ISSN 2079-3316 ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ №2(25), 2015, с. 63–83

УДК 004.77:004.75

Н. С. Абрамов, В. П. Фраленко

Угрозы безопасности вычислительных комплексов: классификация, источники возникновения и методы противодействия

Аннотация. В работе рассмотрены источники возникновения угроз безопасности вычислительных систем. Предложены методы борьбы с возникающими угрозами и приведена их классификация. Особое внимание уделяется перспективным методам защиты. Предложена модель системы обеспечения информационной безопасности.

Ключевые слова и фразы: информационная безопасность, угроза, защита, модель.

Введение

Современные информационно-вычислительные системы в своей основе имеют комплекс программных и аппаратных средств для организации высокопроизводительной обработки и хранения данных. Как правило, подобные комплексы строятся на основе кластерной архитектуры, элементами которой являются узлы, являющиеся мультипроцессорными системами с общей памятью. Такая структура, в общем случае, является гетерогенной и нуждается в высококачественной и точной системе информационной безопасности [1–3]. Сложность построения систем информационной безопасности, охватывающих все аспекты защиты распределенных вычислительных комплексов высокой плотности, заключается в том, что эти комплексы используют:

- различные технологии и протоколы передачи информации;
- сетевое и телекоммуникационное оборудование разных классов и производителей;
- разнообразные операционные системы;

Работа выполнена при частичной поддержке ОНИТ РАН: проект №2.2 «Разработка средств и методов обеспечения информационной безопасности компьютерных сетей и информационно-вычислительных комплексов новых поколений».

- огромное число сетевых сервисов и информационных систем: серверы печати, базы данных, почтовые сервисы, системы доменных имен и др.

Необходимость обеспечения безопасности требует принятия как организационных, так и технических мер для обеспечения защиты от наносящих ущерб несанкционированных воздействий. Современные технологии защиты от несанкционированного доступа и внешнего воздействия базируются на контроле и мониторинге сетевой активности, позволяют выделять аномалии трафика за счет накопления и дальнейшего использования статистики обращений к серверам и предоставляемым ими сервисам. На сегодняшний день не существует универсальных способов защиты, поэтому есть необходимость создания новых средств, обладающих функциями обеспечения полноценной информационной защиты.

Актуальной является задача обеспечения информационной безопасности не только от сетевых атак, но и других угроз. По этой причине целесообразно перейти к новой расширенной концепции построения средств безопасности следующего поколения, опирающейся на применение интеллектуальных методов. В данной работе рассмотрены угрозы безопасности информационно-вычислительных комплексов, выполнена классификация, представлены источники возникновения и методы противодействия. Предложена модель системы информационной безопасности.

1. Классификация угроз

Основную ценность в вычислительных системах представляет информация (данные). Угрозы информации — потенциальные или возможные действия по отношению к информационной сфере, приводящие к несанкционированному изменению свойств информации.

Выделяют следующие угрозы информации, приводящие к информационному ущербу: *ознакомление*, *модификация*, *уничтожение* и *блокирование*. Отмечается и угроза *раскрытия параметров*, реализация которой ведет к полной информированности злоумышленника об уязвимостях вычислительной системы.

В случае *ознакомления* (угроза конфиденциальности) не происходит непосредственного изменения информации, однако происходит нарушение конфиденциальности (секретности) путем ознакомления с

ней лицами, не имеющими на это соответствующих прав, и несанкционированной модификации атрибутов секретности. При *модификации* информации (угроза целостности) происходит изменение состава и содержания сведений, однако полного уничтожения информации не происходит. *Уничтожение* (также считается угрозой целостности) приводит к полному разрушению информации, то есть к ее безвозвратной утере без возможности восстановления. Уничтожение может произойти в случае разрушения или кражи носителя информации, ее стирания с перезаписываемого носителя, пропажи питания и т. д. Легальность действия с информацией определяется политиками и моделями безопасности. При *блокировании* информации происходит потеря доступа к ней; возможности по ознакомлению, копированию, представлению информации могут быть восстановлены после устранения причин ограничения доступа [4].

Возможна и другая классификация угроз информации [5]:

- по объектам (персонал, материальные и финансовые ценности, информация);
- по ущербу (предельный, значительный, несущественный);
- по вероятности возникновения (от 0 до 1);
- по причинам появления (стихийные и преднамеренные);
- по отношению к объекту (внутренние и внешние);
- по характеру действия (активные и пассивные).

Источники информационных угроз можно разделить на источники *внешней* и *внутренней* опасности [6]. К первой группе относят:

- ошибки обслуживающего персонала;
- искажение поступающей от внешних источников и передаваемой информации, а также неприемлемые изменения свойств потоков информации;
- отказы и сбои аппаратуры;
- расширение состава и конфигурации информационной системы за пределы, установленные при испытаниях и сертификации.

