УДК 00456

А. В. Ревнивых, **А. М. Федотов**

Тюменский государственный нефтегазовый университет
ул. Володарского, 38, Тюмень, 625000, Россия

Институт вычислительных технологий СО РАН
пр. Акад. Лаврентьева, 6, Новосибирск, 630090, Россия

E-mail: fedotov@sbras.ru

ДОСТУПНОСТЬ РЕСУРСОВ ИНФОРМАЦИОННЫХ СИСТЕМ

Работа посвящена описанию основных принципов защиты от нарушений доступности ресурсов в информационных системах, а также соответствующим политикам информационной безопасности.

Ключевые слова: информационная безопасность, доступность информационных ресурсов, надежность информационных систем, профили системы, политики информационной безопасности.

Введение

В современном мире, насыщенном информационными технологиями и ресурсами, особую роль начинает играть их доступность. Прежде всего, доступность может быть охарактеризована как наличие определенных условий для того, чтобы была возможность воспользоваться информацией или сервисами (например, само наличие терминала для доступа, его исправность, соблюдение необходимых условий для его работы и т. д.), возможность подключения к сети передачи данных (и работоспособность данного подключения), а также наличие и работоспособность инфраструктуры, в которой запрашиваемая информация хранится и обрабатывается.

Доступность информационных ресурсов – это одно из свойств информационной безопасности (ИБ).

Причины нарушения доступности информации могут быть самыми различными – от банальных неисправностей оборудования и сбоев программного обеспечения до успешных реализаций сетевых атак на отказ в обслуживании (PING-flooding, SYN-flooding, DoS, DDoS). Риск нарушения работоспособности информационной системы (ИС), содержащей запрашиваемую пользователем информацию, зависит от надежности совокупности аппаратных и программных компонентов, составляющих систему, а также от адекватности оператора, управляющего их работой. Нарушения доступности возникают из-за несоблюдения требований стандартов на этапе проектирования, производства или эксплуатации системы. Кроме того, нарушения доступности системы или ее компонентов могут быть вызваны внешними по отношению к ней факторами – отключениями электропитания, стихийными бедствиями и т. д.

Базовые понятия доступности информации

Под доступностью информации будем понимать возможность доступа субъекта к данным по запросу в любое предусмотренное расписанием работы системы время [1]. Доступность ресурсов является одним из аспектов политики ИБ (набора правил для обеспечения ИБ) [2; 3].

Ревнивых А. В., Федотов А. М. Доступность ресурсов информационных систем // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2014. Т. 12, вып. 1. С. 55–63.

ISSN 1818-7900. Вестник НГУ. Серия: Информационные технологии. 2014. Том 12, выпуск 1

Сложно себе представить обеспечение доступности информации без учета и соблюдения других критериев и политик ИБ. Например, тщательная разработка и дальнейшее соблюдение политики мониторинга информационной инфраструктуры (ИИ) позволяет на ранних этапах выявлять возникновение ситуаций, которые потенциально могут привести к нарушениям доступности [4].

Понятие доступности включает обеспечение работоспособности ресурсов, но при этом не ограничено этим. Например, сервис может быть недоступен не потому, что он не работает в принципе, а по причине большой нагрузки, создаваемой задачами других пользователей системы (аналогично, например, автомобильным «пробкам» – дорога и инфраструктура в принципе работоспособны, но перегружены из-за большого числа пользователей). В данной работе подразумевается, что в объем и содержание понятия «пользователи» могут входить не только люди, но и некие системы.

Таким образом, работоспособность ресурса еще не означает его доступности для пользователей, так как у пользователей еще должна быть возможность воспользоваться работоспособным ресурсом. Это можно проиллюстрировать ситуацией, когда у человека есть ключ от входной двери квартиры, но нет ключа от подъезда, в котором данная квартира расположена. Или, аналогично, если квартира и подъезд находятся в таком месте (например, в другом городе), куда человек добраться не может (по крайней мере, с разумными тратами времени и материальных ресурсов). Кроме того, еще возможен случай, когда человек просто не знает, где находится квартира, от которой у него имеются ключи, и поэтому тоже не может ей воспользоваться. Также имеет смысл упомянуть о варианте, когда имеющий ключи человек не знает о том, что это ключи и что с их помощью можно попасть в соответствующую квартиру.

