Раздел VI
Стандарты и правовое регулирование информационной безопасности

А. Г. Додонов, Е. С. Горбачик, М. Г. Кузнецова
Украина, г. Киев, Институт проблем регистрации информации НАН Украины

ЖИВУЧЕСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ И БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В условиях глобализации компьютерные системы становятся компонентами сложных административных, экономических, военных, технических систем, различных систем управления. Постоянно растет зависимость жизнедеятельности общества от развития и эффективности использования средств передачи и обработки информации; информационный продукт приобретает характер общественного ресурса развития, масштабы его использования сопоставимыми с традиционными (энергия, сырье и т.д.) ресурсами. Информационная инфраструктура становится системообразующей, ее устойчивое и стабильное функционирование, безопасность являются необходимыми условиями существования современного общества.

Задача построения функционально устойчивой инфраструктуры, представляющей собой сложную систему, активно взаимодействующую с внешней средой и функционирующую в условиях действия случайных факторов, наличия неблагоприятных воздействий различной природы и высокой стоимости последствий нарушений функционирования, не может быть решена путем простого улучшение показателей надежности, отказоустойчивости или безопасности. Необходим новый подход, учитывающий изменчивость внешней среды, обеспечивающий адекватность реакции компонент инфраструктуры, гарантирующий выполнение требований по безопасности функционирования информационной инфраструктуры в целом, т.е. по существу, обеспечивающий живучесть этой сложной системы.

Обеспечение живучести всей инфраструктуры в целом – весьма сложная проблема, решение которой может потребовать затрат, сравнимых или даже превышающих затраты на непосредственно создание такой инфраструктуры. Повышение живучести отдельных критических компонент инфраструктуры, например, распределенных компьютерных систем, являющихся основой для организации и реализации процессов информационного взаимодействия, позволит заблокировать широкий класс средств и способов неблагоприятного воздействия, минимизировать возможности целенаправленного изменения, уничтожения, копирования, тиражирования, блокирования, модификации информационных потоков и данных; значительно снизит риск дезорганизации работы компьютерных систем и сетей путем воздействия на их системы защиты.

Проблемы безопасности компьютерных систем, как составной части информационной инфраструктуры, решаются на организационном, нормативно-правовом и программно-техническом уровнях. Методы обеспечения безопасности предполагают включение следующих этапов разработки и эксплуатации компьютерных систем:

1. Анализ архитектуры системы и используемых информационных технологий.

2. Выявление на основе проведенного анализа уязвимостей, через которые возможна реализация угроз безопасности.

3. Определение, анализ и классификация возникающих в компьютерных системах угроз:

- несанкционированного использования компьютерных ресурсов (угроз хищения, подлога, разрушения и потери информации, отказов в работе программно-аппаратных средств);
- некорректного использования компьютерных ресурсов (нарушений физической и логической целостности данных, нарушений работоспособности компьютерных систем);
- угроз проявления ошибок пользователей, операторов и администраторов, а также ошибок, допущенных в процессе разработки программно-аппаратных средств;
- безопасности сетевого взаимодействия (безопасности информационного обмена, а также нарушений протоколов взаимодействия);
- несанкционированного изменения состава компьютерной системы и ее компонент (изменений параметров конфигурирования, внедрения вирусоподобных программ и др. несанкционированных элементов);
- нанесения ущерба физическим способом (хищения носителей информации, нарушений системы электроснабжения);
- перехвата электромагнитных излучений и др.

4. Оценка имеющегося уровня компьютерной безопасности и определение рисков.

5. Разработка политики безопасности как совокупности концептуальных решений, направленных на эффективную защиту информации и ресурсов.

6. Формирование полного перечня детальных требований к системам компьютерной безопасности в соответствии с необходимыми классами защищенности.

7. Разработка проектов систем защиты информации с учетом предъявленных требований и возможных рисков.

8. Контроль за соблюдением норм компьютерной безопасности и правильностью функционирования систем защиты.

Распределенным компьютерным системам, как любой сложной системе, присуща определенная избыточность, адаптивность, отказоустойчивость и живучесть. Свойство живучести позволяет системе сохраняться как целому в условиях неблагоприятных (случайных или целенаправленных) воздействий, влекущих разрушение структуры, нарушение целостности, снижение безопасности и качества функционирования.

Живучесть – свойство сложной системы адаптироваться в изменяющихся условиях функционирования, противостоять неблагоприятным воздействиям и достигать цели функционирования за счет изменения поведения и структуры [1].

В качестве «неблагоприятных воздействий» рассматриваются возможные отказы, сбои и нарушения в работе аппаратного и программного обеспечения, различные атаки на систему, катастрофические воздействия природного или техногенного происхождения, причем важна не природа воздействия, а его последствия [4, 5].

Наличие свойства живучести и соответствующих механизмов его обеспечения позволяет иначе взглянуть на организацию безопасности, и, возможно, снизить затраты на ее поддержание. Традиционно повышение безопасности компьютерных систем и сетей основывается на усилении и усложнении систем их защиты либо отдельных их компонент. Разграничение доступа, фильтрация, аутентификация и другие средства защиты не позволяют в полной мере обеспечить безопасность на необходимом уровне на протяжении всего жизненного цикла компьютерной сис-

темы, т.к. постоянно возникают новые средства атак. Для контроля за новыми возникающими угрозами и своевременного и эффективного противодействия им необходимо реализовать возможность постоянного развития и усовершенствования средств поддержания безопасности. Введение адаптивной защиты не только сделает возможным устранение уязвимостей, но и позволит анализировать условия, способствовавшие их появлению. В случае возникновения неблагоприятного воздействия, в режиме реального времени, без остановки функционирования компьютерной системы, эти средства должны обеспечить реконфигурацию программного и аппаратного обеспечения, а также своевременно уведомить ответственных за безопасность специалистов о возникающих проблемах.