Ко второй группе относят:

- системные ошибки проектирования информационной системы, ошибки расчета требований к функциям и характеристикам решения задач и условий функционирования;
- алгоритмические ошибки проектирования при программной реализации программ и баз данных, ошибки определения характера взаимодействия отдельных компонент системы;

- ошибки программирования в текстах программ, ошибки в техническом задании на информационную систему и ошибки в документации на ее отдельные компоненты;
- посредственная эффективность применяемых средств защиты и мероприятий по обеспечению работоспособности в условиях негативных нештатных воздействий.

Факт возникновения угрозы безопасности информационной системы является следствием наличия определенных уязвимостей в системе. Уязвимости относятся к объекту информатизации и могут возникать еще на этапе проектирования информационной системы, например, из-за принятых ограничений функционирования, особенностей архитектуры, выбранных протоколов передачи данных и интерфейсов, используемого в системе программного обеспечения, условий эксплуатации и пр. Поскольку угрозы безопасности и причины их возникновения (уязвимости) неразрывны, каждой угрозе можно сопоставить одну или несколько уязвимостей. В таблице 1 определены три класса уязвимостей: объективные, субъективные и случайные [7].

Объективные уязвимости напрямую зависят от особенностей, возможностей и ограничений технических характеристик оборудования или системы. К данному классу можно отнести несколько типов уязвимостей:

- излучения технических средств системы (звуковые, электромагнитные, электрические и пр.);
- активизируемые (к ним относятся, например, нелегальные копии программного обеспечения, программные вирусы, повышающие риск атаки, или напрямую вызывающие атаки, и пр.);
- особенности элементной базы, на которой построена система;
- особенности защищаемого объекта (местоположение объекта, организация каналов передача информации и др.).

Субъективные уязвимости основываются на человеческом факторе и напрямую зависят от действий персонала, имеющего доступ и влияющего на работу информационной системы. К таким уязвимостям можно отнести:

- ошибки в программном обеспечении, влияющие на процесс инсталляции, эксплуатации и ввода-вывода данных;
- неквалифицированное управление системой;
- неправильная эксплуатация технических средств;

Таблица 1. Классификация уязвимостей

Объективные	**Субъективные**	**Случайные**
излучения технических средств системы	ошибки в программном обеспечении	сбои и отказы технических средств
активизируемые	неквалифицированное управление системой	естественное старение носителей информации
элементная база	неправильная эксплуатация технических средств	сбои сопутствующего программного обеспечения
особенности защищаемого объекта	нарушение установленного режима доступа	сбои электроснабжения
	нарушение режима эксплуатации	повреждения коммуникаций
	нарушение установленных политик безопасности	повреждение ограждающих конструкций

- нарушение установленного режима доступа, охраны и защиты объектов системы;
- нарушение режима эксплуатации технических средств;
- нарушение установленных политик безопасности и конфиденциальности.

Случайные уязвимости возникают, как правило, вследствие обстоятельств непреодолимой силы (например, естественное старение и погодные условия). Эти события затруднительно или вообще невозможно предсказать. К ним относятся:

- сбои и отказы технических средств информационной системы;
- естественное старение носителей информации и сред передачи данных;
- сбои сопутствующего программного обеспечения (операционных систем, СУБД, антивирусных программ и др.);
- сбои электроснабжения;

- повреждения жизнеобеспечивающих коммуникаций;
- повреждение ограждающих конструкций.

Полное устранение уязвимостей первого класса невозможно, однако возможно демпфировать их влияние различными техническими методами защиты безопасности информации. Уязвимости второго класса устраняются организационными и программно-аппаратными методами. Уязвимости третьего класса, в силу своей природы, можно лишь частично «смягчить» посредством проведения комплекса организационных и инженерно-технических мероприятий по обеспечению информационной безопасности.

Существенное подмножество уязвимостей приходится на долю *настроек системы безопасности*. В качестве примера можно привести следующие уязвимости: использование пустых паролей, некорректные права доступа к ключевым системным разделам и файлам, неадекватные угрозам политики обновления системного программного обеспечения и др. В случае большой вычислительной сети даже применение средств автоматизации управления политиками безопасности может не решить имеющихся проблем в связи с огромным количеством сервисов, файлов, разнородных операционных систем и специализированных устройств.

Наиболее часто в литературе упоминаются такие угрозы безопасности, как *программы-закладки* и *вирусы*. Компьютерный вирус — программа, способная заражать другие программы за счет их модификации с добавлением копии вируса или его разновидности. Компьютерная закладка — аппаратное и/или программное средство, реализующее угрозы аппаратным или программным ресурсам ЭВМ с помощью внесенных извне функциональных объектов, которые при некоторых условиях (входных данных) осуществляют выполнение неописанных в документации действий [**5**, **8**].