Точно также и в ИС: для того чтобы воспользоваться работоспособным ресурсом, надо еще иметь работоспособный интерфейс для восприятия информации из этого ресурса, иметь соответствующий канал связи с инфраструктурой хранения и обработки информации, а также знать адрес ресурса. Умение обращаться с интерфейсом и самим ресурсом тоже является необходимым условием целесообразного и эффективного доступа к ресурсу.

Необходимо выделить свойство информационных ресурсов и сервисов, обозначаемое не имеющим в русском языке аналогов словом *Usability*. Обеспечение «usability» является неотъемлемым условием доступности. В качестве иллюстрации значения данного термина и влияния факторов, которые включаются в его смысл, на доступность ИС рассмотрим некий библиотечный каталог, с которым в принципе есть возможность работать через Web-интерфейс. Предположим, что в указанном Web-интерфейсе не реализованы функции многокритериального поиска. В результате ответ на запрос к указанному каталогу пользователь часто получает в виде многостраничного документа в браузере, разбираться в котором и находить нужное издание очень долго, сложно, и при этом еще требуется очень большая внимательность, так как человек может ошибиться при выборе информации. Поэтому в данном примере ресурс библиотечного каталога можно считать доступным только при наличии удобного средства для взаимодействия с ним пользователей (например, в виде отдельной удобной прикладной программы).

Необходимо отметить, что выполнение перечисленных выше условий все равно не гарантирует возможности комфортного использования некого информационного ресурса. В большинстве случаев современных пользователей ИС не устраивает длительная обработка запросов (ранее уже приводился пример с автомобильными «пробками», когда дорога, по сути, «работает», но проехать по ней быстро невозможно, как невозможно и заранее достоверно рассчитать, сколько конкретно потребуется времени на преодоление определенного участка дороги).

Скорость реакции системы на запросы, а также обработка запросов с последующей выдачей результатов должны быть адекватными потребностям пользователей.

ИИ можно представить состоящей из компонентов пяти основных уровней. Здесь уместна некоторая аналогия с сетевой семиуровневой моделью ISO/OSI [5], но уровней вполне достаточно выделить пять.

- На физическом уровне ИИ находятся аппаратные средства серверов, рабочих станций, а также внешние условия эксплуатации ИИ (давление, температура, запыленность и т. д.).
- На канальном уровне – поддержка инфраструктуры сети, канальные коммутаторы.

- На сетевом уровне – пассивное и активное сетевое оборудование (кабели, модемы, маршрутизаторы и т. д.).
- Транспортный уровень ИИ предполагает наличие сетевого оборудования и программного обеспечения. Сюда же отнесем программные и аппаратные средства для поддержки сетевых протоколов (в соответствии с базовой моделью ISO/OSI), сервисы.
- На прикладном (представительском, презентационном) уровне ИИ находятся разнообразные программно-аппаратные ИС, системное и прикладное ПО рабочих станций пользователей и т. д. [5].

Отметим, что для пользователей системы наиболее важен надежный доступ к функционалу ИС, поэтому в целом пользователю не особо важно, какими именно средствами обеспечивается надежность работы ИИ, нарушение которой может произойти на любом из перечисленных выше уровней.

Нарушения работоспособности могут быть следствием двух типов событий: сбоев и отказов. Под сбоем понимается кратковременная самоустраняющаяся утрата работоспособности технического устройства, отказ заключается в относительно длительном нарушении работоспособного состояния объекта.

Необходимо отметить, что сбои и отказы могут не влиять на работоспособность системы (например, при «отказах в обслуживании»), но при этом делать ее недоступной для пользователей, а могут приводить и к нарушениям работоспособности системы.

Обеспечение доступности функционала компонентов информационной инфраструктуры

В составе ИИ используется несколько основных компонентов.

1. Прикладное программное обеспечение (ПО) с определенным пользовательским интерфейсом.
2. Сетевые сервисы, работающие на разных уровнях модели ISO/OSI.
3. Платформы.
4. Сервисы и службы.

