УДК 004.056

А. В. Ревнивых, **А. М. Федотов**

Новосибирский государственный университет
ул. Пирогова, 2, Новосибирск, 630090, Россия

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

E-mail: alexchr@mail.ru; fedotov@nsu.ru

МОНИТОРИНГ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИИ [*]

Работа посвящена описанию основных принципов и классификации задач мониторинга функционала информационной инфраструктуры организации, а также политик информационной безопасности, связанных с мониторингом.

Ключевые слова: информационная безопасность, мониторинг информационной инфраструктуры, надежность информационных систем, профили системы, политики информационной безопасности.

Введение

Надежный мониторинг информационной инфраструктуры (ИИ) особенно критичен в крупных организациях, таких как Новосибирский государственный университет, где один человек чисто физически не способен уследить за всеми программно-аппаратными и организационными компонентами инфраструктуры (и нет ни единого человека, который бы до конца представлял себе в каждый момент времени состояние ИИ полностью). Поэтому важно учитывать необходимость мониторинга при разработке и внедрении политики информационной безопасности (ИБ).

В последние годы в организациях стала популярной практика аутсорсинга ИИ (например, «облачной», виртуализированной). Особенно это удобно небольшим организациям – это избавляет их от необходимости создавать собственную полноценную ИИ и, что немаловажно, в дальнейшем следить за ее состоянием и работоспособностью. В организации-заказчике услуги, по сути, в том или ином виде остаются только кабельные соединения (или беспроводные сети) и автоматизированные рабочие места, что позволяет упростить выполнение политик ИБ в целом и отказаться от большей части мероприятий по поддержанию ИИ в работоспособном состоянии. Хотя и этот подход имеет свои особенности с точки зрения ИБ, так как важная для организации информация передается внешним исполнителям.

Качественная реализация мониторинга ИИ позволяет руководству организаций принимать своевременные и эффективные управленческие решения, в том числе по основному направлению деятельности своих организаций.

[*] Работа выполнена в НГУ при финансовой поддержке Министерства образования и науки Российской Федерации (договор № 02.G25.31.0054).

Ревнивых А. В., Федотов А. М. Мониторинг информационной инфраструктуры организации // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2013. Т. 11, вып. 4. С. 84–91.

Базовые понятия мониторинга информационной инфраструктуры организаций

В объем и содержание понятия о мониторинге ИИ включаются наблюдение, слежение за состоянием ИИ в целом и ее компонентов в частности. Мониторинг является составной частью политик ИБ – наборов правил для обеспечения ИБ [1; 2].

Мониторинг представляет собой процесс наблюдения и регистрации параметров объекта в соответствии с определенными заранее установленными критериями. В процессе мониторинга может также предусматриваться сбор статистики. Например, имеет смысл регистрировать и записывать факты обращения пользователей к информационным ресурсам. При этом в качестве пользователя может выступать не только человек, но и программное приложение. Собранную таким образом статистику можно использовать для принятия решения о целесообразности поддержки каждого конкретного информационного ресурса.

Целью мониторинга ресурсов является своевременное получение информации о текущем состоянии ИИ в целом или каких-то конкретных ее частей (например, отдельных информационных систем (ИС)), а также для констатации факта соответствия или отличия текущего состояния ИБ правилам, заданным в политиках ИБ организации. Под состоянием будем понимать множество стабильных значений переменных параметров некого объекта. Анализ данной информации необходим для выработки эффективной и своевременной реакции на события, происходящие в ИИ, или факты, связанные с ее функционированием.

Принимая во внимание высокую ценность сетевых ресурсов (в первую очередь пропускной способности внешних и внутренних каналов передачи данных и сетевых узлов организаций), следует, прежде всего, обеспечить возможность оперативного и ретроспективного анализа нерегулярностей и аномалий. Одной из основных задач этой технологии является своевременное обнаружение нерегламентированных действий в сети, таких как сетевые атаки и нелегальное использование ресурсов. Для этого необходимо осуществлять мониторинг сетевого трафика и проводить идентификацию различных сетевых приложений и сервисов, а также анализировать особенности их функционирования.

Таким образом, система мониторинга должна также рассматриваться, как важная компонента системы обеспечения безопасности компьютерной сети, лежащей в основе ИИ [3; 4].