Вредоносные программы принято классифицировать по

- методу внедрения в вычислительную среду (оператором, на этапе разработки прикладного программного обеспечения, на этапе разработки программы BIOS, подмена аппаратных составляющих);
- расположению (аппаратная или программная реализация);
- логической структуре (однокомпонентные, двухкомпонентные и многокомпонентные, каждый отдельный компонент осуществляет свои специфические функции);
- функциональным возможностям (искажение информации, нару-

шение работы установленных систем защиты, перехват информации, имитация аппаратных сбоев, диверсия, нарушение работы вычислительной сети);
- способу активизации (внешнее или внутреннее воздействие).

Далее рассмотрим существующие и предлагаемые методы противодействия перечисленным угрозам.

2. Методы противодействия

Рассмотрим методы противодействия угрозам (см. таблицу 2), возникающим вследствие уязвимостей, приведенных в таблице 1. В первом столбце указаны методы, во втором — уязвимости и угрозы, от которых они защищают.

Подробнее о способах и средствах защиты информации:

(1) Препятствие: запрет проникновения на территорию размещения вычислительной сети, доступа к аппаратуре и носителям информации. Применяются физические и аппаратные средства защиты, например, решетки на окнах, охранные сигнализации, электронные ключи-брелоки и т. д.

(2) Управление: регулирование ресурсов системы (баз данных, носителей информации, программ). Наличие правил работы пользователей, технического персонала, программ. Защищаемую систему должна сопровождать актуализированная, комплектная документация, позволяющая осуществлять развитие системы и ее квалифицированную эксплуатацию.

(3) Регламентация:
- управление списком допущенных к оборудованию физических лиц (пользователей и обслуживающего персонала);
- ограничение времени работы с авторизованными терминалами, ограничение доступа к ресурсам системы, ограничение разрешенных для исполнения задач (процедур);
- регламентация мест постоянного хранения носителей информации.

(4) Маскирование (кодирование, шифрование): преобразование данных к такому виду, что они становятся доступны лишь после предъявления ключа. Возможно применение методов стеганографии, позволяющих скрыть не только смысл хранящейся или передаваемой информации, но и сами факты ее передачи и хранения.

Таблица 2. Методы противодействия угрозам

Методы противодействия	**Угрозы**
Препятствие	Субъективные: нарушение установленного режима доступа, нарушение режима эксплуатации
Управление	Субъективные: ошибки в программном обеспечении, неквалифицированное управление системой
Регламентация	Объективные: активизируемые
	Субъективные: нарушение установленных политик безопасности, нарушение режима эксплуатации, нарушение установленного режима доступа, неправильная эксплуатация технических средств
	Случайные: естественное старение носителей информации, сбои и отказы технических средств и пр.
Маскирование	Субъективные: нарушение установленного режима доступа, нарушение установленных политик безопасности
Повышение отказоустойчивости	Объективные: излучение технических средств системы, элементная база, особенности защищаемого объекта

(5) Повышение отказоустойчивости за счет дублирования (полного, частичного и комбинированного) и помехоустойчивого кодирования информации, применения адаптивных схем организации системы [9].

Следует отметить недостатки известных подходов к обеспечению

информационной безопасности и систем на их основе:

- в сетях с шифрованием и коммутацией системы анализа сетевых пакетов не могут обнаруживать атаки в зашифрованном трафике, так как сама атака тоже оказывается зашифрована;
- проблемы мониторинга трафика в коммутируемых сетях;
- отсутствие сигнатур для самых новых уязвимостей приводит к потенциальной незащищенности корпоративной сети;
- гетерогенность сети, наличие разных операционных систем и использование разнородных протоколов, рассредоточенность данных об атаке по сотням узлов;
- проблема ложных срабатываний — малейшие ошибки используемых анализаторов могут приводить к парализации работы вычислительной сети; действия администратора в нештатной ситуации также могут быть восприняты как продолжение атаки, так как такие действия пользователя сети не характерны, то есть не соответствуют обычному профилю;
- проблемы идентификации злоумышленника и хоста, осуществляющего атаку, адрес может изменен (атака типа «спуффинг»);
- проблема атак типа DoS и DDoS на саму систему обнаружения вторжений, когда осуществляется блокировка сенсоров, искажение накопленных статистических данных и пр.;
- проблема нехватки системных ресурсов, необходимых для осуществления системой обнаружения вторжений функций контроля и протоколирования;
- проблема сбора неопровержимых доказательств для суда или контрольной службы;
- проблема интеллектуального анализа собираемых данных.

