злонамеренных целях. Отдельно следует отметить группу бэкдоров, способных распространяться по сети и внедряться в другие компьютеры, как это делают сетевые черви. Отличает такие бэкдоры от червей то, что они распространяются по сети не самопроизвольно (как сетевые черви), а только по специальной команде «хозяина», управляющего данной копией троянской программы
Trojan-Banker	Вредоносная программа, предназначенная для кражи пользовательской информации, относящейся к банковским системам, системам электронных денег и пластиковых карт. Найденная информация передается злоумышленнику. Для передачи данных «хозяину» могут быть использованы электронная почта, FTP, HTTP (посредством указания данных в запросе) и другие способы
Trojan-Dropper	Вредоносная программа, предназначенная для несанкционированной пользователем скрытой инсталляции на компьютер-жертву вредоносных программ, содержащихся в теле этого типа троянцев. Данный тип вредоносных программ обычно без каких-либо сообщений (либо с ложными сообщениями об ошибке в архиве, неверной версии операционной системы и др.) сохраняют на диск жертвы (часто в каталог Windows, системный каталог Windows, временный каталог и т.д.) другие файлы и запускают их на выполнение. В результате использования программ данного класса хакеры достигают двух целей: – скрытной инсталляции троянских программ и вирусов; – защиты от детектирования известных вредоносных программ антивирусами, поскольку не все из них в состоянии проверить все компоненты внутри подобных троянцев
Trojan-Notifier	Вредоносная программа, предназначенная для несанкционированного пользователем сообщения своему «хозяину» о том, что заражённый компьютер сейчас находится «на связи». При этом на адрес злоумышленника отправляется информация о компьютере, например, IP-адрес компьютера, номер открытого порта, адрес электронной почты и т. п. Отсылка осуществляется различными способами: электронным письмом, специально оформленным обращением к веб-странице злоумышленника, ICQ-сообщением. Данные троянские программы используются в многокомпонентных троянских наборах для извещения злоумышленника об успешной инсталляции вредоносных программ в атакуемой системе
Trojan-Spy	Вредоносная программа, предназначенная для ведения электронного шпионажа за пользователем (вводимая с клавиатуры информация, снимки экрана, список активных приложений и т. д.). Найденная информация передается злоумышленнику. Для передачи данных «хозяину» могут быть использованы электронная почта, FTP, HTTP (посредством указания данных в запросе) и другие способы

Продолжение табл. 1.2

Название	Описание
Exploit	Программы, в которых содержатся данные или исполняемый код, позволяющие использовать одну или несколько уязвимостей в программном обеспечении на локальном или удаленном компьютере с заведомо вредоносной целью Обычно эксплойты используются злоумышленниками для проникновения на компьютер-жертву с целью последующего внедрения туда вредоносного кода (например, заражение всех посетителей взломанного веб-сайта вредоносной программой). Также эксплойты интенсивно используются программами типа Net-Worm для проникновения на компьютер-жертву без участия пользователя. Широко известны также так называемые программы-Nuker'ы, которые отправляют на локальный или удаленный компьютер специальным образом сформированные запросы, в результате чего система прекращает свою работу
Trojan-Clicker	Вредоносная программа, предназначенная для несанкционированного пользователем обращения к интернет-ресурсам (обычно, к веб-страницам). Достигается это либо посылкой соответствующих команд браузеру, либо заменой системных файлов, в которых указаны «стандартные» адреса интернет-ресурсов (например, файл hosts в MS Windows). У злоумышленника могут быть следующие цели для подобных действий: – увеличение посещаемости каких-либо сайтов с целью увеличения показов рекламы; – организация DoS-атаки (Denial of Service) на какой-либо сервер; – привлечение потенциальных жертв для заражения вирусами или троянскими программами
Trojan-FakeAV	Класс вредоносных программ, имитирующих работу антивирусного программного обеспечения или защитных компонентов операционной системы с целью получения от пользователя вознаграждения за обнаружение и удаление несуществующих угроз. Такие программы показывают множество нежелательных уведомлений, создают дискомфорт, стимулируя пользователя внести оплату. Иногда препятствуют нормальной работе компьютера, но, как правило, не блокируют систему полностью, чтобы не утратить доверие жертвы
Trojan-Proxy	Вредоносная программа, предназначенная для осуществления злоумышленником несанкционированного пользователем анонимного доступа к различным интернет-ресурсам через компьютер-жертву. Данный тип вредоносных программ обычно используется при рассылке спама через заражённые компьютеры
Trojan-Mailfinder	Вредоносная программа, предназначенная для несанкционированного пользователем сбора адресов электронной почты на компьютере с последующей передачей их злоумышленнику через электронную почту, HTTP, FTP или другими способами. Украденные адреса используются злоумышленниками при проведении последующих рассылок вредоносных программ и спама
Rootkit	Программа, предназначенная для сокрытия в системе определенных объектов, либо активности. Сокрытию, как правило, подвергаются ключи реестра (например, отвечающие за автозапуск вредоносных объектов), файлы, процессы в памяти зараженного компьютера, вредоносная сетевая активность. Сам по себе Rootkit ничего вредоносного не делает, но данный тип программ в подавляющем большинстве случаев используется вредоносными программами для увеличения собственного времени жизни в пораженных системах в силу затрудненного обнаружения
Trojan-DDoS	Вредоносная программа, предназначенная для проведения несанкционированной пользователем DoS (Denial of Service) атаки с пораженного компьютера на компьютер-жертву по заранее определенному адресу. Суть атаки сводится к посылке жертве многочисленных запросов, что приводит к отказу в обслуживании, если ресурсы атакуемого удаленного компьютера недостаточны для обработки всех поступающих запросов. Часто для проведения успешной DDoS-атаки злоумышленники предварительно заражают «троянцами» данного типа множество компьютеров (например, в ходе массированной спам-рассылки), после чего каждый из заражённых компьютеров атакует заданную жертву

Продолжение табл. 1.2

Название	Описание
Trojan-GameThief	Вредоносная программа, предназначенная для кражи пользовательской информации, относящейся к сетевым играм. Найденная информация передается злоумышленнику. Для передачи данных «хозяину» могут быть использованы электронная почта, FTP, HTTP (посредством указания данных в запросе) и другие способы
Trojan-Ransom	Вредоносная программа, предназначенная для несанкционированной пользователем модификации данных на компьютере-жертве таким образом, чтобы сделать невозможным работу с ними, либо блокировать нормальную работу компьютера. После того, как данные «взяты в заложники» (блокированы), пользователю выдвигается требование выкупа. Озвученную в требовании сумму жертва должна передать злоумышленнику, после чего злоумышленник обещает выслать программу для восстановления данных или нормальной работоспособности компьютера
Trojan-PSW	Вредоносная программа, предназначенная для кражи пользовательских аккаунтов (логин и пароль) с пораженных компьютеров. Название PSW произошло от Password-Stealing-Ware. При запуске PSW-троянцы ищут необходимую им информацию в системных файлах, хранящих различную конфиденциальную информацию, или реестре. В случае успешного поиска программа отсылает найденные данные «хозяину». Для передачи данных могут быть использованы электронная почта, FTP, HTTP (посредством указания данных в запросе) и другие способы. Некоторые троянцы данного типа воруют регистрационную информацию к различному программному обеспечению. Примечание: Trojan-PSW, занимающиеся кражей банковских аккаунтов, аккаунтов к интернет-пейджерам, а также аккаунтов к компьютерным играм относятся к Trojan-Banker, Trojan-IM и Trojan-GameThief соответственно. В отдельные типы данные вредоносные программы выделены в силу их многочисленности
Trojan-ArcBomb	Эти троянцы представляют собой архивы, специально сформированные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные — зависание или существенное замедление работы компьютера или заполнение диска большим количеством «пустых» данных. Особенно опасны «архивные бомбы» для файловых и почтовых серверов, если на сервере используется какая-либо система автоматической обработки входящей информации — «архивная бомба» может просто остановить работу сервера. Встречаются три типа подобных «бомб»: – некорректный заголовок архива; – повторяющиеся данные; – одинаковые файлы в архиве. Некорректный заголовок архива или испорченные данные в архиве могут привести к сбою в работе конкретного архиватора или алгоритма разархивирования при разборе содержимого архива. Значительных размеров файл, содержащий повторяющиеся данные, позволяет заархивировать такой файл в архив небольшого размера (например, 5 ГБ данных упаковываются в 200 КБ RAR- или в 480 КБ ZIP-архив). Огромное количество одинаковых файлов в архиве также практически не сказывается на размере архива при использовании специальных методов (например, существуют приемы упаковки 10100 одинаковых файлов в 30 KB RAR- или 230 KB ZIP-архив)

Окончание табл. 1.2

Название	Описание
Trojan-Downloader	Вредоносная программа, предназначенная для несанкционированной пользователем загрузки и установки на компьютер-жертву новых версий вредоносных программ, установки троянцев или рекламных систем. Загруженные из интернета программы затем либо запускаются на выполнение, либо регистрируются троянцем на автозагрузку в соответствии с возможностями операционной системы. Информация об именах и расположении загружаемых программ содержится в коде и данных троянца или скачивается троянцем с «управляющего» интернет-ресурса (обычно, с веб-страницы) Данный тип вредоносных программ в последнее время стал часто использоваться для первоначального заражения посетителей заражѐнных веб-страниц, содержащих эксплойты
Trojan-IM	Вредоносная программа, предназначенная для кражи пользовательских аккаунтов (логин и пароль) от интернет-пейджеров (например, ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype и др.). Найденная на заражѐнном компьютере информация передается злоумышленнику. Для передачи данных «хозяину» могут быть использованы электронная почта, FTP, WWW (посредством указания данных в запросе) и другие способы
Trojan-SMS	Вредоносная программа, предназначенная для несанкционированной пользователем отсылки SMS-сообщений с пораженных мобильных устройств на дорогостоящие платные номера, которые «жестко» записаны в теле вредоносной программы
Trojan	Вредоносная программа, предназначенная для осуществления несанкционированных пользователем действий, влекущих уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей, и при всём при этом не попадающая ни под одно из других троянских поведений. К Trojan также относятся «многоцелевые» троянские программы, т.е. программы, способные совершать сразу несколько несанкционированных пользователем действий, присущих одновременно нескольким другим поведениям троянских программ, что не позволяет однозначно отнести их к тому или иному поведению

Подозрительные упаковщики

Вредоносные программы часто сжимаются различными способами упаковки, совмещенными с шифрованием содержимого файла для того, чтобы исключить обратную разработку программы и усложнить анализ поведения проактивными и эвристическими методами. Антивирусом детектируются результаты работы подозрительных упаковщиков (табл. 1.3) — упакованные объекты. Существуют приемы борьбы с распаковкой: например, упаковщик может расшифровывать код не полностью, а лишь по мере исполнения, или, расшифровывать и запускать вредоносный объект целиком только в определенный день недели.

Таблица 1.3

Типы подозрительных упакощиков

Название	Описание
MultiPacked	Многократно упакованные различными программами упаковки файловые объекты. Антивирусный продукт выдает рассматриваемый вердикт при обнаружении исполняемых файлов, упакованных одновременно тремя и более упаковщиками
SuspiciousPacker	Файловые объекты, сжатые упаковщиками, созданными специально для защиты вредоносного кода от детектирования антивирусными продуктами
RarePacker	Файловые объекты, сжатые различными редко встречающимися упаковщиками, например, реализовывающими какую-либо концептуальную идею

Вредоносные утилиты

Вредоносные программы, разработанные для автоматизации создания других вирусов, червей или троянских программ, организации DoS-атак на удаленные сервера, взлома других компьютеров и т. п. В отличие от вирусов, червей и

троянских программ, представители данной категории не представляют угрозы компьютеру, на котором исполняются.

Основным признаком, по которому различают вредоносные утилиты (табл. 1.4), являются совершаемые ими действия.

Adware, Pornware и Riskware

Программы поведений Adware, Pornware и Riskware — это программы, которые разрабатываются и распространяются абсолютно легально и могут использоваться в повседневной работе, например, системных администраторов. Зачем они детектируются антивирусом? Дело в том, что некоторые программы обладают функциями, которые могут причинить вред пользователю — но только при выполнении ряда условий.

Например, если программа удаленного администрирования установлена на компьютер пользователя системным администратором, то ничего страшного в этом нет, т.к. администратор всего лишь получает возможность удаленно решать возникающие у пользователя проблемы. Но если та же программа установлена на компьютер пользователя злоумышленником, то он, фактически, получает полный контроль над компьютером-жертвой и в дальнейшем может использовать его по своему усмотрению. Таким образом, подобные программы могут быть использованы как во благо, так и во вред — в зависимости от того, в чьих руках они находятся.

Классификация детектируемых объектов «Лаборатории Касперского» выделяет эти программы в отдельную группу условно нежелательных программ — программ, которые невозможно однозначно отнести ни к опасным, ни к безопасным.