Мониторинг имеет смысл настраивать, исходя из функциональных требований к работоспособности ИИ и ее компонентов.

ИИ предприятий можно представить состоящей из компонентов трех основных уровней: физического, транспортного и прикладного. Здесь вполне уместна некоторая аналогия с сетевой семиуровневой моделью ISO/OSI [5], но уровней вполне достаточно выделить три:

- на физическом уровне ИИ находятся аппаратные средства серверов, рабочих станций, кабельные сети, сетевое оборудование, а также внешние условия эксплуатации ИИ (давление, температура, запыленность и т. д.);
- транспортный уровень ИИ предполагает наличие сетевого оборудования и программного обеспечения. Сюда же относятся программные и аппаратные средства для поддержки сетевых протоколов (в соответствии с базовой моделью ISO/OSI), сервисы, сетевые кабели, маршрутизаторы, коммутаторы, концентраторы, модемы и т. д.;
- на прикладном уровне ИИ находятся разнообразные программно-аппаратные ИС, системное и прикладное ПО рабочих станций пользователей и т. д.

Так как задача мониторинга состоит, прежде всего, в проверке функционала, который обеспечивает система, а уж потом – отдельных узлов, то в современных ИИ преимущественно уделяют внимание мониторингу логического состояния ресурсов, изредка принимая во внимание физические аспекты – обычно лишь для выяснения причин сбоя или отказа, что чаще всего уже не является этапом непосредственно мониторинга.

Функции информационной инфраструктуры организаций

Назначение ИИ с принципиальной точки зрения и очень обобщенно можно считать следующим:

1) сбор и регистрация информационных ресурсов;

2) хранение информационных ресурсов;
3) актуализация информационных ресурсов;
4) обработка информационных ресурсов;
5) предоставление информационных ресурсов пользователям [6; 7].

Для предоставления данного функционала 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) обработчики и хранилища данных.

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.

Каждый из этих основных компонентов ИИ нуждается в мониторинге по определенным критериям, которые для каждого из компонентов индивидуальны.

Критерии мониторинга функционала компонентов информационной инфраструктуры

В тех случаях, когда это возможно, имеет смысл выстраивать критерии для проверки функционала ИИ в таком порядке, чтобы имело смысл регулярно мониторить только один (обычно первый) критерий. Тогда следить за состоянием остальных критериев необходимо лишь в тех случаях, если найдены отклонения по первому.

Подобного рода подход можно использовать к модулям ИИ. Каждый модуль за что-нибудь отвечает, например, есть модули, решающие основную задачу ИИ, есть же служебные (например, модуль резервного копирования).

Критерии мониторинга 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. Современные операционные системы (ОС) в основном ограничивают полномочия прикладного ПО в плане его влияния на функционирование ОС, а также сторонних прикладных программ. При этом ОС имеют возможность самостоятельного мониторинга своего состояния и могут информировать о нем пользователей – это функции самой системы.

Мониторинг функциональности прикладного ПО связан с проверками работоспособности, производительности, наличия всех необходимых для правильного функционирования библиотек и других ресурсов, а также согласования версий ПО.

1.1. Нет ли слишком длинных тайм-аутов в работе модулей программы? Не влияют ли эти тайм-ауты на комфортность использования программы пользователем?
1.1.1. Отзывается ли интерфейс на управляющие воздействия?
1.1.2. Не «висит» ли прикладная программа?
1.1.3. Загрузка программного сетевого интерфейса?
1.2. Доступен ли пользователю интерфейс?
1.3. Доступен ли программный сервис?
1.4. Запущена ли прикладная программа?
1.4.1. Имеются ли необходимые и совместимые сервисы (библиотеки, системные программы, макросы, кодеки и т. д.) на стороне сервера, актуальна ли их версия? Вообще есть ли система, в которой можно запуститься?

1.4.2. Имеются ли необходимые и совместимые сервисы (библиотеки, прикладные программы) на стороне клиента, актуальна и совместима ли их версия?

Критерии мониторинга 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 безопасности 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.