К методам обеспечения информационной безопасности обычно относят комплекс мер, направленных на

- предупреждение угроз (превентивные меры по упреждению возможности возникновения угроз);
- выявление, обнаружение и локализация угроз (осуществляется за счет систематического анализа и контроля возможности появления потенциальных угроз или реальных угроз и конкретных преступных действий);
- ликвидация угрозы, последствий угроз и преступных действий, восстановление номинального состояний.

В рамках такого комплекса мер могут применяться как аппарат-

ные, так и программные средства защиты. К аппаратным средствам защиты информации относят различные по принципу действия и возможностям технические решения, обеспечивающие защиту информации от разглашения, утечек и несанкционированного доступа. Они применяются при исследовании технических средств на наличие каналов утечки информации, поиске и обнаружении средств промышленного шпионажа, противодействии несанкционированному доступу к источникам конфиденциальной информации и т. д. Конкретные решения устанавливаются как в отдельных вычислительных машинах (в центральных процессорах: кодовое резервирование; в оперативной памяти: ограничение доступа с помощью специальных регистров контроля и защиты данных, схемы стирания и пр.; в контроллерах ввода-вывода: например, такие аппаратные средства как ключи, кодовые карты, анализаторы голоса и отпечатков пальцев), так и на различных участках сети. Программные же средства могут быть классифицированы следующим образом:

- средства собственной самозащиты, входящие в предусмотренный разработчиком программного обеспечения функционал;
- средства защиты аппаратуры и штатных устройств;
- средства идентификации полномочий пользователя;
- средства активной защиты при особых обстоятельствах, например, в случае ввода неправильного пароля и т. д.;
- средства пассивной защиты, направленные на предостережение.

Например, для борьбы с компьютерными вирусами существует три способа защиты:

- сканеры, просматривающие защищаемые области вычислительной системы и тестирующие ее на наличие вирусов;
- резидентные мониторы, находящиеся в оперативной памяти и следящие за тем, чтобы в системе не производилось недозволенных действий;
- ревизоры диска, работающие со слепком системы и отслеживающие изменения.

Наиболее действенным средством борьбы с вирусами является профилактика, заключающаяся в использовании только лицензионного программного обеспечения, проведении регулярного резервирования, проверке всей поступающей информации на вирусы.

Для эффективной борьбы с закладками применяются инструментальные средства для статического и динамического анализа текстов

исходных программ и динамического анализа процессов их выполнения. Применение всей совокупности указанных средств позволяет повысить результативность работ по выявлению закладок в программном обеспечении.

Межсетевые экраны позволяют разделить зону ответственности на несколько частей и реализовать набор правил прохождения пакетов с данными через границы зон. Фильтрацию сетевых пакетов с помощью межсетевых экранов можно осуществлять на разных уровнях сетевого взаимодействия: межсетевые экраны можно классифицировать на экранирующие маршрутизаторы, шлюзы сеансового уровня и шлюзы прикладного уровня. *Первые* функционируют на сетевом уровне модели OSI, но в своей работе используют информацию и из заголовков протоколов транспортного уровня, фильтрация может осуществляться как по IP-адресам отправителя/получателя, так и по портам TCP и UDP. Не защищают от атак с подменой участников соединений. *Вторые* работают на сеансовом уровне модели OSI и могут также контролировать информацию транспортного и сетевого уровне. Могут контролировать установку соединений, осуществлять проверку сетевых пакетов. *Третьи* могут осуществлять анализ пакетов на всех уровнях модели OSI, обеспечивая тем самым максимальный уровень защиты, в том числе за счет возможностей по аутентификации пользователей; проверки команд, передаваемых по протоколам прикладного уровня; проверки передаваемых данных на вирусы и нарушения политик безопасности [4]. Однако, межсетевые экраны не обеспечивают полной защиты от специальных программно-технических воздействий, они лишь способны обнаружить порядка 30% атак на сети, подключенные к международным информационным сетям. То же самое относится и к антивирусным средствам.

Шифрование может применяться как в фоновом, незаметном режиме (в случае канального шифрования осуществляется защита всей передаваемой по каналам связи информации, в том числе и служебной), так и эпизодически (оконечное шифрование для защиты конкретной передачи между двумя абонентами). На практике используют системы шифрования с симметричными и асимметричными алгоритмами. В первом случае отправитель (источник) и получатель (адресат) должны иметь общий устанавливаемый заранее секретный ключ. Во втором случае для шифрования информации используется один открытый ключ, который можно дать всем потенциальным респондентам получателя. Расшифровать информацию сможет только

тот, кто имеет секретный закрытый ключ. Однако, при использовании систем шифрования данных могут возникнуть проблемы, связанные со снижением производительности вычислительной системы, увеличением времени шифрования и дешифрования; достижением требуемого уровня секретности; надежным функционированием вычислительной системы: нечеткость и несовершенство используемых алгоритмов могут привести к потере данных, невозможности их восстановления.