Таблица 1.4

Типы вредоносных утилит

Название	**Описание**
Constructor	Программы, предназначенные для изготовления новых компьютерных вирусов, червей и троянских программ. Известны конструкторы вредоносных программ для DOS, Windows и макроплатформ. Подобные программы позволяют генерировать исходные тексты вредоносных программ, объектные модули и непосредственно зараженные файлы. Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вредоносной программы, наличие или отсутствие самошифровки, противодействие отладчику и т. п.
HackTool	Программа, используемая злоумышленниками при организации атак на локальный или удаленный компьютер (например, несанкционированное пользователем внесение нелегального пользователя в список разрешенных посетителей системы; очистка системных журналов с целью сокрытия следов присутствия в системе; снифферы с выраженным вредоносным функционалом и т. д.)
Spoofer	Программы, позволяющие отправлять сообщения и сетевые запросы с поддельным адресом отправителя. Программы данного типа могут быть использованы с различными целями (например, затруднить обнаружение отправителя или выдать сообщение за сообщение, отправленное оригиналом)
DoS	Программа, предназначенная для проведения DoS-атаки (Denial of Service) с ведома пользователя на компьютер-жертву. Суть атаки сводится к посылке жертве многочисленных запросов, что приводит к отказу в обслуживании, если ресурсы атакуемого удаленного компьютера недостаточны для обработки всех поступающих запросов
Hoax	Программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. К «злым шуткам» относятся, например, программы, которые «пугают» пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), выводят странные вирусоподобные сообщения и т. д. — в зависимости от «чувства юмора» автора такой программы
VirTool	Программы, позволяющие злоумышленнику модифицировать другие вредоносные программы таким образом, чтобы они не детектировались антивирусным программным обеспечением
Email-Flooder	Программы, функцией которых является «забивание мусором» (бесполезными сообщениями) каналов электронной почты. Данные программы могут использоваться спамерами
IM-Flooder	Программы, функцией которых является «забивание мусором» (бесполезными сообщениями) каналов интернет-пейджеров (например, ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype и др.). Данные программы могут использоваться спамерами
Flooder	Программы, функцией которых является «забивание мусором» (бесполезными сообщениями) сетевых каналов, отличных от почтовых, интернет-пейджеров и SMS (например, IRC). Программы, «забивающие» каналы почтовых служб, интернет-пейджеров и SMS-каналы, относятся соответственно к Email-Flooder, IM-Flooder и SMS-Flooder
SMS-Flooder	Программы, функцией которых является «забивание мусором» (бесполезными сообщениями) каналов передачи SMS-сообщений

Adware

Adware (Adware, Advware, Browser Hijackers) — рекламное программное обеспечение, предназначенное для показа рекламных сообщений (чаще всего, в виде графических баннеров); перенаправления поисковых запросов на рекламные веб-страницы; а также для сбора данных маркетингового характера об активности пользователя (например, какие тематические сайты посещает пользователь), позволяющих сделать рекламу более таргетированной.

За исключением показов рекламы, подобные программы, как правило, никак не проявляют своего присутствия в системе — отсутствует значок в системном трее, нет упоминаний об установленных файлах в меню программ. Часто у Adware-программ нет процедур деинсталляции, используются пограничные с вирусными технологии, позволяющие скрытно внедряться на компьютер пользователя и незаметно осуществлять на нѐм свою деятельность.

Проникновение

На компьютеры пользователей Adware чаще всего попадает двумя способами:

– путем встраивания рекламных компонентов в бесплатное и условно-бесплатное программное обеспечение (freeware, shareware);

– путем несанкционированной пользователем установки рекламных компонентов при посещении пользователем «заражённых» веб-страниц.

Большинство программ freeware и shareware прекращает показ рекламы после их покупки или регистрации. Подобные программы часто используют встроенные Adware-утилиты сторонних производителей. В некоторых случаях эти Adware-утилиты остаются установленными на компьютере пользователя и после регистрации программ, с которыми они изначально попали в операционную систему. При этом удаление Adware-компонента, всѐ еще используемого какой-либо

программой для показа рекламы, может привести к сбоям в функционировании этой программы.

Базовое назначение Adware данного типа — неявная форма оплаты программного обеспечения, осуществляемая за счет показа пользователю рекламной информации (рекламодатели платят за показ их рекламы рекламному агентству, рекламное агентство — разработчику Adware). Adware помогает сократить расходы как разработчикам программного обеспечения (доход от Adware стимулирует их к написанию новых и совершенствованию существующих программ), так и самим пользователям.

В случае установки рекламных компонентов при посещении пользователем «заражённых» веб-страниц в большинстве случаев используются хакерские технологии: проникновение в компьютер через «дыры» в системе безопасности интернет-браузера, а также использование троянских программ, предназначенных для скрытной установки программного обеспечения (Trojan-Downloader или Trojan-Dropper). Adware-программы, действующие подобным образом, часто называют «Browser Hijackers».

Доставка рекламы

Известны два основных способа доставки рекламной информации:

– скачивание рекламных текстов и изображений с веб- или FTP-серверов, принадлежащих рекламодателю;

– перенаправление поисковых запросов интернет-браузера на рекламный веб-сайт.

Перенаправление запросов в некоторых случаях происходит только при отсутствии запрашиваемой пользователем веб-страницы, т.е. при ошибке в наборе адреса страницы.

Сбор данных

Многие рекламные системы помимо доставки рекламы также собирают конфиденциальную информацию о компьютере и пользователе:

– IP-адрес компьютера;

– версию установленной операционной системы и интернет-браузера;

– список часто посещаемых пользователем интернет-ресурсов;

– поисковые запросы;

– прочие данные, которые можно использовать при проведении последующих рекламных кампаний.

Примечание: не стоит путать Adware, занимающиеся сбором информации, с троянскими шпионскими программами. Отличие Adware состоит в том, что они осуществляют подобный сбор с согласия пользователя.

Если Adware никак не уведомляет пользователя об осуществляемом ей сборе информации, то она попадает под поведение Trojan-Spy и относится к категории вредоносных программ.

Pornware

Pornware — программы, которые так или иначе связаны с показом пользователю информации порнографического характера.

Программы категории Pornware могут быть установлены пользователем на свой компьютер сознательно, с целью поиска и получения порнографической информации. В этом случае они не являются вредоносными.

С другой стороны, те же самые программы могут быть установлены на пользовательский компьютер злоумышленниками – через использование уязвимостей операционной системы и интернет-браузера или при помощи вредоносных троянских программ классов Trojan-Downloader или Trojan-Dropper (табл. 1.5). Делается это обычно с целью «насильственной» рекламы

платных порнографических сайтов и сервисов, на которые пользователь сам по себе никогда не обратил бы внимания.

Таблица 1.5

Типы Pornware

Название	Описание
Porn-Dialer	Программы, дозванивающиеся до порнографических телефонных служб, параметры которых сохранены в теле этих программ. Отличие от вредоносных скрытых программ дозвона состоит в том, что пользователь уведомляется программой о совершаемых ею действиях
Porn-Downloader	Программы, выполняющие загрузку из сети на компьютер пользователя данных порнографического характера. Отличие от вредоносных программ загрузки состоит в том, что пользователь уведомляется программой о совершаемых ею действиях
Porn-Tool	Программы, так или иначе связанные с поиском и показом порнографических материалов (например, специальные панели инструментов для интернет-браузера и особые видеоплееры)

Riskware

Riskware – к этой категории относятся обычные программы (некоторые из них свободно продаются и широко используются в легальных целях), которые, тем не менее, в руках злоумышленника способны причинить вред пользователю (вызвать уничтожение, блокирование, модификацию или копирование информации, нарушить работу компьютеров или компьютерных сетей).

В списке программ категории Riskware можно обнаружить коммерческие утилиты удаленного администрирования, программы-клиенты IRC, программы дозвона, программы для

загрузки («скачивания») файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, а также многочисленные интернет-серверы служб FTP, Web, Proxy и Telnet.

Все эти программы не являются вредоносными сами по себе, однако обладают функционалом, которым могут воспользоваться злоумышленники для причинения вреда пользователям.

Выбор, детектировать или нет подобные программы, лежит на пользователе. По умолчанию в антивирусных продуктах «Лаборатории Касперского» детектирование Riskware отключено. У вас нет повода для беспокойства, если подобная программа установлена на компьютер вами или вашим сетевым администратором.

К этой категории детектируемых объектов относятся (табл. 1.6):

Таблица 1.6

Типы Riskware

Название	Описание
Client-IRC	Программы, используемые для общения в Internet Relay Chats. Вредоносными не являются. Детектирование добавлено по причине частого использования злоумышленниками расширенного функционала этих программ — с завидной периодичностью обнаруживаются вредоносные программы, устанавливающие Client-IRC на пользовательские компьютеры со злонамеренными целями
Downloader	Программы, позволяющие осуществлять в скрытом режиме загрузку различного контента с сетевых ресурсов. Вредоносными не являются. Подобные программы могут использоваться злоумышленниками для загрузки вредоносного контента на компьютер-жертву
PSWTool	Программы, позволяющие просматривать или восстанавливать забытые (часто — скрытые) пароли. С таким же успехом в подобных целях данный тип программ может быть использован злоумышленниками. Вредоносными не являются
Server-Proxy	Программы, содержащие функциональность proxy-сервера. По этой причине включаются злоумышленниками в пакеты вредоносных программ, например, для рассылки спама или иного вредоносного контента от имени компьютера-жертвы. Вредоносными не являются
Client-P2P	Программы, используемые для работы в peer-to-peer сетях. Вредоносными не являются. Детектирование добавлено по просьбам пользователей, т.к. ряд программ подобного рода стал причиной утечки конфиденциальной информации
FraudTool	Программы, которые выдают себя за другие программы, хотя таковыми не являются. Часто предлагают пользователю перечислить финансовые средства на определенные счета для оплаты «услуг». В качестве примера таких программ можно привести псевдоантивирусы, которые выводят сообщения об «обнаружении» вредоносных программ, но на самом деле ничего не находят и не лечат
RemoteAdmin	Программы, используемые для удаленного управления компьютером. Вредоносными не являются. Будучи установленными злоумышленником дают ему возможность полного контроля над компьютером-жертвой
Server-Telnet	Программы, содержащие функциональность telnet-сервера. По этой причине включаются злоумышленниками в пакеты вредоносных программ, например, для организации удаленного доступа к компьютеру-жертве, где установлена эта программа. Вредоносными не являются
Client-SMTP	Программы, используемые для отправки электронной почты и имеющие скрытый режим работы. Вредоносными не являются. Эти программы могут включаться злоумышленниками в состав пакета вредоносных программ для рассылки спама или иного вредоносного контента с компьютеров пользователей
Monitor	Программы, содержащие функции наблюдения за активностью на компьютере пользователя (активные процессы, сетевая активность и т.д.). Вредоносными не являются. В этих же целях могут быть использованы злоумышленниками
RiskTool	Программы, обладающие различной функциональностью (например, сокрытие файлов в системе, сокрытие окон запущенных приложений, уничтожение активных процессов и т.д.), позволяющей использование их киберпреступниками со злонамеренными целями. Вредоносными не являются. В отличие от NetTool, подобные программы предназначены для локальной работы
Server-Web	Программы, содержащие функциональность веб-сервера. По этой причине включаются злоумышленниками в пакеты вредоносных программ, например, для организации удаленного доступа к компьютеру-жертве, где установлена эта программа. Вредоносными не являются
Dialer	Программы, позволяющие устанавливать в скрытом режиме телефонные соединения через модем. Вредоносными не являются

Продолжение табл. 1.6

Название	Описание
NetTool	Программы, обладающие различной сетевой функциональностью (например, удаленная перезагрузка компьютера, сканирование открытых сетевых портов, удаленный запуск произвольных приложений и т.д.), позволяющей использование их киберпреступниками со злонамеренными целями. Вредоносными не являются. В отличие от RiskTool, подобные программы предназначены для работы с сетью
Server-FTP	Программы, содержащие функциональность FTP-сервера. По этой причине включаются злоумышленниками в пакеты вредоносных программ, например, для организации удаленного доступа к компьютеру-жертве, где установлена эта программа. Вредоносными не являются
WebToolbar	Программы, которые с разрешения пользователя расширяют возможности пользовательского программного обеспечения путѐм установки панелей инструментов, позволяющих использовать одну или несколько поисковых систем при работе в интернете. Вредоносными не являются. Детектирование добавлено по причине частого распространения подобных панелей с помощью различных вредоносных программ в виде вложенных в них файлов

2. РЕКОМЕНДУЕМАЯ МЕТОДОЛОГИЯ РИСК-АНАЛИЗА

2.1. Расчёт параметров рисков для компонентов систем

Многоальтернативность и непредсказуемость атак на компоненты системы зачастую не оставляют надежд для детерминированного описания этих процессов и возникающих в результате их реализации ущербов. Поэтому при создании защищенных автоматизированных систем, рассмотрение ущерба как случайной величины представляется вполне обоснованным. В этом случае описание принято осуществлять с использованием различных законов распределения, среди которых наибольшее популярностью пользуются регулярные законы. В этом классе наиболее практическое применение нашли законы, определенные на $[0, \infty]$ экспоненциальный и логнормальный законы; гамма-распределение; распределения Эрланга, Вейбулла и Релея.

Рассмотрим это семейство в контексте построения риск-моделей атакуемых систем, имея ввиду следующие обозначения:

$\varphi(u)$ – плотность вероятности наступления ущерба u;

$a_1 = \int_0^\infty u^k \varphi(u) du$ – k-ый начальный момент $\varphi(n)$;

$a_k = M$ – среднее значение u;

$\mu_k = \int_0^\infty (u - M)^k \varphi(u) du$ – k-ый центральный момент $\varphi(n)$;

$\sqrt{\mu_2} = \sigma$ – среднеквадратическое отклонение u от среднего значения M;

u_0 – мода, соответствующая максимальному значению $\varphi(n)$

$A_s = \frac{\mu_3}{\sqrt{\mu_2^3}}$ – асимметрия, характеризующая отклонение кривой $\varphi(u)$ от симметрии;

$E_x = \frac{\mu_4}{\mu_2^2} - 3$ – эксцесс, характеризующий островершинность $\varphi(u)$ в сравнении с нормальной кривой.