Комплекс ИБ крупной сети передачи данных должен работать надежно и без сбоев, выполняя свои основные задачи, а именно обеспечивать:

- защиту от несанкционированного доступа к информационным ресурсам;
- своевременное выявление угроз и атак (как внутренних, так и внешних);
- выявление потенциально слабых и незащищенных мест сети;
- контроль над соблюдением корпоративного регламента;
- выявление скрытых, зашифрованных сообщений, передаваемых под видом легитимного трафика.

С задачами мониторинга тесно связана проблема обеспечения безопасности сети в целом и отдельных ее абонентов. 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 работоспособности сетевого оборудования.

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 [3].

Сетевые сервисы, критерии для оценки работоспособности которых приведены ниже, работают на разных уровнях модели ISO/OSI и, очевидно, обеспечиваются совместным функционированием множества программно-аппаратных компонентов.

2.1. Корректны ли реакции сетевого сервиса на управляющие воздействия (несколько запросов с заранее известным правильным результатом)?

2.2. Доступен ли сетевой сервис?

2.3. Доступны ли сетевые сервисы, без которых этот не может работать (например, для сервиса проксирования трафика необходим работоспособный сервис DNS, зачастую DHCP и т. д.)?

2.4. Отзывается ли сетевой интерфейс на управляющие воздействия (например, на ICMP-пакеты, отправленные PING'ом)?

2.5. Есть ли связь с нужным направлением сети или подсетью (например, с Интернетом)?

2.6. Имеется ли связь в сторону клиента?

2.7. Запущены ли на стороне клиента необходимые сервисы (библиотеки, прикладные программы, кодеки и т. д.)? Совместимы ли их версии?

2.8. Нет ли аномальной сетевой активности (для того чтобы судить об аномальности сетевой активности, необходимо иметь данные за предыдущие этапы эксплуатации системы и сравнивать их с текущими значениями – при большой разнице между тем, что было, и тем, что есть, делаем выводы об аномальном режиме работы)?

2.8.1. Общее количество сетевого трафика по размеру и по количеству пакетов.

2.8.2. Появление пакетов такого типа, которого раньше не было.

2.8.3. Длительное отсутствие пакетов такого типа, пакеты которого до этого в трафике регистрировались регулярно.

2.8.4. Коэффициент сегментированных пакетов.

2.8.5. Большое количество пакетов в новом направлении.

2.8.6. Длительное отсутствие пакетов в том направлении, в котором они регулярно отправлялись.

2.8.7. Попытки несанкционированного доступа к информации.

Критерии мониторинга обработчиков и хранилищ данных. В качестве «обработчиков данных» будем рассматривать программно-аппаратные ресурсы, состоящие из сочетания оборудования и работающей на нем операционной системы (ОС) и системы управления базами данных (СУБД). Обычно сочетание этих компонентов называют «платформой».

В первую очередь необходимо следить за функциональностью ОС, но в некоторых случаях требуется мониторинг состояния оборудования.

В данном разделе под термином «хранилища данных» будем понимать технические средства, непосредственно осуществляющие запись, хранение и последующее считывание данных. Сюда относятся дисковые носители серверов и рабочих станций, системы хранения данных (СХД), а также различного рода устройства резервного копирования.

Отметим, что современное ПО может осуществлять проверку аппаратных компонентов в автоматическом режиме. Например, в ОС есть средства диагностики исправности аппаратных средств.

3.1. Корректно ли работают сервисы ОС, сетевые сервисы (несколько тестов с заранее известным правильным результатом)?

3.2. Какие ошибки выдает операционная система?

3.3. Запущена ли операционная система?

3.4. Есть ли возможность запустить операционную систему?

3.5. Правильно ли выдается ранее записанная информация?

3.5.1. Тест на запись / чтение информации.

3.6. Есть ли доступ к чтению / записи информации?

3.7. Подключен ли носитель информации к системе?

3.8. Исправно ли оборудование?

3.8.1. Скорость вращения электродвигателей кулеров.

3.8.2. Температура с датчиков.

3.8.3. Закрыт ли корпус?

3.8.4. Напряжение на основных компонентах.

3.8.5. Контакт с основными компонентами.

3.8.6. Ошибки памяти.

3.9. Исправен ли носитель информации?

3.9.1. Ошибки считывания информации с носителей.

3.9.2. Износ жестких дисков с датчиков.

3.10. Скорость доступа к данным?