3. Методология защиты

Все перечисленные выше средства по отдельности неспособны решить поставленную задачу обеспечения информационной безопасности, что *требует разработки новой пошаговой методологии*. Например, можно предложить следующий вариант.

На первом шаге по организации защиты вычислительных систем и сетей следует выполнить максимально широкую оценку имеющихся информационных ресурсов, в том числе их основных компонентов, взаимозависимостей и уязвимостей. Такая оценка осуществляется администраторами системы и специалистами по безопасности. В сложных информационных системах невозможно обеспечить хотя бы частичное отсутствие дефектов проектирования и реализации. Средства тестирования защищенности позволяют вести автоматизированный поиск уязвимостей в сетевых сервисах. На основании собранных о сети данных осуществляется выдвижение предположений о наличии тех или иных уязвимостей, далее эмулируются атаки на эти ресурсы. Качество функционирования подобных средств напрямую зависит от полноты базы уязвимостей.

Второй шаг предусматривает установку многоступенчатой защиты, включая программы обнаружения вторжений, корпоративные системы управления и сканеры зловредных кодов. Эти программы необходимы для

- регулирования правил доступа и работы авторизованных пользователей и их программного обеспечения — для определения аномальной активности законных пользователей;
- мониторинга находящихся в сети компьютеров, настройки правил доступа и работы;
- статического и динамического анализа кодов операционной системы и другого программного обеспечения.

Третий шаг подразумевает разработку средств своевременного предупреждения и информирования о нападениях. В рамках подобных решений может предусматриваться создание эффективной системы, обрабатывающей и контролирующей информацию об атаках в режиме, максимально близком к реальному времени. Благодаря качественной интеллектуальной обработке и за счет доступа к базам типовых образцов вторжений, могут обнаруживаться схожие инциденты.

На четвертом шаге — разработка решений, способствующих прогнозированию дальнейшей активности нападающих, средств восстановления способности сети справляться с информационным нападением, средств обеспечения непрерывности работы сети. В качестве ответных действия могут выступать:

- блокировка доступа к сети подозрительных пользователей;
- принятие дополнительных мер по защите безопасности, не применяемых в нормальном режиме функционирования вычислительной сети;
- установка обновлений программного обеспечения для повышения безопасности подверженного атаке программного обеспечения;
- изолирование элементов сети;
- уведомление правоохранительных органов.

Для разработки соответствующих программных и аппаратных решений классификации конкретных видов атак на практике применяется множество подходов. Обычный подход к обнаружению и классификации атаки сводится к анализу профилей поведения или к поиску специфических строковых сигнатур. Используя эти методы, невозможно подготовить обучающую базу данных, содержащую полные варианты сигнатур для большей части атак.

Сигнатурный анализ эффективен лишь в случаях, когда деструктивное воздействие заключается или завершается специфическим сетевым пакетом или их малой последовательностью. Методы, основывающиеся на анализе поведения, сильно зависимы от выбора показателей, периодичности сбора данных и характеристик защищаемой сети. Для составления профилей в том числе может применяться следующая информация: количество процедур аутентификации в сутки, предполагаемое самое раннее время входа, максимальная длительность сессии, статистика использования ресурсов вычислительной системы, частота чтения и записи определенных файлов и пр. Задача сопоставления профиля штатного поведения является трудоемкой и не

имеет универсального решения; штатный профиль модифицируется в течение времени.

Для указанных задач, как показывает практика, с успехом могут применяться искусственные нейронные сети, которые имеют способности к самообучению на нормальном и анормальном сетевом трафике, чем объясняется их высокая эффективность при решении рассматриваемой задачи. Нейросеть может использоваться в разных вариациях, например, участвовать в составлении профилей (осуществляя кластеризацию многомерных данных), анализировать весь сетевой трафик, рассматривать последовательности вводимых пользователем команд, переходов состояний и т. д. В качестве примера можно привести работы [10–12]. В первой из них описаны результаты исследований разработанной нейросетевой системы обнаружения атак на основе самоорганизующихся карт Кохонена. Тестирование показало, что нейросетевой подход к решению проблемы защиты информационных сетей достаточно уверенно обнаруживает атаки и при этом имеет низкий показатель ложных срабатываний. В работах [11, 12] представлено методологическое обеспечение информационной защиты, в том числе последовательность разработки средств обнаружения и распознавания сетевых атак, логическая структура интеллектуальной системы, концепция многоуровневого анализа данных. Подготовлены рекомендации для оптимизации имеющихся программно-инструментальных средств для обеспечения защиты систем облачных вычислений. Экспериментальные исследования показывают, что могут быть достигнуты близкие к нулю ошибки первого и второго рода. Полученные решения с применением комитетов нейросетевых и статистических классификаторов позволяют успешно обнаруживать закономерности и аномалии в потоках данных, распознавать модифицированные и новые атаки.