Опираясь на этот параметрический базис, постараемся проанализировать функцию риска, которая в общем случае имеет следующий вид:

$$Risk(u) = u\varphi(u). \qquad (2.1)$$

При этом, будем исходить из того, что на основе статистики определен закон распределения φ(u), т.е. выдвинута и доказана гипотеза (скажем, с помощью критериев Пирсона или Колмогорова), определены параметры φ(u), соответствующие статданным.

На основании вышеизложенного найдем аналитические выражения для параметров риска через перечисленные параметры плотности вероятности наступления ущерба. Рассмотрим прежде начальные моменты риска:

$$a_k^* = \frac{\int_0^\infty u^k Risk(u)du}{\int_0^\infty Risk(u)du} = \frac{\int_0^\infty u^k u\,\varphi(u)du}{\int_0^\infty u\,\varphi(u)du} =$$

$$= \frac{\int_0^\infty u^{k+1} u\,\varphi(u)du}{\int_0^\infty u\,\varphi(u)du} = \frac{a_{k+1}}{a_1}, \qquad (2.2)$$

Отсюда среднее значение ущерба для кривой риска равно

$$M^* = \frac{a_2}{a_1}.$$

Соответственно для центральных моментов риска имеем:

$$\mu_k^* = \frac{\int_0^\infty (u - M^*)^k Risk(u)du}{\int_0^\infty Risk(u)du} = \frac{\int_0^\infty (u - M^*)^k u\,\varphi(u)du}{\int_0^\infty u\,\varphi(u)du}. \qquad (2.3)$$

Так, для центрального момента риска получаем выражение:

$$\mu_2^* = \frac{\int_0^\infty (u - M^*)^2 u\,\varphi(u)du}{a_1} =$$

$$= \frac{1}{a_1}\int_0^\infty [u^2 - 2uM^* + (M^*)^2\varphi(u)du =$$

$$= \frac{1}{a_1}\{\int_0^\infty u^3\,\varphi(u)du - 2M^*\int_0^\infty u^2\varphi(u)du + (M^*)^2\int_0^\infty u\varphi(u)du\} =$$

$$= \frac{1}{a_1}[a_3 - 2M^* a_2 + (M^*)^2 a_1] = \frac{a_3}{a_1} - 2M^* \frac{a_2}{a_1} + (M^*)^2 =$$

$$= \frac{a_3}{a_1} - \left(\frac{a_2}{a_1}\right)^2. \qquad (2.4)$$

Отсюда среднеквадратическое отклонение будет равно:

$$\sigma^* = \sqrt{\frac{a_3}{a_1} - 2M^* \frac{a_2}{a_1} + (M^*)^2}. \qquad (2.5)$$

Следует заметить, что подобное отклонение может быть найдено относительно моды риска, которая может быть определена из решения следующего уравнения:

$$Risk'(u) = [u\varphi(u)]' = \varphi(u) + u\varphi'(u) = 0 \qquad (2.6)$$

Для оценки ассиметрии и островершинности кривой риска необходимо найти подобные аналитические выражения для третьего и четвертого центральных моментов риска:

$$\mu_3^* = \frac{\int_0^\infty (u - M^*)^k Risk(u)du}{\int_0^\infty Risk(u)du} = \frac{\int_0^\infty (u - M^*)^3 u\,\varphi(u)du}{\int_0^\infty u\,\varphi(u)du} =$$

$$= \frac{1}{a_1}\int_0^\infty [u^3 - 3u^2M^* + 3(M^*)^2 u - (M^*)^3]u\,\varphi(u)du =$$

$$= \frac{1}{a_1}\{\int_0^\infty u^4\,\varphi(u)du - 3M^*\int_0^\infty u^3\varphi(u)du +$$

$$+(M^*)^3\int_0^\infty u\varphi(u)du\} = \frac{1}{a_1}[a_3 - 3M^* a_3 + 3(M^*)^2 a_2 +$$

$$+(M^*)^2 a_1] = \frac{a_4}{a_1} - 3M^*\frac{a_3}{a_1} + 3(M^*)^2\frac{a_2}{a_1} + (M^*)^3; \qquad (2.7)$$

$$\mu_4^* = \frac{\int_0^\infty (u - M^*)^4 Risk(u)du}{\int_0^\infty Risk(u)du} = \frac{\int_0^\infty (u - M^*)^4 u\,\varphi(u)du}{\int_0^\infty u\,\varphi(u)du} =$$

$$= \frac{1}{a_1}\int_0^\infty [u^4 - 4u^3M^* + 6(M^*)^2u^2 - 4(M^*)^3 u +$$

$$+ (M^*)^4]u\,\varphi(u)du =$$

$$= \frac{a_5}{a_1} - 4M^*\frac{a_4}{a_1} + 6(M^*)^2\frac{a_2}{a_1} - 4(M^*)^3\frac{a_2}{a_1} + (M^*)^4 \qquad (2.8)$$

Осуществляя подстановку $M^* = \frac{a_2}{a_1}$ получим:

$$\mu_4^* = \frac{a_5}{a_1} - 4\frac{a_5}{a_1} + 6\frac{a_5\mu_3^*}{a_1} - 3\frac{a_2^4}{a_1^4}. \quad (2.9)$$

Для удобства дальнейшего анализа, все они сведены в нижеприведённую таблицу (табл. 2.1).

Таблица 2.1

Обобщённые аналитические выражения для расчёта параметров риска

Параметры риска	Аналитические выражения параметров
Начальные моменты	$\frac{a_{k+1}}{a_1}$
Среднее значение ущерба	$M^* = \frac{a_2}{a_1}$
Второй центральный момент	$\frac{a_3}{a_1} - (\frac{a_2}{a_1})^2.$
Среднеквадратическое отклонение ущерба	$\sqrt{\frac{a_3}{a_1} - 2M^*\frac{a_2}{a_1} + (M^*)^2}$
Третий центральный момент	$\mu_3^* = \frac{a_4}{a_1} - 3M^*\frac{a_3}{a_1} + 3(M^*)^2\frac{a_2}{a_1} - (M^*)^3$
Четвёртый центральный момент	$\mu_4^* = \frac{a_5}{a_1} - 4\frac{a_5}{a_1} + 6\frac{a_5\mu_3^*}{a_1} - 3\frac{a_2^4}{a_1^4}$
Ассиметрия	$A_s^* = \frac{\mu_3}{\sqrt{(\mu_2^*)^3}}$
Эксцесс	$E_x^* = \frac{\mu_4^*}{(\mu_2^*)^2} - 3$
где a_k – начальные моменты плотности вероятности наступления ущерба	

Как видно, для проведения численных расчетов вышеуказанных параметров достаточно знать величины первых начальных моментов плотности вероятности наступления ущерба.

Что же касается моды, то для рассматриваемого

семейства экспоненциальных распределений можно сделать следующее обобщение

$$\varphi(u) = \frac{A(u)}{\exp[B(u)]}, \qquad (2.10)$$

где функции и определяются видом распределения.

Поиск экстремума риска сводится к решению уравнения:

$$\varphi(u) = u\varphi'(u) = \frac{A(u)}{\exp[B(u)]} + \left[\frac{A'(u)}{\exp[B(u)]} - \frac{A(u)B'(u)}{\exp[B(u)]}\right] = 0, \qquad (2.11)$$

или

$$A(u) = uA'(u) - uA(u)B'(u) = 0. \qquad (2.12)$$

Решение этого уравнения u_0^* позволяет найти пик риска $Risk_{max} = Risk(u_0^*)$. Представленные параметры достаточно полно характеризуют кривую риска.

Однако возможен и более упрощенный вариант, когда уместно ограничиться нахождением моды и среднего значения, а также их среднеквадратических отклонений. Упрощенный алгоритм изображен на рис. 1.1, 1.2.

Воспользовавшись данными алгоритмами, можно рассчитать риск-параметры компонент системы с последующим обобщением ее анализом с учетом вклада всех компонентов. На этапе оценки риска компонента системы возможны две стратегии:

– экстремальная оценка:

$$Risk^{(\text{экс})} = m_u \mp \sigma_u = u_0^* \mp \sigma_0^*, \qquad (2.13)$$

и

– средняя оценка:

$$Risk^{(\text{ср})} = m_u \mp \sigma_u = M_0^* \mp \sigma^*. \qquad (2.14)$$

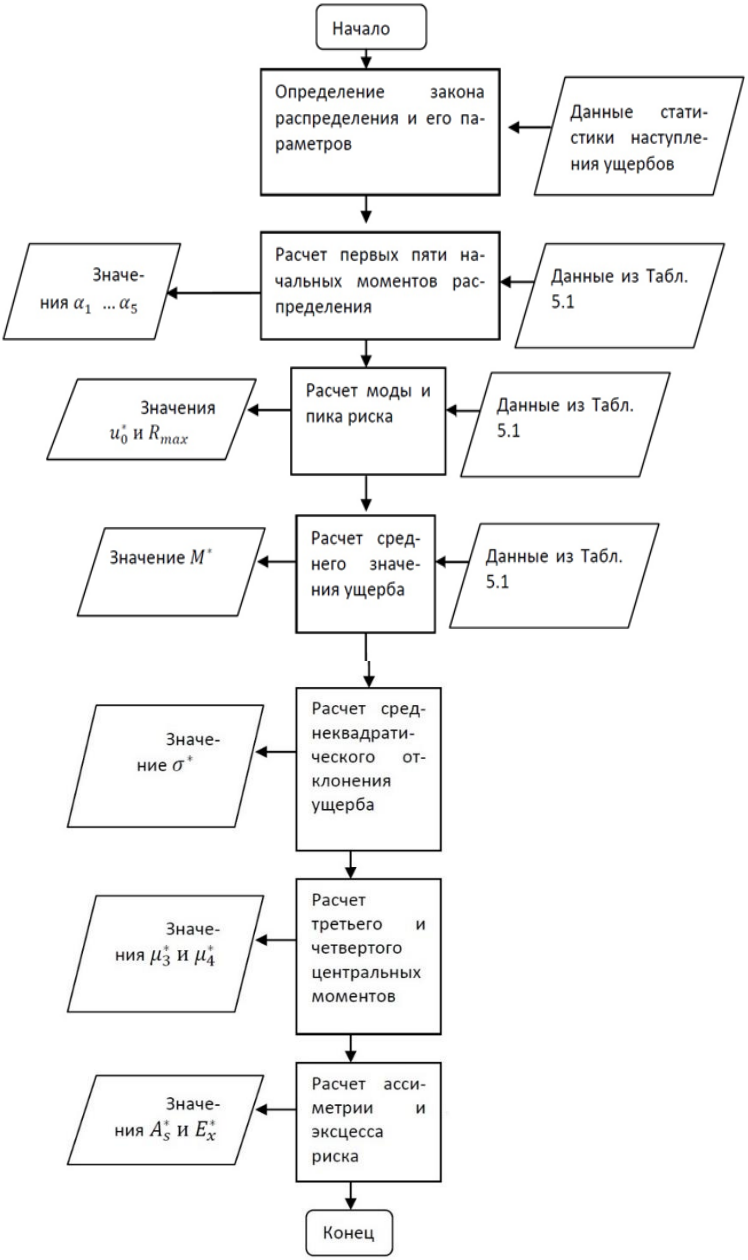

Рис. 2.1. Упрощенный алгоритм расчёта параметров риска

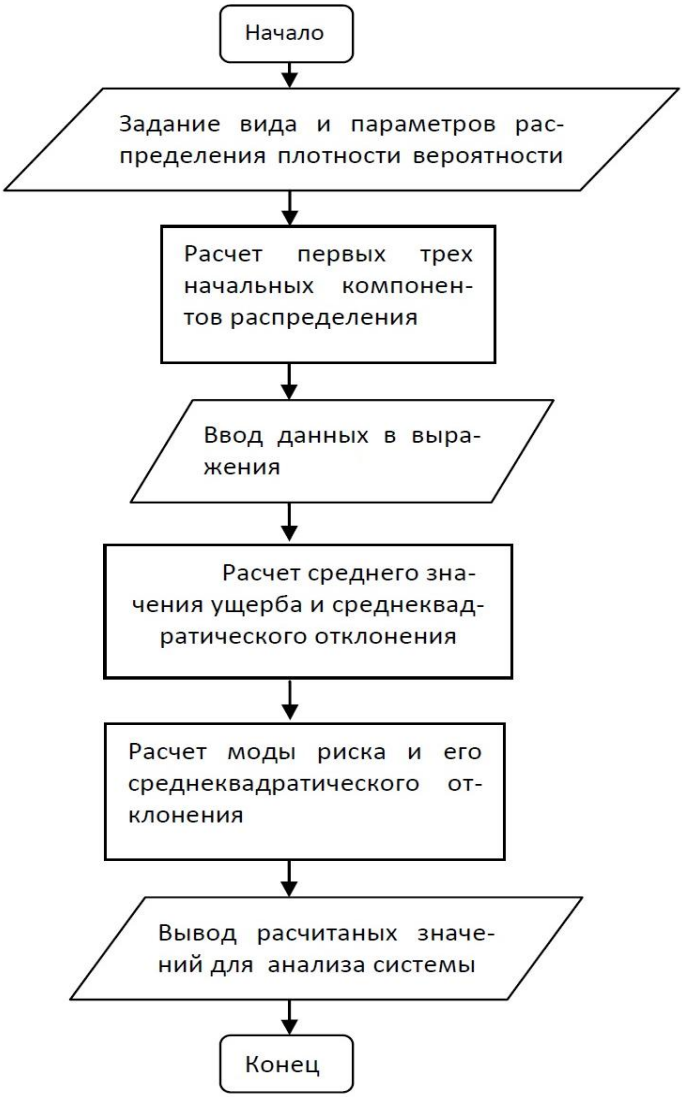

Рис. 2.2. Упрощенный алгоритм расчёта параметров риска для компонентов систем

2.2. Алгоритмическое обеспечение риск-анализа систем в диапазоне ущербов

Рассмотрим экспоненциальное семейство распределений плотности вероятности $\varphi(u)$ наступления ущерба с областью определения u>0. К таковым относятся логнормальное, экспоненциальное и гамма-распределения, распределения Релея, Вейбула и Эрланга. Соответствующие им аналитические выражения риска представлены в табл. 2.2.