В основе каждого из этих компонентов, разумеется, лежит целый комплекс программно-аппаратных средств. Порядок следования компонентов в данном перечислении не особо важен, так как будет разным в случаях с разной структурой и функционалом ИИ. Например, в одних системах обработка информации в основном идет на стороне сервера, а в других – на стороне клиента [4].

Каждый из основных компонентов ИИ нуждается в защите доступности по определенным критериям, которые для каждого из компонентов будут индивидуальными.

Доступность прикладного программного обеспечения. Прикладное ПО является наиболее интенсивно используемым и знакомым для пользователей. При этом, учитывая множественность производителей такого рода ПО, оно бывает весьма разного качества с точки зрения надежности и безопасности функционирования.

Работоспособность прикладного ПО в целом, а также ее нюансы (например, скорость и надежность функционирования) зависят от множества факторов, связанных с программно-аппаратными ресурсами, работающими на нижних уровнях [4]. Очевидно, что в случае сбоев или отказов оборудования либо операционной системы (ОС) прикладное ПО, работающее уровнем выше, в свою очередь, тоже либо не будет работать вообще, либо будет работать нестабильно.

Основные причины нарушения работоспособности прикладного ПО:

- сбои и отказы компонентов ИИ, находящихся ниже по уровню;
- ошибки и недоработки в ПО;
- несовместимость компонентов прикладного ПО между собой либо же с ОС или оборудованием.

Главным тезисом данного раздела является констатация факта, что ПО с каждым годом усложняется, кроме того, увеличивается количество наименований разнообразного ПО. Для подтверждения данного факта был проведен соцопрос на тему: «Изменилось ли количество наименований ПО, используемого Вами, за последние 10 лет?». Респондентам предлагалось

самостоятельно выбрать, к какой категории пользователей информационных технологий они себя относят:

- пользователь офисного прикладного программного обеспечения;
- пользователь специализированного программного обеспечения;
- ИТ-профессионал – «эксплуататор»;
- ИТ-профессионал – «разработчик» (системный программист).

Данным соцопросом было охвачено 94 респондента, из них по 30 относят себя к одной из первых двух категорий, 22 – к третьей, а 12 – к четвертой.

В результате соцопроса выяснилось, что количество наименований ПО, используемых первыми двумя группами, а также четвертой группой, существенно увеличилось. В третьей группе мнения разделились, но ни один из респондентов этой группы не указал в ответах, что количество наименований ПО, которым он пользуется для работы, существенно уменьшилось (рис. 1).