4. Модель системы защиты информации

Для эффективной защиты информационных объектов предлагается модифицировать архитектуру системы защиты [13], добавив в нее полное перекрытие, предусматривающее не менее одного барьера на каждое возможное действие нарушителя безопасности. Систему защиты информации можно описать как $S = \{O, Y, M\}$, где O — перечень объектов, подлежащих защите; Y — перечень возможных угроз; M — средства обеспечения безопасности. В качестве модели системы защиты информации вычислительных комплексов предлагается использовать трехдольный граф (см. рис. 1).

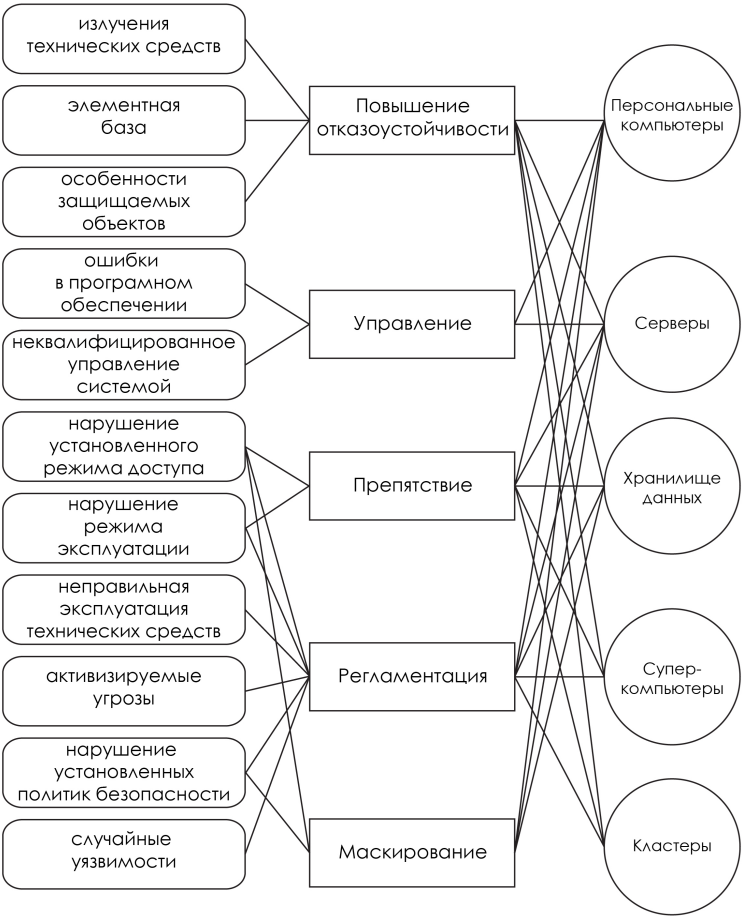

Рис. 1. Модель системы защиты информации

Система защиты, представляющая собой множество средств обеспечения защиты информации M, играет роль некого «барьера» между объектами защищаемой информационной системы O и множеством угроз Y. Данная графовая структура позволяет модернизировать систему, например, добавляя новый объект защиты, следует добавить/использовать существующий метод его защиты, при этом возникнут новые связи, в том числе, добавится некоторый набор новых или уже существующих угроз.

Заключение

В работе рассмотрены основные и наиболее распространенные на сегодняшний день угрозы безопасности вычислительных систем. Приведены классификация возможных угроз по источникам их возникновения и классификация уязвимостей, приводящих к угрозам безопасности. Дано описание возможных угроз, требующих особого внимания при построении системы информационной безопасности, и предложена модель системы защиты информации вычислительных комплексов.

На основании сделанного информационно-аналитического обзора следует, что перспективная система защиты информации может быть построена на следующих принципах:

- защищенность информации от утечек по каналам технических средств, несанкционированных изменений, повреждений и уничтожения на всех этапах работы с ней (в том числе за счет криптозащиты, создания территориально разнесенных копий, средств контроля целостности и пр.);
- аутентификация производящих обмен информацией сторон с помощью средств цифровых сертификатов и подписей;
- разграничение прав пользователей и обслуживающего контингента при работе с информационными ресурсами (в том числе — конфиденциальными);
- полное документирование работы как самой вычислительной сети, так и подсистемы защиты;
- защита программного обеспечения от несанкционированной модификации;
- сертификация всех ключевых компонентов;
- принцип ответной реакции.

Принцип ответной реакции, служащий основой построения активной защитной системы, можно сформулировать следующим образом:

- автоматическая блокировка объектов, осуществляющих нарушения целостности и достоверности информации;
- статистический учет, протоколирование и своевременное извещение уполномоченного персонала о заблокированных процессах;
- фаза активной реакции завершается привлечением уполномоченного персонала или специализированных средств принятия решений для экспертной оценки характера ущерба, способов ней-

трализации и осуществления действий технического и организационного характера.