Анализ аналитических выражений риска (табл. 2.2) позволяет для первых пяти видов распределения сделать следующее обобщение:

$$Risk(x) = \frac{ax^b}{\exp(x)}, \qquad (2.15)$$

где $x = \lambda u, (\lambda u)^2, (\lambda u)^d$;

$b = \frac{1}{2}, 1, n$;

$a = 1, 2, \frac{\lambda^c}{\Gamma(c)}, \frac{1}{(n-1)!}, d.$

Таблица 2.2

Анализ аналитических выражений риска.

Вид распределения плотности вероятности ущерба	Аналитическое выражение для риска
Экспоненциальный	$Risk(u) = \frac{\lambda u}{\exp(\lambda u)}$
Релея	$Risk(u) = \frac{2\lambda u}{\exp(\lambda u)^2}$
Гамма	$Risk(u) = \frac{\lambda^c}{\Gamma(c)} \frac{(\lambda u)^c}{\exp(\lambda u)}$
Эрланга	$Risk(u) = \frac{1}{(n-1)!} \frac{(\lambda u)^n}{\exp(\lambda u)}$
Вейбулла	$Risk(u) = d \frac{(\lambda u)^d}{\exp[(\lambda u)^d]}$
Логнонормальный	$Risk(u) = \frac{1}{\sigma\sqrt{2\pi}} \frac{1}{\exp[\frac{(\ln u - m)^1}{1\sigma^2}]}$

С целью нахождения значений ущерба по заданному уровню риска для (2.15) составим следующее уравнение:

$$R_{max}k = \frac{ax^b}{\exp(x)}, \quad (2.16)$$

где R_{max} – пиковое значение риска;

k – коэффициент (k<1) задающий уровень отсчёта от R_{max}.

Для поиска решения уравнения 2.16 прологарифмируем его:

$$\ln a + b \ln x - x = lnR_{max} + \ln k.$$

Далее разложим натуральный логарифм в ряд:

$$\ln a + 2b\left[\frac{x-1}{x+1} + \frac{1}{3}\left(\frac{x-1}{x+1}\right)^3\right] - x = lnR_{max} + \ln k. \quad (2.17)$$

Произведем следующую замену переменных:

$$y = \frac{x-1}{x+1},$$

где -1<y<1 – область определения.

В результате получим уравнение:

$$2b\left[y + \frac{1}{3}y^3\right] - \frac{1+y}{1-y} = c, \quad (2.18)$$

где $c = lnR_{max} + \ln k - \ln a$.

Приведя к общему знаменателю и сгруппировав члены по степеням получим уравнение четвёртой степени:

$$y^4 - y^3 + 3y^2 + 3\left(\frac{1-c}{2b} - 1\right)y + \frac{3}{2b}(c+1) = 0. \quad (2.19)$$

Данное уравнение, как известно может быть решено в аналитическом виде. Два корня этого уравнения будут комплексными числами, а два других, имеющими физический смысл, действительными.

Графически это решение можно проиллюстрировать с помощью рис. 2.3.

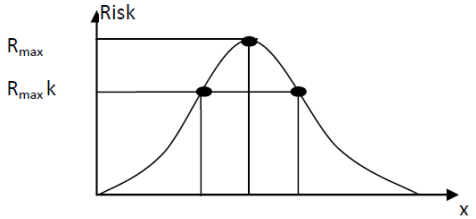

Рис. 2.3. Границы ущербов по заданному значению

2.3. Расчёт риском распределённых систем на основе параметров рисков их компонентов

При создании защищенных автоматизированных систем, рассмотрение ущерба как случайной величины довольно распространено. Причем описание принято осуществлять с использованием различных законов распределения, среди которых наибольшее популярностью пользуются регулярные законы. В данном классе существенное практическое применение нашло экспоненциальное (x>0) семейство: экспоненциальный и логнормальный законы; гамма-распределение; распределение Эрланга, Вейбулла и Релея.

Рассмотрим это семейство в контексте построения риск-моделей атакуемых систем, имея ввиду следующие обозначения:

$\varphi(u)$-плотность вероятности наступления ущерба u;

$\alpha_k \int_0^\infty u^k \varphi(u) du$ – k-ый начальный момент $\varphi(n)$;

$Risk(u) = u\ \varphi(u)$ – риск наступления ущерба u.

Будем исходить из того, что на основе статистики определен закон распределения $\varphi(u)$, т.е. выдвинута и доказана гипотеза (скажем, с помощью критериев Пирсона или Колмогорова), определены параметры $\varphi(u)$, соответствующие стандартным. Когда оценка рисков компонентов распределенной системы осуществлена, т. е. известны законы распределения риска и найдены его параметры для каждого компонента, представляется возможность рассчитать риск системы в целом. При этом, будем исходить из того, что ущербы, возникающие в ее компонентах при отказах и атаках на них слабо коррелированны между собой. Тогда ожидаемый общий ущерб системы можно найти как сумму ущербов в отдельных ее компонентах. Причем это допустимо не только для детерминированных, но и для случайных величин. С другой стороны относительная независимость этих параметров открывает перспективу соответствующих вероятностных оценок, рассматривая вероятность наступления общего ущерба как произведение вероятностей возникновения ущербов в компонентах системы. В этой связи может быть

предложено следующее выражение оценки риска.

$$Risk_{\Sigma} = \left(\sum_{i=1}^{n} u_i\right) \prod_{i=1}^{n} \varphi_i u_i, \qquad (2.20)$$

где u_i – мера ущерба в i-ой компоненте;

$\varphi_i u_i$ – плотность вероятности наступления ущерба u_i;

n – количество компонентов системы.

В случае использования экспоненциального семейства распределений последнее выражение примет вид:

$$Risk_{\Sigma} = \left(\sum_{i=1}^{n} u_i\right) \prod_{i=1}^{n} \frac{A_i(u_i)}{\exp[B_i(u_i)]} =$$

$$= \left(\sum_{i=1}^{n} u_i\right) \frac{\prod_{i=1}^{n} A_i(u_i)}{\exp[\sum_{i=1}^{n} B_i(u_i)]}, \qquad (2.21)$$

где A_i и B_i– функции ущерба i-ого компонента, определенные на основе соответствующего типа регулярного распределения экспоненциального семейства.

Данное выражение может быть конкретизировано, если законы распределения для ущербов в компонентах однотипны (имеют общие выражения) и отличаются друг от друга лишь параметрически. Такое в принципе возможно при однотипности компонентов, различающихся только настройкой на свою задачу. В этом случае, к примеру, для экспоненциального распределения имеем выражение для общего риска системы:

$$Risk_{\Sigma} = \left(\sum_{i=1}^{n} u_i\right) \frac{\prod_{i=1}^{n} \lambda_i}{\exp[\sum_{i=1}^{n} \lambda_i(u_i)]}, \qquad (2.22)$$

где λ_i – параметр распределения плотности вероятности наступления ущерба в i-ой компоненте.

После получения выражений остается открытым вопрос о том, какие значения u_i следует принимать во внимание. Здесь возможны по крайней мере два варианта: пиковая и средняя оценка.

При пиковой оценке используются координаты максимума риска (R_{max}, u_0^*) и общее выражение будет

выглядеть следующим образом:

$$Risk_{\Sigma}^{(max)} = \left(\sum_{i=1}^{n} u_{0i}^{*}\right) \prod_{i=1}^{n} \frac{R_{\max i}}{u_{0i}^{*}}, \qquad (2.23)$$

где $R_{\max i}$ - значение максимума риска в i-ой компоненте системы;

u_{0i}^{*} – значение ущерба, при котором имеет место быть пик риска в i–ой компоненте системы, т.е. мода риска.

Алгоритм расчета общего риска в данном случае должен предусматривать прежде всего ввод данных о виде и параметрах распределений плотности вероятности наступления ущерба в каждой из компонент распределенной системы. Далее необходимо определить (в зависимости от вида распределения) координаты пика для всех компонентов системы. Полученные данные в результате следует использовать для расчета общего риска. Блок-схема данного алгоритма представлена на рис. 2.4.

При использовании усредненных оценок в компонентах общий риск системы можно рассчитать с помощью выражения:

$$Risk_{\Sigma}^{(\text{ср})} = \left(\sum_{i=1}^{n} M_i\right) \prod_{i=1}^{n} \varphi_i(M_i). \qquad (2.24)$$

В случае однотипных распределений плотности вероятности наступления ущерба в компонентах последнее выражение может быть конкретизировано.

Алгоритм расчета общего риска системы при усредненных оценках риска в ее компонентах прежде всего включает ввод данных о виде параметрах распределения плотности вероятности наступления ущерба в компоненте. Далее находятся координаты среднего значения для ущерба в данной компоненте. Блок-схема данного алгоритма изображена на рис. 2.5.

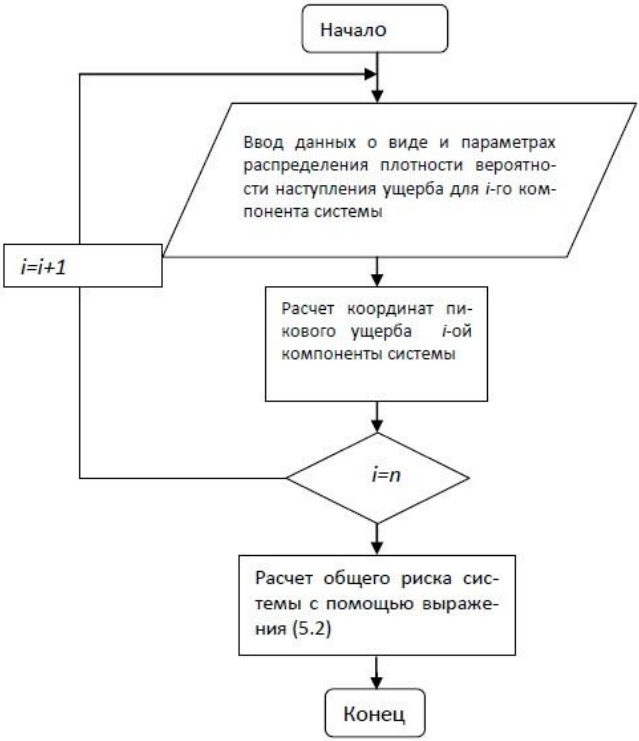

Рис. 2.4. Алгоритм расчета общего риска системы на основе пиковых оценок риска в её компонентах

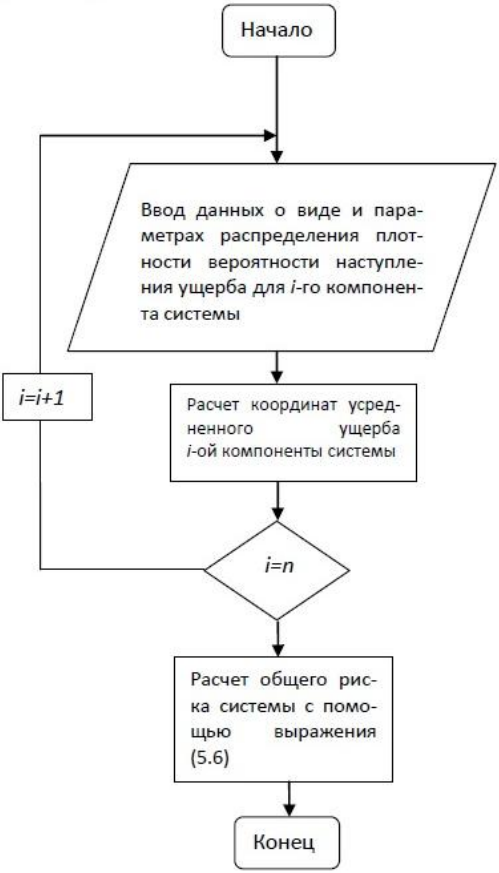

Рис. 2.5. Алгоритм расчёта общего риска системы на основе усредненных оценок риска в её компонентах

2.4. Методология оценки эффективности систем в условиях атак

Детерминированный подход в предсказании поведения систем имеет множество ограничений, что собственно и обусловило применение аппарата теорий вероятности и нечеткости, которые фактически пытаются оценить возможности выпадения тех или иных значений недетерминированных переменных. Поэтому введено понятие «возможность» как некоторый

обобщающий термин для описания шанса (возможность получения пользы) и риска (возможность наступления ущерба). При этом введена функция возможности как аналитической форма, необходимая для определения мер риска и шанса, а также для прогнозной оценки параметров эффективности систем.