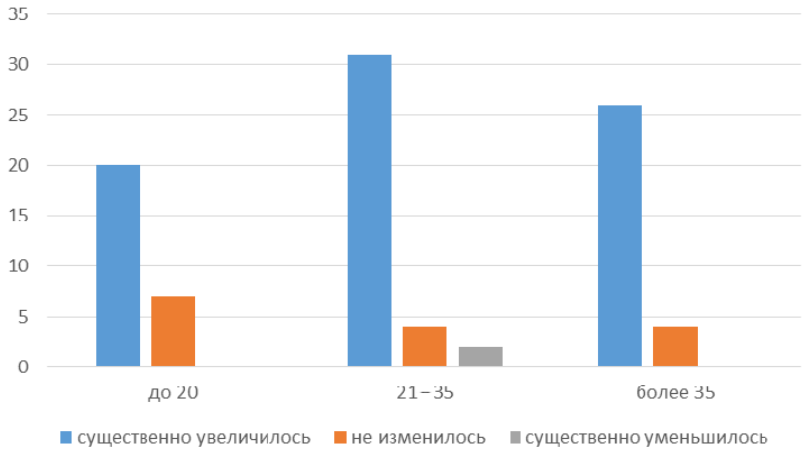

Рис. 1. Динамика изменения количества ПО в зависимости от группы пользователей

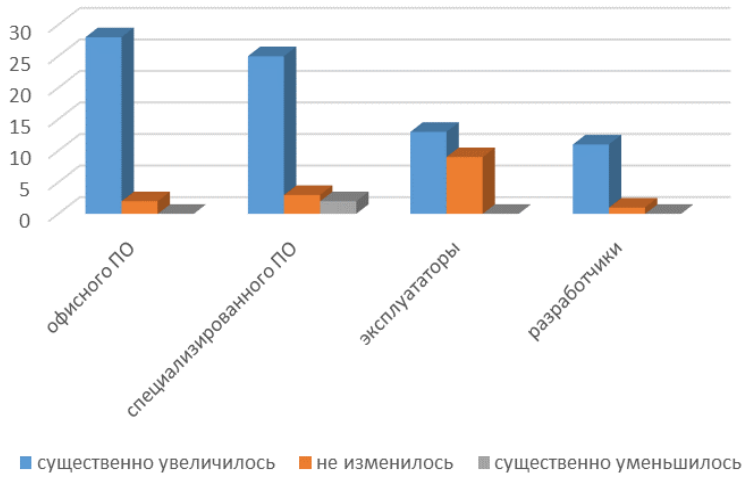

Рис. 2. Динамика изменения количества ПО в зависимости от возраста пользователей

Также интересно взглянуть на данные об изменении количества наименований используемых программ за последние 10 лет, в зависимости от возраста респондентов (рис. 2).

Программисты не всегда могут достоверно знать, в каком окружении будет использоваться их продукт, так как не может существовать двух совершенно одинаковых вычислительных машин (как в плане оборудования, так и в плане конфигурации программного обеспечения). В технике считается вариантом нормы ситуация, при которой программа не устанавливается или не запускается с первого раза после установки, а в результате повторения пользователем тех же самых действий успешный запуск все-таки осуществляется. Причем поиск причины такого поведения ПО не всегда может выявить сколь-нибудь конкретную проблему.

Казалось бы, теоретически таких ситуаций в исправных ОС возникать не должно, но функционирование современного ПО весьма сложное и не всегда предсказуемое. В качестве примера возьмем семейство ОС «Windows». На двух компьютерах практически не может быть одинаковых версий системного реестра. В системном реестре, кстати, за период работы компьютера может образоваться большое количество взаимоисключающих значений ключей (особенно характерно это для компьютеров, пользователи которых часто устанавливают и потом удаляют прикладное ПО).

Примерно аналогичная ситуация с состоянием динамических системных библиотек (.DLL) – многие прикладные программы, устанавливаемые на компьютер, стремятся внести изменения в уже существующие динамические библиотеки. Содержимое данных библиотек будет зависеть не только от того, какие конкретно программы устанавливались, но и от последовательности их установки и некоторых других факторов.

В некоторых случаях неудачный запуск или зависание ПО можно объяснить особенностями работы механизма доступа к используемым файлам в «Windows» (файл может использоваться одновременно только одним приложением, второе в очереди приложение получит к нему доступ после «закрытия» предыдущим).

Кроме того, на одинаковых платформах могут быть различные настройки (причем это относится как к оборудованию, так и к ПО). Данный аспект может влиять не только на доступность саму по себе, а еще на правильность отображения доступной информации.

Еще один аспект – повсеместно применяемое в настоящее время шифрование. Время от времени системы не могут «договориться» об используемых для конкретной сессии связи протоколах шифрования, что, разумеется, также нарушает доступность систем пользователей.

Доступность сетевых сервисов. Характерной особенностью подавляющего большинства современных корпоративных сетей передачи данных является комплексное использование большого числа разнообразных аппаратно-технических средств. Они различаются своими характеристиками, производительностью, аппаратными платформами и базовыми технологиями. Подобное разнообразие объясняется несколькими причинами:

- аппаратура приобреталась в разное время;
- ее подключение производилось разными специалистами, использовавшими различные технологии построения информационной сети;
- при соединении нескольких ранее разобщенных корпоративных сетей происходит существенное изменение топологии.

Указанные обстоятельства порождают ряд серьезных проблем для обеспечения информационной совместимости и доступности ИС, функционирующих в сетях передачи данных. Современные крупные распределенные системы с учетом условий их эксплуатации, а также потенциальных проблем их функционирования предъявляют серьезные требования к обеспечению безопасности. Во-первых, эти системы должны «выдерживать» радикальные изменения направлений развития. Во-вторых, они должны быть достаточно гибкими и допускать контроль своего поведения в сложных условиях эксплуатации.