3.10.1. Скорость носителей информации.

3.11. Производительность платформы (проверяется тестовыми прикладными программами).

3.11.1. Процессоров.

3.11.2. Памяти.

3.11.3. Сетевых интерфейсов.

3.12. Нет ли «лишних» активных программ в памяти (как в целом полезных, так и заведомо вредоносных)?

3.13. Имеется ли актуальная и корректная резервная копия данных?

3.14. Есть ли «свободное» место на носителях?

Мониторинг внешней среды и отдельных компонентов информационной инфраструктуры

Как уже упоминалось, мониторинг имеет смысл, в первую очередь, выстраивать от функционала ИИ. Проверкам в основном подлежит логическое состояние ресурсов. Но в целях раннего предупреждения потенциальных проблем в работе ИИ, а также для первичной диагностики причин изменения логического состояния ресурсов имеет смысл внедрять и слежение за состоянием внешней среды и отдельных компонентов ИИ. Сама по себе диагностика не входит в политики мониторинга, но сбор первичной информации для диагностики немыслим без слежения за программно-аппаратными компонентами ИИ и состоянием внешней среды.

Политика мониторинга ИИ должна рассматриваться в сочетании с другими политиками ИБ. В конечном счете контроль за исполнением всех политик ИБ осуществляется средствами мониторинга.

Способы мониторинга можно классифицировать на два основных типа: автоматизированный (программно-аппаратный) и неавтоматизированный. При этом полностью автоматизированного мониторинга всех аспектов работы ИИ добиться практически невозможно, так как нельзя предсказать абсолютно все варианты событий, происходящих в ИИ и вызывающих определенные реакции системы мониторинга.

Кроме того, во многих случаях бороться за полную автоматизацию системы мониторинга нет смысла, так как реакция на некоторые ее сообщения так или иначе будет связана с вмешательством человека, например, для устранения аппаратных проблем, скажем, в системе охлаждения серверной.

Неавтоматизированный способ мониторинга предполагает непосредственное участие человека на всех этапах этого процесса, автоматизированный – основан на применении в качестве «органов чувств» различного рода сенсоров, а также автоматизированной интерпретации их показаний программно-аппаратными средствами.

Любое компьютерное оборудование требует определенных благоприятных физических условий (температуры, давления, влажности, а также ограничения уровней электромагнитных помех, запыленности, ударов и вибраций). Для слежения за внешней средой используются соответствующие сенсоры (датчики), которые обычно размещаются в помещении, где находятся компоненты ИИ. В качестве инструмента также может быть использована система видеонаблюдения.

Мониторинг ресурсов подаппаратного уровня можно разделить на два аспекта: мониторинг наличия определенных ресурсов, относящихся к подаппаратному уровню, а также состояния этих ресурсов.

Наличие подаппаратных средств проверяется по результатам интерпретации данных, поступающих от взаимосвязанных с проверяемыми устройств подаппаратного, аппаратного и программно-аппаратного уровней.

Информацию о состоянии подаппаратных средств оператор получает в основном в результате интерпретации сигналов, поступающих от встроенных в эти устройства датчиков и сенсоров. Интерпретация данных, полученных с взаимосвязанных устройств, также может быть источником информации о состоянии подаппаратных средств. Например, повреждение кабеля, соединяющего два узла локальной сети, можно диагностировать в случае, если между этими двумя узлами сети нет физического соединения. При этом важно отметить, что в подобного рода случаях повреждение кабеля является далеко не единственной возможной причиной отсутствия физической связи между узлами сети.

Мониторинг наличия и состояния ресурсов аппаратного уровня производится как за счет встроенных в них датчиков, так и с помощью интерпретации результатов диагностики взаи-

мосвязанных ресурсов подаппаратного, аппаратного, программно-аппаратного и прикладного уровней. Кроме того, в некоторых случаях возможны и неавтоматизированные (ручные) проверки. Например, температура в системном блоке персонального компьютера проверяется как встроенными в материнскую плату датчиками, так и вручную – прикоснувшись к корпусу системного блока или компонентам компьютера (скажем, к процессору или блоку питания), человек-оператор может сделать вывод о неисправности системы охлаждения (в случае, если почувствует избыточное тепло). Кроме того, на примере системы охлаждения персонального компьютера, в состав которой часто входят вентиляторы (кулеры), можно показать, что визуальный контроль тоже является эффективным методом в некоторых случаях (если вентилятор блока питания неподвижен – почти наверняка что-то неисправно и в какой-то момент может перегреться).