Функция возможности может быть $Pos(x)$ определена на множестве значений случайной величины$X = \{0, x_1, \dots, x_i, \dots, x_n\}$, причем $0 \leq Pos(x) \leq 1$и возможен инвариант, когда:

$$\sum_i Pos(x_i) = const. \quad (2.25)$$

Функция возможности Pos может быть задана различными способами:

– исходя из статистической частоты выпадения различных значений случайной величины;

– путем аппроксимации вышеуказанных статданных с помощью некоторого аналитического закона распределения вероятности;

– непосредственным аналитическим заданием закона распределения для типового случая;

– посредством нечетких чисел и экспертных оценок;

– а также другими комбинированными способами.

Функция возможности фактически является некоторым обобщением, необходимым для формализации понятий шанса и риска систем.

Будем исходить из того, что случайная переменная может носить для системы как позитивный, так и негативный характер:

$x = v$ – польза;

$x = u$ – ущерб.

Отсюда представляется возможным задать:

$$Chs(v_i) = v_i * Pos(v_i); \quad (2.26)$$

$$Risk(u_i) = u_i * Pos(u_i). \quad (2.27)$$

Рассматривая их фактически как парную оценку возможности наступления пользы величиной v_i и ущерба величиной u_i. Оператор (*) зачастую представляет собой алгебраическое произведение, однако не факт, что это

единственно возможное определение (измерение) шанса и риска. Такая форма удобна и поэтому в дальнейших выкладках уместно пользоваться именно ей.

Интегрально шанс и риск можно оценить усреднением. Для случая применения вероятностной модели это чаще всего матождание:

$$m_v = \frac{\int_0^\infty v\varphi(v)dv}{\int_0^\infty \varphi(v)dv}; \tag{2.27}$$

$$m_u = \frac{\int_0^\infty u\varphi(u)du}{\int_0^\infty \varphi(u)du}. \tag{2.28}$$

С другой стороны можно оценить разброс (среднеквадратичное отклонение) шанса и риска от их средних значений:

$$\sigma_v \frac{\sqrt{\int_0^\infty (m_v - v)^2\varphi(v)dv}}{\int_0^\infty \varphi(v)dv}; \tag{2.29}$$

$$\sigma_u \frac{\sqrt{\int_0^\infty (m_u - u)^2\varphi(u)du}}{\int_0^\infty \varphi(u)du}. \tag{2.30}$$

Знаменатели вышеуказанных выражений могут не быть инвариантами за счет нормирования и ограничения по максимально допустимым значениям пользы v_{max} и ущерба u_{max}. Значения v_{max} и u_{max} соответствуют границам, за которыми система переходит в качественно иное состояние.

Возможна также и синтетическая мера:

$$Chs(v) = m_v + \beta\sigma_v; \tag{2.31}$$

$$Risk(u) = m_u + \beta\sigma_u. \tag{2.32}$$

К примеру, возможно значение $\beta = \pm 1$.

Существуют другие прогнозные оценки. Так, исходя из мер риска и шанса, ожидаемая эффективность системы может быть найдена следующим образом:

$$Э = \frac{(m_v - m_u) + \beta(\sigma_v - \sigma_u)}{z} - 1, \tag{2.33}$$

где z- суммарные затраты системы на обеспечение ее функций и безопасности.

Последнее выражение исходит из того, что ущерб и польза имеют одинаковые размерности. Аналогично можно спрогнозировать эффективность системы на основе других мер риска и шанса.

Практический интерес также представляют ряд других параметров систем. Например, коэффициент полезности и коэффициент ущербности:

$$K_v = \frac{\int_0^\infty v\varphi(v)dv}{\int_0^\infty v[1-\varphi(v)]dv}; \quad (2.34)$$

$$K_u = \frac{\int_0^\infty u\varphi(u)du}{\int_0^\infty u[1-\varphi(u)]du}, \quad (2.35)$$

Полученные аналитические выражения могут послужить методической основой для оценки и прогнозирования параметров систем различного назначения, в том числе распределенных систем. С использованием вышеуказанного аппарата рассмотрим:

– возможные модели распределенных систем, подвергающихся воздействию угроз;

– атаки на компоненты распределенных систем;

– прогнозирование эффективности противодействия атакам в распределенных системах.

При этом, для иллюстрации методологии используем вероятности как частный случай оценки возможности.

Постараемся привести примеры оценки эффективности реальных распределенных систем.

Современные распределенные системы (РС) обречены существовать в условиях постоянно реализуемых в отношении них операций и атак кибернетического характера. Противо--действие информационным атакам (ИА), организуемое в РС, нуждается в регулярной оценке его эффективности. Однако методология этой оценки обычно слишком обща и требует разработки более инженерного подхода, удобного для практического применения. Определенные перспективы в этом

направлении открывает использование теории вероятности и математической статистики.

Допустим, что для распределенной системы существует статистика частоты наступления ущербов, наносимых деструктивными информационными атаками. При этом, вышеуказанная статистика позволяет описать данный случайный процесс с помощью законов распределения возможности $\varphi(u)$ или плотности вероятности $\varphi(u)$ ущерба *и.* Тогда представляется возможным (на некотором временном интервале наблюдения РС) определить матожидание m_uи дисперсию σ^2 ущерба:

$$m_u = \frac{\int_0^\infty u\varphi(u)du}{\int_0^\infty \varphi(u)du}; \qquad (2.36)$$

$$\sigma_u^2 = \int_0^\infty (m_u - u)^2\varphi(u)du. \qquad (2.37)$$

Предположим, что ресурс системы *R,* которому нанесен ущерб, сам ущерб и затраты Z на противодействие ИА определены в единой размерности. Тогда в абсолютных единицах эффективность противодействия ИА в РС предлагается оценить следующим образом:

$$Э = R - (m_u + \beta\sigma_u) - Z. \qquad (2.38)$$

Соответственно в относительных единицах данная эффективность может быть оценена выражением:

$$\overline{Э} = \frac{R - (m_u + \beta\sigma_u)}{z} - 1. \qquad (2.39)$$

Однако подобный подход не учитывает временную динамику процесса. Поэтому введем следующие обозначения:

Z_0- стартовые (капитальные) затраты на противодействие ИА в РС в момент времени t_0;

z - усредненные текущие затраты на противодействие в интервале времени ;

k - номер временного интервала наблюдения системы;

$m_u(t_0 + k\tau)$- матожидание ущерба на *k-ом* интервале наблюдения системы;

$\sigma_u(t_0 + k\tau)$- СКО ущерба на k-ом интервале наблюдения системы;

R_0- стартовое состояние атакуемого ресурса системы в момент времени t_0;

r - усредненное текущее восстановление (развитие) атакуемого ресурса в интервале времени ;

n - количество интервалов априорного наблюдения.

С учетом данных обозначений на интервале *(n+1)* с некоторой точностью (она будет определяться величиной *n)* представляется возможным спрогнозировать эффективность противодействия с помощью следующего выражения:

$$\overline{Э}[t_0 + (n+1)\tau] = \\ = \frac{[R_0 + (n+1)r]\sum_{k=1}^{n+1}[m_u(t_0 + k\tau) + \beta\sigma_u(t_0 + k\tau)]}{Z_0 + (n+1)z} - 1, \quad (2.40)$$

В данном случае $m_u[t_0 + (n+1)\tau]$ и $\sigma_u[t_0 + (n+1)\tau]$ являются продуктами экстраполяции значений матожидания и СКО ущерба. Предсказание вполне применимо в отношении сравнительно монотонных процессов. В его основе используются как относительно детерминированные переменные, так и числовые характеристики случайной переменной (ущерба), неизбежно присутствующей при реализации деструктивных ИА в отношении РС. При этом точность предсказания будет определяться объемом интервалов *n.*

В случае, когда изменения матожидания и СКО несущественны при переходе от одного интервала к другому, последнее выражение может быть упрощено:

$$\overline{Э}[t_0 + (n+1)\tau] = \\ = \frac{[R_0 + (n+1)r] - (n+1)[m_u + \beta\sigma_u]}{Z_0 + (n+1)z} - 1. \quad (2.41)$$

На основе полученных выражений попытаемся провести некоторую алгоритмизацию процесса предсказания эффективности противодействия (рис. 2.6). Здесь очевидно вырисовываются три блока вычислений:

- расчёт атакуемого ресурса $[R_0 + (n+1)r]$;
- расчёт ущерба ресурса $(n+1)[m_u + \beta\sigma_u]$;
- расчёт затрат на противодействие $Z_0 + (n+1)z$.

При этом, очевидно, необходим цикл наращивания

интервалов наблюдения $k=k+1$ и блок экстраполяции эффективности на основе выражений.

Рис. 2.6. Алгоритм прогнозирования эффективности противодействия в атакуемой системе

Распределенная система в наиболее общем виде представляет собой связь элементов множества компонентов (узлов).

$$S = S(X), \qquad (2.42)$$

где $X = \{X_1, \dots, X_k, \dots, X_n\}$– множество узлов, концентрирующих информацию и т. п.

Исходя из вышеуказанного, может быть построена

соответствующая модель, которая в условиях противоборства учитывает атакующие РС деструктивные (негативные) факторы $D = \{d_1, \dots, d_i, \dots, d_n\}$ и защищающие РС конструктивные (позитивные) факторы $C = \{c_1, \dots, c_i, \dots, c_m\}$. Всевозможные взаимодействия факторов в отношении узлов S иллюстрирует трехмерный тензор. Для него имеет место набор шанса и риска.

$$Chs(x_k, c_{j,} d_i), Risk(x_k, c_j, d_i).$$

Сечение трехмерного тензора представляет собой двумерные тензоры. Так для сечения по узлу может быть предложена оценка эффективности:

$$\overline{Э_{x_k}} = \frac{\sum_{ij} Chs(x_k, c_{j,} d_i) - \sum_{ij} Risk(x_k, c_j, d_i)}{Z(x_k)} - 1, \qquad (2.43)$$

где $Z(x_k)$ – суммарные затраты по формированию и обеспечению функционирования узла x_k.

По аналогии для другого сечения можно оценить эффективность средства защиты c_j по отношению множеству узлов:

$$\overline{Э_{c_j/X}} = \frac{\sum_{ik} Chs(x_k, c_{j,} d_i) - \sum_{ik} Risk(x_k, c_j, d_i)}{\sum_k Z(x_k)} - 1. \quad (2.44)$$

В свою очередь опасность для множества X средства атаки d_i, может быть оценена так:

$$\overline{Э_{d_i/X}} = \frac{\sum_{jk} Chs(x_k, c_{j,} d_i) - \sum_{jk} Risk(x_k, c_j, d_i)}{\sum_k Z(x_k)} - 1. \quad (2.45)$$

Интересны также интегральные оценки эффективности. Попытаемся сделать их в следующем виде для множества узлов системы:

$$\overline{Э_X} = \frac{\sum_{jk} Chs(x_k, c_{j,} d_i) - \sum_{jk} Risk(x_k, c_j, d_i)}{\sum_k Z(x_k)} - 1. \qquad (2.46)$$

Очевидно, в данном случае не рассматриваются отдельные сечения, а анализируются соответствующие соотношения для всего множества узлов-компонентов РС. Последнее выражение вполне согласуется с алгоритмом (рис. 6) и также может быть положено в его основу для решения соответствующих задач.

Полученные выражения очевидно являются статистическими и прогностическими оценками, предполагающими:

– отсутствие зависимости между рассматриваемыми факторами;

– наличие статистики по рискам и шансам для всех компонент анализируемой распределенной системы;

– исходные данные являются приемлемой основой для предсказания параметров, в т. ч. эффективности.

Рассмотрим прогнозирование динамики эффективности системы при переходе из одного состояния в другое. При этом будем исходить из того, что анализируемый процесс носит стационарный характер и предыстория системы (статистика полезности и ущербности, лежащая в основе определения ее шансов и рисков) позволяет уверенно предсказывать ее поведение, в том числе для важнейшего параметра Э- эффективности. Такой подход особенно актуален при оценке безопасности и устойчивости развития систем различных классов и разнообразного назначения, включая информационные системы.

Воспользуемся предлагаемой в оценкой эффективности системы, основанной на триаде «шанс, риск, затраты». В этом случае для системы, переходящей из состояния 1 к состоянию 2 уместно предложить следующие оценки ее эффективности в моменты времени t1 (состояние 1) и t2 (состояние 2):

$$\overline{Э}(t_1) = \frac{Chs(v, t_1) - Risk(u, t_1)}{Z(t_1)} - 1;$$

$$\overline{Э}(t_2) = \frac{Chs(v, t_2) - Risk(u, t_2)}{Z(t_2)} - 1,$$

где Chs – шанс получения пользы v соответственно в моменты времени t1 и t2;

Risk – риск возникновения ущерба u соответственно в моменты времени t1 и t2;

Z – затраты, которые понесла система соответственно к моментам времени t1 и t2;

t1 > t2.