С задачами защиты доступности тесно связана проблема обеспечения безопасности сети в целом и отдельных ее компонентов. Техническая сторона обеспечения ИБ базируется на использовании специального оборудования (например, сетевых экранов) и программных средств (например, средств антивирусного контроля).

Существуют также специальные протоколы (например, SNMP) для сбора информации о доступности сетевого оборудования, благодаря которым можно своевременно обнаружить ее нарушения. При этом надо иметь в виду, что с помощью данного специализированного протокола проверяются далеко не все аспекты работоспособности, поэтому возможны даже парадоксальные, на первый взгляд, ситуации, в которых доступность есть, а работоспособности, по сути, нет.

Организационная сторона определяется рядом нормативных документов (международных, национальных и ведомственных), задающих политику безопасности корпоративной сети, которая определяет комплекс мероприятий, направленных на обеспечение функционирования сети круглый год, 7 дней в неделю, 24 часа в сутки. Мероприятия должны проводиться на постоянной основе, в режиме, не препятствующем нормальному рабочему процессу.

Безопасность ИИ должна обеспечиваться всеми ее субъектами, в том числе и абонентами сети, которые должны отвечать за корректное использование сетевых служб, а также за своевременное оповещение администраторов о замеченных запрещенных действиях в сети [4].

Основными причинами нарушения работоспособности сетевых сервисов являются:

- сбои и отказы компонентов ИИ, находящихся ниже по уровню;
- ошибки и недоработки реализации сетевых сервисов;
- отключение по «непонятным» причинам работоспособных сервисов (например, из-за переполнения сокетов из-за множества незавершенных запросов);
- несовместимость сетевых сервисов между собой и другими компонентами ИИ.

Необходимо отметить также и «риск величины», связанный с увеличением размера и сложности информационной инфраструктуры (ИИ), используемой современным обществом. В очень больших ИС возникают явления, которые достаточно сложно однозначно объяснить сколь-нибудь адекватной конкретной причиной [1].

Доступность на уровне платформы. В качестве платформ будем рассматривать программно-аппаратные ресурсы, состоящие из сочетания оборудования и работающей на нем ОС, а также системы управления базами данных (СУБД). Кроме того, в понятие о платформе входят технические средства, непосредственно осуществляющие запись, хранение и последующее считывание данных. Сюда будут относиться дисковые носители серверов и рабочих станций, системы хранения данных (СХД), а также различного рода устройства резервного копирования [4].

Скорость восстановления информации после потерь, связанных со сбоями, отказами или другими причинами, зависит от того, существует ли резервная копия данной информации, а также, в случаях, когда существует, на какого рода носителе она записана. Например, восстановление информации со стриммерной ленты занимает значительное время и зачастую сопряжено с необходимостью частичной или полной остановки ИС. В случаях, когда в ИИ для хранения информации используются RAID-массивы (или похожие по смыслу системы), перерывов в работоспособности в подавляющем количестве случаев не происходит. В данном примере необходимо отметить, что дисковые массивы, организованные по RAID-технологии, как правило, являются довольно дорогостоящими, но при необходимости высокого коэффициента готовности системы и большой стоимости информации, которая в ней хранится, затраты на внедрение данных технологий оправданы. При этом надо также понимать, что RAID-массивы в целом защищают информацию в основном от чисто физических неисправностей (связанных, например, с износом) носителей. Программные логические ошибки нарушат сразу все копии данных на носителях RAID-массива. Поэтому в организациях целесообразно использовать несколько разных технологий защиты данных от потерь, что опять же сопряжено с дополнительными затратами материальных средств.

Основными причинами нарушения работоспособности на уровне платформы являются:

- сбои и отказы компонентов ИИ, находящихся ниже по уровню;
- ошибки и недоработки реализации оборудования и системного ПО;
- несовместимость оборудования и системного ПО между собой и другими компонентами ИИ.

Оборудование и системное ПО постоянно усложняются, в них добавляются все новые и новые функции. Каждая новая или модернизированная старая функция подразумевает усложнение программного кода и / или аппаратной части устройства.