Мониторинг профилей системы и кадровых ресурсов

Важной задачей мониторинга является слежение за актуальностью профилей системы, так как любая ИИ должна работать в соответствии с документацией. Если вовремя не актуализировать саму документацию, то работа ИИ быстро перестанет соответствовать нормативным документам.

Кадровая политика организации должна предусматривать санкции за невыполнение требований политик ИБ, а также подбор и поощрение сотрудников с соответствующей квалификацией и личными качествами. Безусловно, политика мониторинга ИИ организации имеет связь с кадровой, так как для качественного создания и последующего соблюдения политики мониторинга нужны сотрудники с соответствующими личностными и деловыми качествами, а также продуманная система мотивации и демотивации.

Слежение за деятельностью сотрудников организации осуществляется в соответствии с политикой мониторинга кадровых ресурсов. Например, именно с помощью средств, предусмотренных в политике мониторинга, выявляются нарушения, связанные с матрицей доступа сотрудников к ресурсам ИИ, с изменениями в матрице доступа (например, при переходе сотрудников с одной должности на другую, приеме новых сотрудников на работу, увольнении, отбытии в длительный отпуск или на лечение и т. д.).

В соответствии с политикой мониторинга кадровых ресурсов производятся проверки, в том числе за исполнением мер по мотивации и демотивации сотрудников.

Заключение

Мониторинг обеспечивает своевременное информирование оператора о событиях, происходящих в системе, а также предоставляет ему возможность вовремя принять эффективное решение по реакции на эти события.

Итак, мониторинг – это слежение за состоянием компонентов ИИ на трех уровнях (физическом, транспортном и прикладном) и статистика (журналирование, протоколирование).

Взаимодействие с ИИ в контексте мониторинга предполагает следующие этапы:

1) обнаружение некоторого события;
2) первичная интерпретация произошедшего события, классификация по области знаний и степени важности;
3) выработка вариантов реакции на данное событие;
4) выбор варианта реакции на событие;
5) реакция на событие.

В качестве способов реакции на возникшие факты или события может быть бездействие (чаще всего это отсутствие каких-либо действий, кроме занесения информации о возникшей ситуации в протоколы работы) или формирование и отправка соответствующего информационного сообщения определенному набору адресатов. Дальнейшая обработка событий (повторная интерпретация, выработка вариантов реакции, выбор варианта реакции, реакция) – функция уже не системы мониторинга, а оператора, принявшего сообщение. Оператором при этом может быть как человек, так и ИС.

Список литературы

1. *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.

2. *Ревнивых А. В.* Подходы к онтологизации политик информационной безопасности // Распределенные информационные и вычислительные ресурсы (DICR-2012): Материалы XIV Рос. конф. с междунар. участием. Новосибирск, 2012.

3. *Федотов А. М., Молородов Ю. И.* Введение в Интернет и информационные технологии: Учеб. пособие. Новосибирск, 2008. Ч. 2: Структура и сервисы сетей Интернет.

4. *Белов С. Д., Жижимов О. Л., Федотов А. М., Осипов Г. С., Тихомиров И. А., Сочен-ков И. В.* Комплексная защита крупных корпоративных сетей передачи данных // Системный анализ и информационные технологии (САИТ-2009): Материалы III Междунар. конф. М., 2009. С. 20–29.

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

6. *Миндалев И. В.* Теория экономических информационных систем: Электрон. учеб.-метод. комплекс. Красноярск, 2006–2009.

7. *Кагаловский М. Р.* Перспективные технологии информационных систем. М.: Пресс; Компания АйТи, 2003. 288 с.

Материал поступил в редколлегию 03.12.2013

A. V. Revnivykh, A. M. Fedotov

MONITORING OF INFORMATION INFRASTRUCTURE OF THE ORGANIZATIONS

This paper describes the classification of information infrastructure monitoring policies in modern information-processing systems.

Keywords: information security, information security policy, infrastructure monitoring, system profiles.