Изменение (не обязательно позитивное) эффективности системы при переходе из состояния 1 в состояние 2, очевидно, составит:

$$\Delta\overline{Э} = \overline{Э}(t_2) - \overline{Э}(t_1),$$

или

$$\Delta\overline{Э} = \frac{Chs(v,t_2) - Risk(u,t_2)}{Z(t_2)} - \frac{Chs(v,t_1) - Risk(u,t_1)}{Z(t_1)}.$$

В случае незначительности переходных затрат:

$$Z(t_1) \cong Z(t_2) = Z; \quad (2.47)$$

$$Z = Z(t_2) - Z(t_1) \to 0; \quad (2.48)$$

$$\Delta\overline{Э} = \frac{\Delta Chs - \Delta Risk}{Z}, \quad (2.49)$$

где $\Delta Chs = Chs(v,t_2) - Chs(v,t_1)$;

$\Delta Risk = Risk(u,t_2) - Risk(u,t_1)$.

С учетом нормирования последнее выражение можно интерпретировать следующим образом:

$$Chs(v,t) = v_{max}Chs(\bar{v},t); \quad (2.50)$$

$$Risk(u,t) = u_{max}Chs(\bar{u},t), \quad (2.51)$$

где v_{max} – максимально допустимое (в данном качестве системы) значение пользы;

u_{max} - максимально допустимое (в данном качестве системы) значение ущерба;

$\bar{v}$ – нормированное по v_{max} текущее значение пользы;

$\bar{u}$ – нормированное по u_{max} текущее значение ущебра;

t – текущее время.

Задавая изменение затрат ΔZ, шанса ΔChs и риска $\Delta Risk$, при переходе системы из состояния 1 в состояние 2, получаем выражение для измерения ее эффективности:

$$\overline{Э} = \frac{(Chs + \Delta Chs) - (Risk - \Delta Risk)}{Z + \Delta Z} - \frac{Chs - Risk}{Z} =$$

$$= \frac{Zchs + Z\Delta Chs - ZRisk - Z\Delta Risk - ZChs + ZRisk - \Delta ZChs + \Delta ZRisk}{(Z + \Delta Z)Z} =$$

$$= \frac{Z\Delta Chs - Z\Delta Risk - \Delta ZChs + \Delta ZRisk}{(Z + \Delta Z)Z} =$$

$$= \frac{(\Delta Chs - \Delta Risk) - \frac{\Delta Z}{Z}(Chs + Risk)}{Z + \Delta Z} =$$

$$= \frac{\frac{\left(\frac{\Delta Z}{Z}\right)(\Delta Chs - \Delta Risk)}{\Delta Z} - \frac{\left(\frac{\Delta Z}{Z}\right)(\Delta Chs + \Delta Risk)}{Z}}{1 + \frac{\Delta Z}{Z}}. \quad (2.52)$$

С учётом следующих обозначений:

$CR/_Z = \frac{Chs-Risk}{Z}$ – относительный шансориск;

$\Delta CR/_Z = \frac{C\Delta hs-\Delta Risk}{Z}$ – прирост относительного шансориска;

$K_Z = \frac{\Delta Z/_Z}{1+\Delta Z/_Z}$ – коэффициент динамики затрат, последнее выражение можно записать следующим образом:

$$\overline{Э} = K_Z\left(\frac{\Delta CR}{Z} - \frac{CR}{Z}\right). \quad (2.53)$$

Соответствующий алгоритм представлен на рис. 2.7.

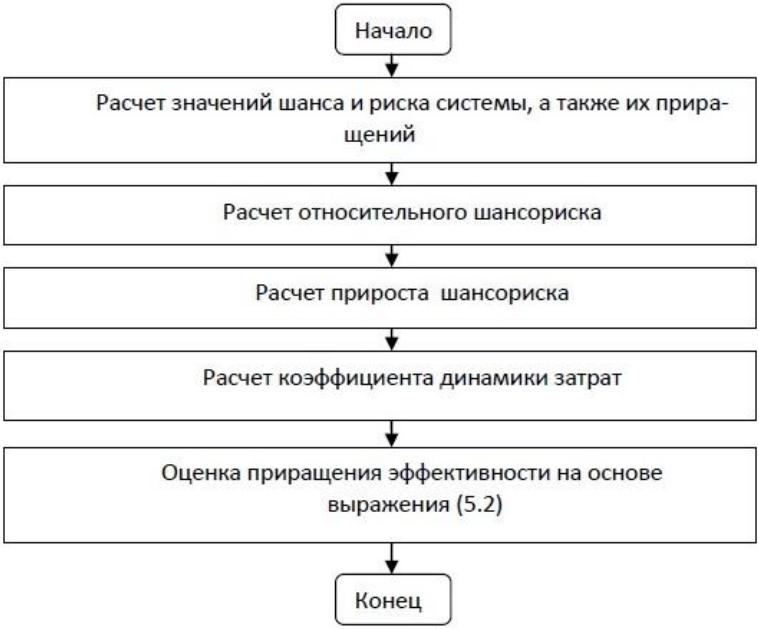

Рис. 2.7. Алгоритм оценки динамики эффективности системы

Положительное изменение (прирост) эффективности возможно при условии, когда:

$$\frac{\Delta CR}{Z} > \frac{CR}{Z} \text{ или } \frac{\Delta Chs-\Delta Risk}{\Delta Z} > \frac{Chs-Risk}{Z}.$$

Отсюда условие роста эффективности может быть представлено следующим выражением:

$$\frac{\Delta Chs - \Delta Risk}{Chs - Risk} > \frac{\Delta Z}{Z}. \quad (2.53)$$

Иными словами, динамика шансориска должна превышать динамику затрат при переходе системы из одного состояния в другое.

Характерно отметить, что представленное выше условие уверенно коррелируют с таким практическими случаями, как атака системы извне ($\Delta Z \to 0$).

Здесь:

$$\overline{Э} = K_Z\left(\frac{\Delta CR}{Z} - \frac{CR}{Z}\right), K_Z * \frac{CR}{Z} \to 0. \quad (2.54)$$

В ракурсе информационных систем полученные соотношения применимы для оценки уничтоженной или вбрасываемой в результате атаки информации. Изменение шансориска открывает здесь возможность оценить вредоносность или полезность данной информации для атакуемой системы. Предложенные аналитические выражения послужат удобной методической базой для описания динамики эффективности РС.

2.5. Управление рисками систем

В случае реализации синхронной атаки на компоненты системы риск может быть оценен следующим образом:

$$\mathrm{Risk}_{\sum} = \left(\sum_{i=1}^{n} u_i\right)\prod_{i=1}^{n} \varphi_i\,(u_i), \quad (2.55)$$

где u_i - ожидаемый ущерб в i-ой компоненте при реализации атаки;

$\varphi_i(u_i)$ - значение плотности вероятности наступления ущерба u_i;

n – количество компонентов системы.

Однако данная характеристика носит усредненный (нормированный) вид. Поэтому с учетом ценности обрабатываемой информации (или другого ресурса) в компоненте системы последнее выражение следует переписать следующим образом:

$$\mathrm{Risk}_{\Sigma}^{(CA)} = \left(\sum_{i=1}^{n} u_i c_i\right) \prod_{i=1}^{n} \varphi_i(u_i), \qquad (2.56)$$

где c_i – ценность ресурса (информации и т.п.) i-ого компонента;

$$\sum_{i=1}^{n} c_i = C. \qquad (2.57)$$

Фактически c_i задает масштаб характеристики риска. Таким образом, представляется возможность управления риском путем перераспределения ценности ресурса между ее компонентами. Одним из таких способов, способствующих снижению общего риска, является уравнивание ущербов, возникающих в ее компонентах. Его уместно применять при синхронных атаках. Здесь для выражения может быть предложено распределение ценности:

$$c_i = \frac{c \sum_{i=1}^{n} u_i}{n^2 u_i}, \qquad (2.58)$$

где наблюдается обратная пропорция между c_i и u_i, т.е. в компоненты с повышенным возможным ущербом направляется ресурс с минимальной ценностью. В результате общий риск равен:

$$\mathrm{Risk}_{\Sigma}^{(CA)} = \left(\frac{c \sum_{i=1}^{n} u_i}{n}\right). \qquad (2.59)$$

При этом, в выражении в качестве u_i могут быть использованы как усредненные, так и пиковые оценки.

При асинхронных атаках общий риск может быть оценен следующим выражением:

$$\mathrm{Risk}_{\Sigma}^{(AA)} = \left(\sum_{i=1}^{n} u_i c_i\right) \prod_{i=1}^{n} \varphi_i(u_i), \qquad (2.60)$$

В данном случае уместно реализовать уравнение рисков в компонентах. К примеру, для пиковой оценки при логнормальном законе распределения плотности вероятности наступления ущерба в компонентах можно записать:

$$\mathrm{Risk}_{\Sigma}^{(AA)} = \left(\sum_{i=1}^{n} \frac{c_i}{\sigma_{i\sqrt{2\pi}}}\right), \quad (2.61)$$

где σ_i – дисперсия ущерба в i-ой компоненте системы.

Отсюда можно предложить соотношение:

$$c_i = \sigma_i \frac{c}{\sum_{i=1}^{n} \sigma_i}, \quad (2.62)$$

позволяющее уравнять риски в компонентах и получить следующее значение общего риска

$$\mathrm{Risk}_{\Sigma}^{(AA_{max})} = \left(\frac{nc}{\sqrt{2\pi}\sum_{i=1}^{n} \sigma_i}\right), \quad (2.63)$$

Последнее выражение демонстрирует способ уравнивания рисков для асинхронных атак на компоненты системы. Выше указанные способы регулирования рисков могут быть формализованы с помощью алгоритма, представленного на рис. 2.8.

В процессе управления (регулирования) очень важно интегрально оценить (синхронизировать) ресурсную динамику системы через изменения ресурсов ее компонентов.

Рассмотрим систему, состоящую из m компонентов. При этом, в РС по всем компонентам распределены задачи (операторы) $F=\{F_1,\ldots, F_i,\ldots F_m\}$ и ресурсы $R=\{r_1,\ldots, r_i,\ldots r_m\}$.

Положим, что для каждого компонента известны меры риска (Riski) и шанса (Chsi) для выполнения оператора F_i. Отсюда в простейшей оценке шансориска имеем итоговый ресурс i-го компонента.

$$r_i' = r_i - m_{ui} + m_{vi}, \quad (2.64)$$

или в целом для системы

$$R' = \sum_{i} k_i r_i', \quad (2.65)$$

где R_i – мера чувствительности компонента;

m_{ui} и m_{vi} – мера риска и шанса.

Рис. 2.8. Блок-схема алгоритма управления риском системы на основе уравнивания ущербов и рисков в ее компонентах

Мера чувствительности i-го элемента системы представляется возможным определить с помощью следующего выражения

$$k_i = \frac{P(F, \overline{\overline{r_i}}) - P(F, r_i)}{1 - P(F, r_i)}, \qquad (2.66)$$

где $P(F, \overline{r_i})$ – вероятность реализации оператора F при отсутствии ресурса r_i i-го элемента системы;

$P(F,r_i)$ – вероятность реализации оператора F при наличии ресурса r_i i-го элемента системы.

Такой подход уместен для распределения ресурса в ходе администрирования системы с учетом возможного выхода из

строя атакуемой компоненты.

Выше приведенные рассуждения относятся к управлению на макроуровне, где фактически выделяются два подмножества (синхронно и асинхронно) атакуемых компонентов системы, между которыми осуществляется соответствующее перераспределение ресурса.

Вместе с тем, представляется возможность регулирования общего риска на макроуровне, т.е. уровне компонентов системы. Для пояснения рассмотрим характеристику общего риска для случая, когда система состоит из трех компонентов. Очевидно, что управляя положением экстремумов и разбросом для риска каждой из компонент, можно регулировать как неравномерность, так и полосу П общей характеристики.

Аналитически этот способ можно пояснить на примере логнормального распределения плотности вероятности наступления ущерба в компоненте системы, где для асинхронных атак общий риск определяется следующим выражением

$$\mathrm{Risk}_{\Sigma}^{(AA)} = \left(\sum_{i=1}^{n} \frac{1}{\sigma_{i\sqrt{2\pi}}} \exp\left[-\frac{(\ln u - \ln m_i)^2}{2\sigma_i^2} \right] \right), \quad (2.67)$$

где m_i и σ_i – параметры распределения в i–ой компоненте.

Вышеприведенные регулировки достигаются соответствующей настройкой средств защиты, применяемых в компонентах системы. В этом отношении может быть осуществлена соответствующая алгоритмизация процесса.

3. РЕКОМНЕДУЕМЫЙ ИНСТРУМЕНТАРИЙ ПРОГНОЗИРОВАНИЯ РИСКОВ, ЖИЗНЕСТОЙКОСТИ И ЭФФЕКТИВНОСТИ ЗАЩИТЫ

3.1. Основные виды функций полезности

Зачастую при проведении риск-анализа ставится задача определения возможной пользы и возможного ущерба в результате реализации некоторых атак.

В данном контексте исследование уместно проводить не относительно времени, а относительно некоторой переменной состояния, которая характеризует работу исследуемого объекта. Задавать такую переменную состояний следует специальной функций полезности.

Можно выделить два вида функций полезности:

– показательная функция полезности (3.1);

– экспоненциальная функция полезности (3.2).