Надо отметить, что на современном этапе развития информационных технологий сложно найти электронное изделие, изготовленное «с нуля», без использования уже готовых компонентов оборудования или ПО. Например, процессоры фирмы «Intel» для персональных компьютеров из поколения в поколение наследуют систему команд, которая постоянно модифицируется, оставаясь совместимой с ПО предыдущих поколений. Что характерно, архитектура каждого следующего поколения процессоров сильно меняется. При этом появились еще и «клоны» данной архитектуры у других производителей процессоров.

ОС разных производителей, так или иначе, пишутся не «с чистого листа», а уже на базе ранее разработанных программ. Скажем, ОС для мобильных устройств Android в качестве ядра использует Linux; ОС для компьютеров фирмы «Apple» под названием «MacOS», по сути, представляет собой BSD с модифицированной графической оболочкой (а BSD, с свою очередь, основывается на BSDi 4.4 и т. д.).

То же можно сказать в принципе о любых видах оборудования и ПО. Так, любой интерпретатор и компилятор современного языка программирования написан на ранее появившемся языке (обычно более низкого уровня). Да и интерпретаторы более ранних языков оказываются, в свою очередь, созданными на базе языка Ассемблера, который также написан на языке машинных кодов, имеющем еще более низкий уровень.

Для создания прикладного ПО в настоящее время вообще практически не используются языки программирования низкого уровня (если только для небольших «ассемблерных вставок»). Это обусловлено как сложностью современного прикладного ПО (и, следовательно, практической невозможностью досконально разрабатывать его на языке низкого уровня), так и системами безопасности ОС, которые не дают приложениям прямого доступа к ресурсам процессора, памяти и портов. Можно даже сформулировать такой тезис: чем современнее и совершеннее ОС, тем более закрыта от пользовательских приложений ее «внутренняя кухня» (т. е. механизм пропуска задач, работа с памятью, портами и т. д.).

Из вышеупомянутых примеров следует, что, по сути, нет ни одного человека, который бы досконально представлял, каким образом работает та или иная система. Оборудование разрабатывается одними людьми, производится другими, программное обеспечение для этого оборудования пишется третьими, а интегрируются эти компоненты в ИИ снова другими коллективами людей. Таким образом, гарантировать стопроцентно безотказную работу ИИ невозможно. Благодаря тщательной разработке и соблюдению политик ИБ можно добиться лишь снижения вероятности сбоев и отказов ИИ.

Доступность сервисов и служб. В современных условиях платформа может быть предоставлена в виде сервиса. При этом появляется два вида доступности такой системы – локальная и сетевая. Система может быть вполне работоспособной, но не доступной по сети. В результате пользователи не смогут получить доступ к такого рода сервису, пока не будет обеспечен доступ к нему по сети.

В качестве еще одного варианта иллюстрации причин недоступности системы приведем случай, когда система виртуальных машин недоступна из-за того, что закончились свободные пользовательские лицензии на доступ. Пока не появятся свободные лицензии, с системой поработать не удастся, даже если в целом она работоспособна и к ней имеется доступ по сети.

На доступность влияет также и мощность ресурсов, которыми располагает организация. ИИ у организации может быть собственной или отданной на «аутсорсинг». Например, известно, что в США крупным компаниям в большинстве случаев выгоднее иметь собственную ИИ, а малым и средним – отдавать на «аутсорсинг». В России ситуация аналогичная.

Обеспечение доступности информационных ресурсов в зависимости от обстоятельств внешней среды

Любое компьютерное оборудование требует определенных благоприятных физических условий (температуры, давления, влажности, а также ограничения уровней электромагнитных помех, запыленности, ударов и вибраций) [4]. Компьютерное оборудование рассчитано на исправную работу в весьма узком диапазоне условий.

Основные физические внешние факторы, оказывающие влияние на работоспособность ИИ:

- давление;
- запыленность;
- температура;
- влажность;
- освещенность;
- проникающие излучения;
- электропитание;
- химическая активность (агрессивность) окружающей среды;
- вибрационные помехи, физические перегрузки;
- электромагнитные помехи.

Кроме указанных внешних факторов, которые связаны с физическими условиями среды эксплуатации, существует масса других аспектов, от которых также зависит работоспособность систем и доступность информации.