Выделен ряд необходимых подсистем.

(1) *Подсистема управления доступом* выполняет функции идентификации и проверки подлинности субъектов доступа вычислительной системы; контроля и управления доступом к защищаемым данным в соответствии с заданным уровнем конфиденциальности и правами доступа.
(2) *Подсистема регистрации и учета* выполняет функции регистрации, создания, изменения и удаления учетных записей субъектов доступа; регистрации и учета конфиденциальной информации; регистрации изменения полномочий субъектов доступа; регистрации изменений общего уровня секретности.
(3) *Криптографическая система* осуществляет функции шифрования трафика в сети, конфиденциальной информацию на отчуждаемых и встраиваемых носителях.
(4) *Подсистема обеспечения целостности* обеспечивает контроль целостности основных модулей информационной системы, контроль целостности файлов.

Список литературы

[1] Ю. Г. Емельянова, В. П. Фраленко. «Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления», *Программные системы: теория и приложения*, 2011, №4(8), с. 17–31, URL http://psta.psiras.ru/read/psta2011_4_17-31.pdf ↑ 63.

[2] А. А. Кондратьев, И. П. Тищенко, В. П. Фраленко. «Разработка распределенной системы защиты облачных вычислений», *Программные системы: теория и приложения*, 2011, №4(8), с. 61–70, URL http://psta.psiras.ru/read/psta2011_4_61-70.pdf ↑ 63.

[3] Ю. Г. Емельянова, А. А. Талалаев, И. П. Тищенко, В. П. Фраленко. «Нейросетевая технология обнаружения сетевых атак на информационные ресурсы», *Программные системы: теория и приложения*, 2011, №3(7), с. 3–15, URL http://psta.psiras.ru/read/psta2011_3_3-15.pdf ↑ 63.

[4] С. А. Нестеров, *Информационная безопасность и защита информации*, Учебное пособие, Изд-во Политехн. ун-та, СПб., 2009, 126 с. ↑ 65, 73.

[5] *Информационная безопасность и защита информации*, Учебное пособие, Ростовский юридический институт МВД России, Ростов-на-Дону, 2004, 82 с. ↑ 65, 68.

[6] В. Липаев. *История развития программного обеспечения*, http://www.computer-museum.ru/histsoft/ji97061.htm ↑ 65.

[7] С. В. Вихорев. *Классификация угроз информационной безопасности*, http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml, 19.09.2001 ↑ 66.

[8] *Защита от несанкционированного доступа к информации. Часть 1: Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей*, Руководящий документ, http://www.profinfo.ru/biblio/rdnsd.pdf, Гостехкомиссия России, 1992 ↑ 68.

[9] Ю. А. Гатчин, В. В. Сухостат. *Теория информационной безопасности и методология защиты информации*, СПбГУ ИТМО, СПб., 2010, 98 с. ↑ 70.

[10] А. Ю. Балахонцев, Д. В. Сидорик, А. Н. Сидоревич, М. В. Якутович. «Нейросетевая система для обнаружения атак в локальных вычислительных сетях», 62-я научная конференция студентов и аспирантов БГУ (Минск, 2005) ↑ 76.

[11] А. А. Кондратьев, А. А. Талалаев, И. П. Тищенко, В. П. Фраленко, В. М. Хачумов. «Методологическое обеспечение интеллектуальных систем защиты от сетевых атак», *Современные проблемы науки и образования*, 2014, №2, URL http://www.science-education.ru/pdf/2014/2/610.pdf ↑ 76.

[12] А. А. Кондратьев, А. А. Талалаев, И. П. Тищенко, В. П. Фраленко, В. М. Хачумов. «Процессы проектирования и разработки интеллектуальной защиты вычислительных систем и сетей», Материалы 4-й научно-практической internet-конференции (Тольятти, 2014), *Междисциплинарные исследования в области математического моделирования и информатики*, с. 234–242 ↑ 76.

[13] Е. К. Баранова, А. В. Бабаш, *Информационная безопасность и защита информации*, Учебное пособие, Изд. Центр ЕАОИ, М., 2012, 311 с. ↑ 76.