Показательная функция полезности имеет вид:

$$w(x) = \sqrt[\alpha_в]{\frac{x}{X_{ср}}}\left[1 - \left(\frac{x}{X_{ср}}\right)^{\alpha_з}\right], \qquad (3.1)$$

где x – исследуемая переменная состояния;

$X_{ср}$ – среднее значение переменной состояния в момент отказа исследуемого объекта;

$\alpha_в > 1, \alpha_з > 1$ – коэффициенты нелинейности, задающие крутизну «восхода» и «заката» соответственно.

Экспоненциальная функция полезности имеет вид:

$$w(x) = \left\{1 - \exp\left[-\left(\frac{x}{\tau_в}\right)\right]\right\} \exp\left[-\left(\frac{x}{\tau_з}\right)\right], \qquad (3.2)$$

где x – исследуемая переменная состояния;

$\tau_в$, $\tau_з$ – положение «бровки» для периодов «восхода» и «заката» жизненного цикла рассматриваемого объекта.

Выбор функции полезности следует осуществлять в зависимости от параметров функционирования исследуемого объекта.

Стоит отметить, что на практике приходится зачастую вводить некоторые упрощения кривой полезности.

Можно выделить три основных вида упрощения кривой полезности:

– трапецевидное упрощение (рис. 3.1);
– прямоугольное упрощение (рис. 3.2);
– треугольное упрощение (рис. 3.3).

Трапецевидное упрощение следует применять, в тех случаях когда величина вероятных «восходов» и «закатов» не может быть установлена точно. Данное упрощение позволяет провести достаточно точный анализ кривой полезности, но всё же не такой точный как в случае, когда величина «восходов» и «закатов».

На рис. 3.1 легко заметить, что данное упрощение позволяет проводить анализ с данными максимально приближенными к реальным.

Рис. 3.1. Трапецевидное упрощение

Прямоугольное упрощение следует применять в случаях, когда даже примерные величины вероятных «восходов» и «закатов» неизвестны. Такое упрощение носит достаточно сильный характер и его применение необходимо лишь в случаях, когда получить достоверные сведения не представляется возможным.

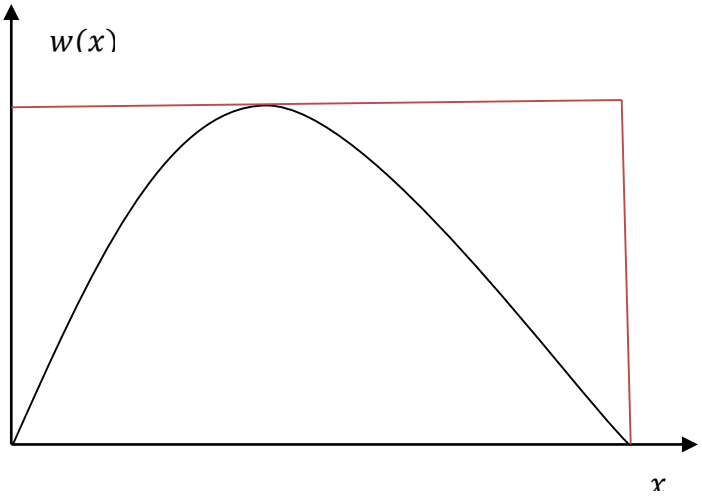

Рис. 3.2. Прямоугольное упрощение

Треугольное упрощение (рис. 3.3) следует применять в случаях, когда известно, что функция полезности имеет примерно равные величины «восходов» и «закатов», а также в случаях когда известна лишь одна из величин. Позволяет получить достаточно точные значения.

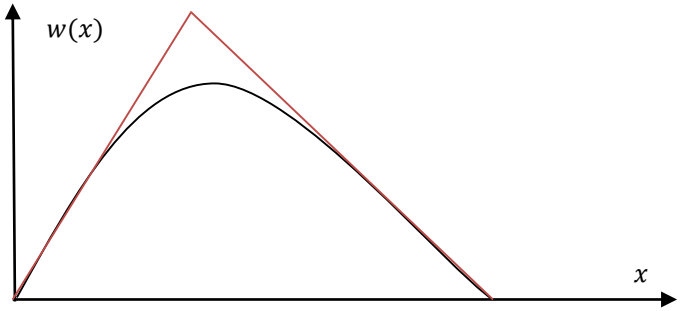

Рис. 3.3. Треугольное упрощение

Очевидно, что данные упрощения применимы только в случаях когда требуется проведение экспресс-анализа.

3.2. Аналитические выражения пользы и ущерба

При рассмотрении функции полезности можно заметить, что аналитические выражения пользы и ущерба легко находятся интегрированием функций полезности (3.1), (3.2).

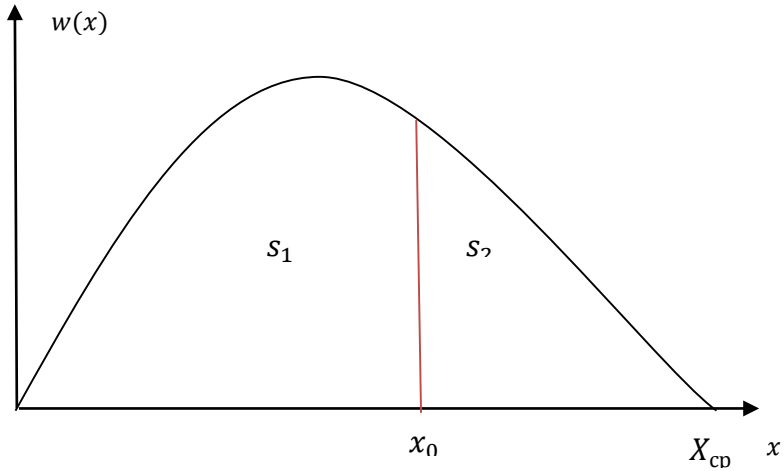

Рис. 3.4. Интегрирование функции полезности

Из рис. 3.4 очевидно, что площадь фигуры S_1 есть ни что иное как ожидаемая польза, а соответственно S_2 – ущерб.

Соответственно аналитические выражения для пользы ущерба будут иметь вид (3.3) и (3.4):

$$u(x) = \int_0^{x_0} w(x)dx; \quad (3.4)$$

$$v(x) = \int_{x_0}^{X_{\text{ср}}} w(x)dx. \quad (3.4)$$

В зависимости от выбранной функции полезности проинтегрировав выражения (3.3), (3.4) можно найти соответствующие значения пользы и ущерба.

Соответствующее аналитические выражения риска и шанса можно определить следующим образом:

$$Risk(x_0) = \frac{u(x_0)f(x_0)}{k \cdot f_{max}}; \quad (3.5)$$

$$Chance(x_0) = v(x_0) \cdot [1 - F(x_0)], \quad (3.6)$$

где x_0 – значение переменной состояния в момент ожидаемого отказа;

$f(x_0)$ – плотность вероятности;

f_{max} – пик плотности вероятности;

k – степень дискретизации;

$u(x_0)$ – ожидаемый ущерб;

$v(x_0)$ – ожидаемая польза.

3.3. Общие сведения о жизнестойкости

Жизнестойкость следует рассматривать как величину обратную вероятности фатальной атаки на объект, представленную в логарифмическом масштабе.

Отсюда область определения этого параметра составит:

$$0 \leq L_f \leq +\infty$$

Исходя из выше сказанного можно определить как:

$$L_f = \frac{f(x_0)dx}{1-F(x_0)}, \quad (3.7)$$

где x_0 – значение переменной состояния в момент отказа;

$f(x_0)$ – плотность вероятности для выбранного закона распределения;

$F(x_0)$ – накопленная вероятность.

Очевидно, что на практике применяются несколько иные оценки жизнестойкости.

Выделяют два вида оценки жизнестойкости:

- мгновенная жизнестойкость;
- интервальная жизнестойкость.

Мгновенная жизнестойкость

При выполнении работы по риск-анализу зачастую бывает необходимо получить мгновенное значение жизнестойкости с целью определения свойств объекта в конкретный момент времени.

Соответствующее аналитическое выражение для мгновенной жизнестойкости будет иметь вид (3.8):

$$L_f(x_0) = \ln\left(\frac{1 - F(x_0)}{f(x_0)(\Delta x)}\right), \quad (3.8)$$

где x_0 – значение переменной состояния в момент отказа;

$f(x_0)$ – плотность вероятности для выбранного закона распределения;

$F(x_0)$ – накопленная вероятность;

Δx – шаг дискретизации.

Интервальная жизнестойкость

Интервальную жизнестойкость следует рассматривать как жизнестойкость в промежутке времени $x_0 \leq x \leq X_{\text{ср}}$ (в общем случае $x_1 \leq x \leq x_2$) (3.9).

Соответствующую оценку интервальной жизнестойкости следует представить в виде:

$$L_f\left(x_0, X_{\text{ср}}\right) = \ln\left(\frac{1 - F(x_0)}{F\left(X_{\text{ср}}\right) - F(x_0)}\right). \quad (3.9)$$

В случае если оценку жизнестойкости необходимо провести не на конечном периоде функционирования исследуемого объекта, то выражение интервальной жизнестойкости примет вид (3.10):

$$L_f(x_1, x_2) = \ln\left(\frac{1 - F(x_1)}{F(x_2) - F(x_1)}\right). \quad (3.10)$$

где x_1, x_2 – некоторый период функционирования системы.

Данная оценка может проводится в целях анализа возможный последствий на периодах функционирования объекта отличных от конечного.

3.4. Анализ ожидаемой эффективности защиты атакуемого объекта

Эффективность ожидаемой защиты представляет собой отношения к шанса успешной защиты к вероятности отказа.

Как и в случае с живучестью ожидаемую эффективность

защиты уместно рассматривать в случае когда требуется мгновенная эффективность и в случае когда требуется эффективность за некоторый период функционирования.

Мгновенную эффективность можно представить в виде (3.11):

$$E_f(x_0) = \frac{1 - F(x_0)}{f(x_0)(\Delta x)} \cdot \frac{v(x_0)}{u(x_0)}, \qquad (3.11)$$

где x_0 - значение переменной состояния в момент отказа;

$f(x_0)$ – плотность вероятности;

$F(x_0)$ – накопленная вероятность;

Δx – шаг дискретизации;

$v(x_0)$ – ожидаемая польза;

$u(x_0)$ – ожидаемый ущерб.

Несложно заметить, что данное выражение приводимо к виду:

$$E_f(x_0) = \frac{Chance(x_0)}{Risk(x_0)}, \qquad (3.12)$$

где $Chance(x_0)$ – шанс успешного функционирования со значением переменной состояния x_0.

$Risk(x_0)$ – риск отказа со значением переменной состояния x_0.

Интервальная же оценка эффективности ожидаемой защиты представляется выражением (3.13):

$$\boldsymbol{E_f(x_0, X_{\text{ср}}) = \frac{1 - F(x_0 + x_r)}{f(x_0 + x_r)(\Delta x)} \cdot \frac{v(x_0, x_r)}{u(x_0, x_r)}}, \qquad \boldsymbol{(3.13)}$$

где x_0 - значение переменной состояния в момент отказа;

$x_r = \frac{\int_{x_0}^{X_{\text{ср}}}(x - x_0)f(x)dx}{1 - F(x_0)}$ – ожидаемое среднее успешного функционирования атакуемого объекта;

$f(x_0 + x_r)$ – плотность вероятности;

$F(x_0 + x_r)$ – накопленная вероятность;

Δx – шаг дискретизации;

$v(x_0 + x_r) = \int_0^{x_0 + x_r} w(x)dx = \frac{1}{n}\sum_{i=k+1}^{r} w(\frac{i}{n})$ – ожидаемая польза;

$u(x_0 + x_r) = \int_{x_0 + x_r}^{X_{\text{ср}}} w(x)dx = \frac{1}{n}\sum_{j=r+1}^{n} w(\frac{j}{n})$ – ожидаемый ущерб.

Значения вышеперечисленных параметров можно получить только с учётом дискретизации.

Для правильного выбора шага дискретизации следует воспользоваться теоремой Котельникова.

Дискретизация проведённая согласно теореме Котельникова называется равномерной дискретизацией.

Согласно этой теореме шаг дискретизации должен удовлетворять следующему условию:

$$\Delta x \leq \frac{1}{2F_{max}}, \tag{3.14}$$

где F_{max} – максимальное значение плотности вероятности.

Очевидно что максимально допустимое $\Delta x = \frac{1}{2F_{max}}$.

$$X_{\text{ср}} = \int_0^{\infty} xf(x)dx. \tag{3.15}$$

$$\Delta x \leq X_{\text{ср}} - x_{max}. \tag{3.16}$$

Отсюда можно сделать вывод:

$$\Delta x \leq \min\left(\left(X_{\text{ср}} - x_{max}\right), \frac{1}{2f(x_{max})}\right). \tag{3.17}$$

3.5. Программное обеспечение для автоматизации анализа

Для оценки различный параметров можно воспользоваться прилагаемым к данным методическим пособию программным обеспечением.

1. Анализ пользы и ущерба производится следующим образом.

На главной форме программы следует сначала задать параметры работы исследуемого объекта (рис. 3.5).

Затем следует указать выбранную функцию полезности (рис. 3.6).