От экономических ресурсов при проектировании, создании и эксплуатации ИИ зависит, каким конкретно образом и с помощью каких программно-технических средств будет организована работа ИИ. Например, ширина каналов связи между элементами системы, а также между эксплуатируемыми ИС и локальной или глобальной сетью, из которой пользовательское ПО осуществляет доступ к информационным ресурсам, будет иметь определяющее значение при увеличении количества одновременных попыток удаленного доступа к ИС. Следовательно, чем больше ширина канала передачи данных, тем, при прочих равных условиях, выше его стоимость.

В качестве примера системы, разработчики которой имеют большой опыт разработки и эксплуатации систем с высоким показателем доступности, можно привести поисковую и почтовую системы компании «Google». Пользовательские данные продублированы на серверах «Google» несколько сотен раз, пользователь чаще всего получает информацию с ближайшего к нему сервера с максимально возможной скоростью. Если ближайший к пользователю сервер будет недоступен в момент запроса сервиса, то информация будет использоваться с одного из множества других аналогичных серверов. Таким образом достигается избыточность дублирования данных, реализация которой, естественно, требует вложений очень существенных материальных средств.

Как уже упоминалось, надежность функционирования систем также зависит от их общего размера. Чем больше система, тем она сложнее и, как правило, неоднороднее. В больших ИИ начинают происходить процессы, которые сложно объяснить. При этом для больших систем действует принцип Ле Шателье – Брауна, подразумевающий, что большую систему можно перевести из одного состояния в другое только маленькими воздействиями, а если воздействовать ударно – она возвратится обратно в свое нормальное состояние.

Имеются в обеспечении доступности и явно нетехнические аспекты. Важно, чтобы сервис был не просто доступен, но еще и выдавал «правильную» информацию. Например, в общеизвестной и широкодоступной «Википедии» содержатся, в том числе, статьи, смысл которых искажен или полностью не соответствует общепринятым представлениям о действительности. Еще одним классическим примером выдачи некорректной информации можно считать прогноз погоды, который зачастую не оправдывается в реальности.

Заключение

Итак, обеспечение доступности – это, прежде всего, поддержка функционирования системы или сервиса. Вопрос обеспечения доступности в основном касается организационных мероприятий. Доступность информации является также важным свойством ИБ. Поддержка доступности информации определяется правильным функционированием компонентов ИИ, их правильным администрированием, соответствием интерфейсов ПО друг другу и требованиям оборудования, а также «портабельностью» ПО (правильностью функционирования в нужной операционной среде).

Обеспечение доступности информации в ИИ предприятий и организаций возможно только при эффективно разработанной и соблюдаемой политике обеспечения доступности информации. Причем данная политика имеет очень тесную связь с другими политиками ИБ и ее эффективное применение в отсутствие, например, политики мониторинга инфраструктуры невозможно.

Список литературы

1. *Мазов Н. А., Ревнивых А. В., Федотов А. М.* Классификация рисков информационной безопасности // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2011. Т. 9, вып. 2. С. 80–89.

2. *Ревнивых А. В., Федотов А. М.* Обзор политик информационной безопасности // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2012. Т. 10, вып. 3. С. 66–79.

3. *Ревнивых А. В.* Подходы к онтологизации политик информационной безопасности // XIV Рос. конф. с международным участием «Распределенные информационные и вычислительные ресурсы» (DICR-2012).

4. *Ревнивых А. В., Федотов А. М.* Мониторинг информационной инфраструктуры организаций // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2013.

5. *Муханова А. А., Ревнивых А. В., Федотов А. М.* Классификация угроз и уязвимостей информационной безопасности в корпоративных системах // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2013. Т. 11, вып. 2. С. 55–72.

Материал поступил в редколлегию 25.03.2014

A. V. Revnivykh, A. M. Fedotov

AVAILABILITY OF RESOURCES IN INFORMATION-PROCESSING SYSTEMS

This paper describes the basic principles of protection against violations of availability of resources in information systems, and also corresponding the policies of information security in modern information-processing system.

Keywords: information security, information security policy, availability of information resources, system profiles.