Рекомендовал к публикации *д.т.н., проф. В. М. Хачумов*

Об авторах:

Николай Сергеевич Абрамов

К.т.н., научный сотрудник ИЦМС ИПС им. А.К. Айламазяна РАН. Область научных интересов: математические методы синтеза, обработки и анализа изображений и сигналов, искусственный интеллект и принятие решений, интеллектуальный анализ данных и распознавание образов, геометрия.

e-mail: n-say@nsa.pereslavl.ru

Виталий Петрович Фраленко

К.т.н., старший научный сотрудник ИЦМС ИПС им. А.К. Айламазяна РАН, автор более 70 публикаций. Область научных интересов: интеллектуальный анализ данных и распознавание образов, искусственный интеллект и принятие решений, параллельные алгоритмы, сетевая безопасность, диагностика сложных технических систем.

e-mail: alarmod@pereslavl.ru

Пример ссылки на эту публикацию:

Н. С. Абрамов, В. П. Фраленко. «Угрозы безопасности вычислительных комплексов: классификация, источники возникновения и методы противодействия», *Программные системы: теория и приложения*, 2015, **6**:2(25), с. 63–83.

URL http://psta.psiras.ru/read/psta2015_2_63-83.pdf

Nikolai Abramov, Vitaly Fralenko. *Computer systems security threats: classification, sources of origin and counteraction methods.*

Abstract. The paper discusses the computer systems security threats sources. Proposed scientific response for emerging threats and implemented their classification. Particular attention is given to promising protection methods. Proposed model of information security management system. (*In Russian*).

Key Words and Phrases: information security, threat, protection, model.

References

[1] Yu. G. Yemel'yanova, V. P. Fralenko. "Problems and prospects analysis for cloud computing network attacks detection and prevention intelligent system creation", *Program Systems: Theory and Applications*, 2011, no.4(8), pp. 17–31 (in Russian), URL http://psta.psiras.ru/read/psta2011_4_17-31.pdf.

[2] A. A. Kondrat'yev, I. P. Tishchenko, V. P. Fralenko. "Development of the distributed security system for cloud computing", *Program Systems: Theory and Applications*, 2011, no.4(8), pp. 61–70 (in Russian), URL http://psta.psiras.ru/read/psta2011_4_61-70.pdf.

[3] Yu. G. Yemel'yanova, A. A. Talalayev, I. P. Tishchenko, V. P. Fralenko. "Neural network technology of detection network attacks on information resources", *Program Systems: Theory and Applications*, 2011, no.3(7), pp. 3–15 (in Russian), URL http://psta.psiras.ru/read/psta2011_3_3-15.pdf.

[4] S. A. Nesterov, *Information security and information protection*, Textbook, Izd-vo Politekhn. un-ta, SPb., 2009 (in Russian), 126 p.

[5] *Information security and information protection*, Textbook, Rostovskiy yuridicheskiy institut MVD Rossii, Rostov-na-Donu, 2004 (in Russian), 82 p.

[6] V. Lipayev. *The software history*, http://www.computer-museum.ru/histsoft/ji97061.htm (in Russian).

[7] S. V. Vikhorev. *Classification of information security threats*, http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml, 19.09.2001 (in Russian).

[8] *Protection against unauthorized access to information. Part 1: Software for information protecting. the classification by undeclared features control level*, Rukovodyashchiy dokument, http://www.profinfo.ru/biblio/rdnsd.pdf, Gostekhkomissiya Rossii, 1992 (in Russian).

[9] Yu. A. Gatchin, V. V. Sukhostat. *The theory of information security and information protection methodology*, SPbGU ITMO, SPb., 2010 (in Russian), 98 p.

[10] A. Yu. Balakhontsev, D. V. Sidorik, A. N. Sidorevich, M. V. Yakutovich. "Neural network system for intrusion detection in local area networks", 62-ya nauchnaya konferentsiya studentov i aspirantov BGU (Minsk, 2005) (in Russian).

[11] A. A. Kondrat'yev, A. A. Talalayev, I. P. Tishchenko, V. P. Fralenko, V. M. Khachumov. "Methodological support for network attacks intelligent protection systems", *Modern problems of science and education*, 2014, no.2 (in Russian), URL http://www.science-education.ru/pdf/2014/2/610.pdf.

[12] A. A. Kondrat'yev, A. A. Talalayev, I. P. Tishchenko, V. P. Fralenko, V. M. Khachumov. "Design and development processes in computer and networks intellectual protection", Materialy 4-y nauchno-prakticheskoy internet-konferentsii (Tol'yatti, 2014), *Mezhdistsiplinarnyye issledovaniya v oblasti matematicheskogo modelirovaniya i informatiki*, pp. 234–242 (in Russian).

[13] Ye. K. Baranova, A. V. Babash, *Information security and protection of information*, Textbook, Izd. Tsentr YeAOI, M., 2012 (in Russian), 311 p.

Sample citation of this publication:

Nikolai Abramov, Vitaly Fralenko. "Computer systems security threats: classification, sources of origin and counteraction methods", *Program systems: theory and applications*, 2015, **6**:2(25), pp. 63–83. (*In Russian.*)

URL http://psta.psiras.ru/read/psta2015_2_63-83.pdf