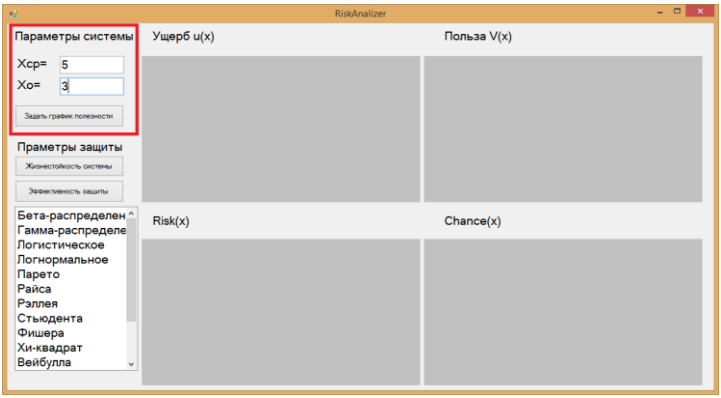

Рис. 3.5. Задание параметров функционирования системы

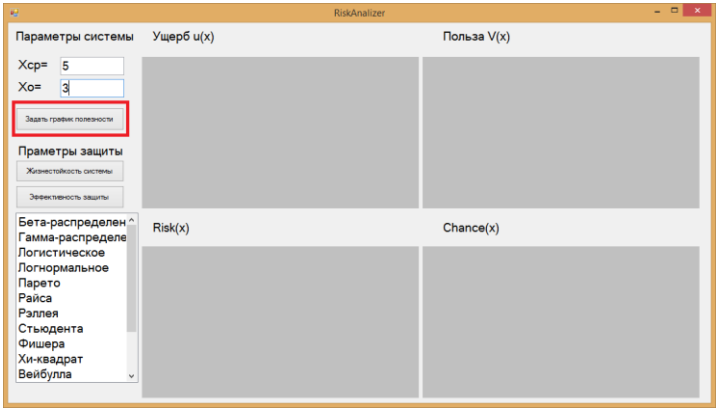

Рис. 3.6. Выбор функции полезности

Далее следует указать параметры для выбранной функции полезности (рис. 3.7).

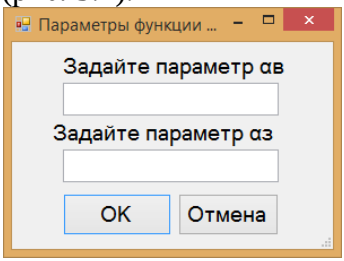

Рис. 3.7. Выбор параметров функции полезности

После этого следует оценить полученный график функции полезности (рис. 3.8).

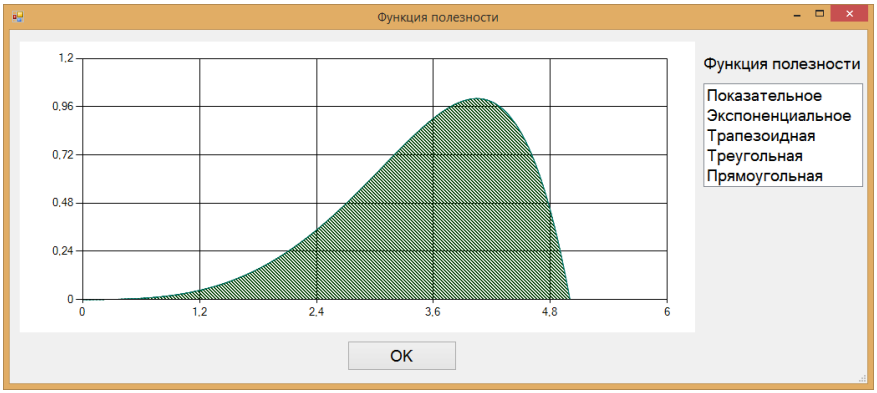

Рис. 3.8. График функции полезности

После задания функции полезности следует выбрать (рис. 3.9) из представленных законов распределения подходящий и исходя из этого оценить полученные значения полезности, ущерба, риска и шанса (рис. 3.10).

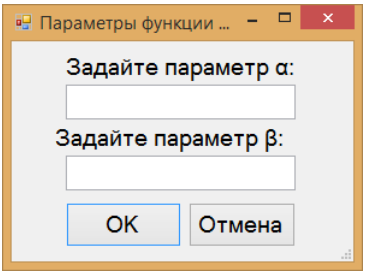

Рис. 3.9. Параметры распределения

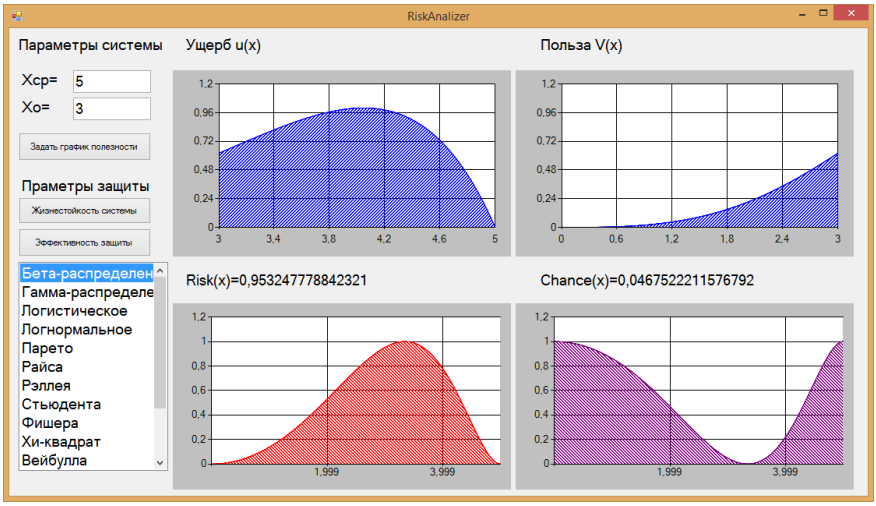

Рис. 3.10. Полученные значения и графики

2. Анализ жизнестойкости производится следующим образом.

Для анализа жизнестойкости исследуемого атакуемого объекта следует выбрать соответствующий пункт на главной форме программы (рис. 3.11).

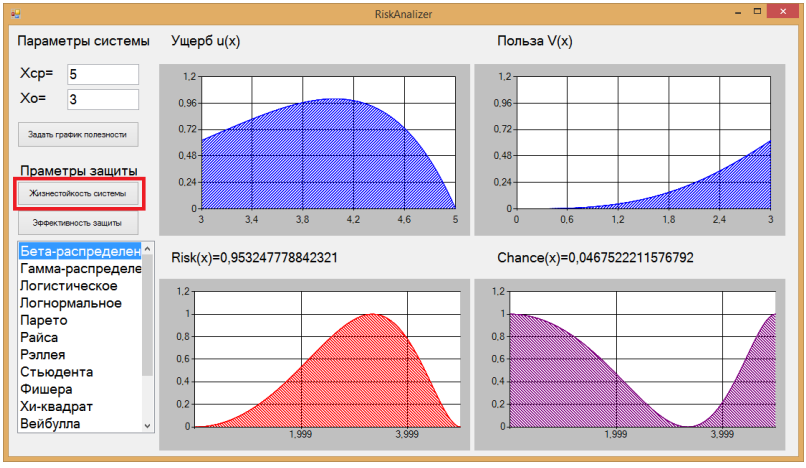

Рис. 3.11. Выбор жизнестойкости

После выбора соответствующего пункта можно выбрать мгновенную или интервальную жизнестойкость (рис. 3.12).

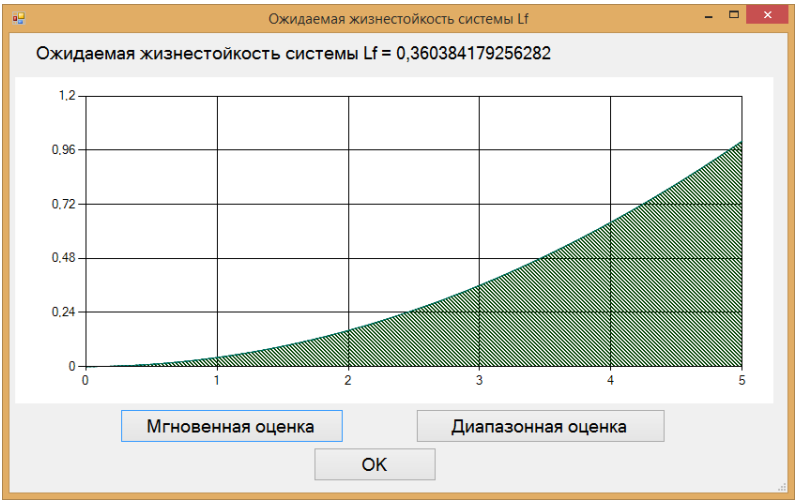

Рис. 3.12. Оценка жизнестойкости

3. Анализ эффективности защиты производится следующим образом.

Для анализа эффективности защиты следует воспользоваться соответствующим пунктом на главной форме (рис. 3.13).

После этого можно выбрать мгновенную или интервальную жизнестойкость, а также оценить полученные значения и графики (рис. 3.14).

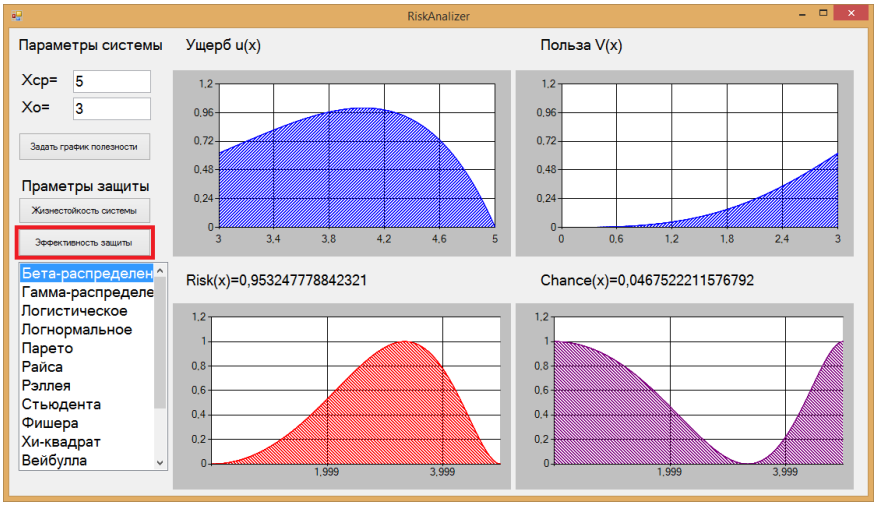

Рис. 3.13. Выбор эффективности

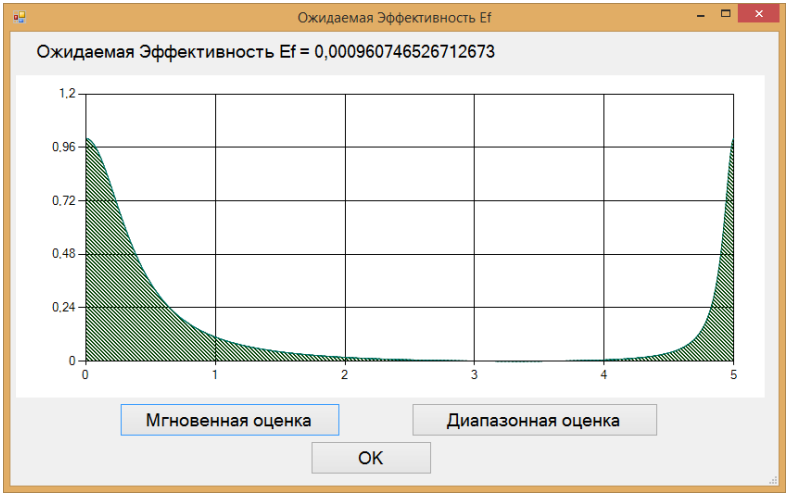

Рис. 3.14. Оценка эффективности ожидаемой защиты

Полученные с помощью данного программного обеспечения результаты могут помочь с анализом возможных недостатков защиты и представить данные для её улучшения.

ЗАКЛЮЧЕНИЕ

Настоящие методические рекомендации нацелены на обоснование актуальности темы ВКР, конкретизацию её объекта и предмета, формулировку цели и задач исследования. В них предлагается методическая основа для реализации вышеперечисленных процедур в контексте анализа известных литературных источников, выявления в них противоречий и определения направления исследований ВКР с использованием рекомендуемого инструментария.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Остапенко, А. Г. Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обеспечением [Текст] / А. Г. Остапенко, Д. Г. Плотников. – Воронеж: ВГТУ, 2012. – 187 с.

2. Остапенко, Г. А. Основы оценки рисков и защищенности компьютерно атакуемых информационных систем и технологий [Текст]: учеб. пособие / Г. А. Остапенко, Д. Г. Плотников, О. А. Остапенко. – Воронеж: ВГТУ, 2013. – 180 с.

3. 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.

4. 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.

5. Остапенко, О. А. Методология оценки риска и защищенности систем [Текст] / О. А. Остапенко // Информация и безопасность. – 2005. – Вып. 2. – С. 28-32.

6. 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.

7. 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.

8. 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.

9. 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.

10. Райншке, К. Модели надёжности и чувствительности систем [Текст] / К. Райншке. –М.: МИР, 1979. – 434 с.

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к преддипломной практике
для студентов специальностей
090301 «Компьютерная безопасность»,
090302 «Информационная безопасность
телекоммуникационных систем»,
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Составители:
Остапенко Александр Григорьевич
Горобцов Александр Михайлович
Грачёв Александр Андреевич

В авторской редакции

Подписано к изданию 27.08.2015.
Уч.-изд. л. 4,2.

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