Наличие механизмов обеспечения живучести позволяет выбирать оптимальный относительно определенной цели (установленного объема функций) режим функционирования компьютерной системы при наличии неблагоприятных воздействий за счет внутренних ресурсов, перестройки структуры, изменения функций отдельных подсистем или, возможно, алгоритмов их функционирования. Учитывая, что неблагоприятные воздействия могут вызвать существенные изменения в поведении системы в целом или отдельных ее компонент, выбор поведения должен осуществляться в соответствие с изменениями внешних условий и функциональным инвариантом системы, который можно определить как внутреннюю цель функционирования [2]. Выбор предполагает наличие некоторого множества возможных различных следствий, объединенных общим свойством соответствия одной внешней причине в данных условиях. Следовательно, менять поведение могут только системы, в принципе исключающие жесткую связь внешней причины выбора с фактическим поведением системы в результате выбора (внешние причины вызывают следствия, которые не могут быть предсказаны однозначно).

При оценке живучести распределенных компьютерных систем различают функциональную, структурную и информационную живучесть. Под функциональной живучестью понимается способность системы при наличии неблагоприятных воздействий выполнять с заданным качеством заданную цель функционирования. Структурная живучесть – это способность системы поддерживать в неблагоприятных условиях системную структуру, необходимую для выполнения цели функционирования с заданным качеством. Информационная живучесть – способность системы поддерживать доступность, целостность и конфиденциальность информации на уровне, позволяющем выполнять с заданным качеством цель функционирования системы, независимо от внешних и внутренних неблагоприятных воздействий и нарушений в использовании информационных ресурсов. При рассмотрении живучести распределенных компьютерных систем предполагают наличие в той или иной степени функциональной, структурной и информационной живучести. Обеспечение и повышение живучести таких систем осуществляется развитыми механизмами распознавания, противодействия, восстановления, а также специальными средствами адаптации, реконструкции, реконфигурации и реорганизации [1 - 4].

Механизмами распознавания в системах выявляются атаки, успешные вторжения, повышение риска выхода из строя жизненно важных (критических) компонент систем, а также риска потери или искажения информации. Базой для организации механизмов распознавания являются методы диагностики. Средства идентификации, оповещения, регистрации событий, анализа шаблонов поведения пользователей интегрируются в механизмы распознавания при решении задач повышения живучести распределенных информационных систем.

Механизмы противодействия ориентированы на поддержку заданных условий функционирования и минимизацию потерь при переходе системы в нештат-

ный режим функционирования (при снижении качества функционирования, например, увеличении времени выполнения заданий, времени отклика; при переходе к новой цели функционирования). Механизмы противодействия основываются на методах резервирования, используют возможности средств архивирования, идентификации, авторизации, ограничения прав доступа пользователей, межсетевых экранов (технически отделяющих средства распределенных компьютерных систем от внешней среды).

Механизмы восстановления обеспечивают восстановление функциональности и работоспособности компонент системы и компьютерной системы в целом при наличии неблагоприятных воздействий или после их прекращения. Эти механизмы разрабатываются на основе целого спектра специализированных аппаратно-программных методов и средств восстановления. Стратегии восстановления информации, которые используются в распределенных информационных системах, предполагают репликацию критических информационных ресурсов и сервисов, использование отказоустойчивых архитектурных решений и специализированных средств поддержки процессов восстановления. Для восстановления информации требуется наличие сведений относительно изменений и дополнений информации, которая сохраняется или циркулирует в системе, использование надежных технологий хранения, наличие «процедур отката», чтобы гарантировать целостность или восстановление состояния информации до каких-либо конкретных изменений или неблагоприятных воздействиях.

Средства адаптации позволяют системе целенаправленно изменять параметры и структуру (на основе информации об изменениях в условиях функционирования, возникновении непредвиденных ситуаций, информации о последствиях нарушения защищенности информационного ресурса), корректировать функционирование соответственно сложившимся условиям и максимизировать эффективность функционирования.

К особым и достаточно дорогостоящим средствам обеспечения живучести, требующим специальной разработки еще на этапе проектирования системы, относятся средства реорганизации, реконфигурации и реконструкции. Процедуры реорганизации осуществляют перераспределение функций компонент системы, потерявших работоспособность, между работоспособными или, в случае невозможности перераспределения, переход к новой цели функционирования. Процедуры реконфигурации реализуют автоматическую перестройку структуры сети обмена информацией, обеспечивая достижение наибольшей эффективности выполнения цели функционирования на имеющихся работоспособных ресурсах компьютерной системы или сети. Процедуры реконструкции выполняют редукцию цели функционирования и ресурсов системы до некоторых базовых уровней, при этом система может выполнять только четко определенное минимальное множество функций или обеспечивается плавная деградация и безопасный останов системы.

Анализируя особенности информационной инфраструктуры, где используются распределенные компьютерные системы, следует отметить неограниченность сетевой среды, наличие как централизованного, так и децентрализованного административного управления, отсутствие в среде функционирования единой политики безопасности.

В неограниченной сетевой среде отсутствует возможность глобальной наблюдаемости; не всегда могут быть определены число и тип узлов (разнообразных аппаратно-программных комплексов), подключенных к сетям в любой момент времени; сложным является установление доверительных отношений между узлами в открытых системах; не существует средств жесткого разделения узлов на

«заслуживающих доверие» и «потенциально опасных». Следовательно, имеет место «естественная» неопределенность условий функционирования, т.е. постоянно возникают условия, в которых существенно наличие свойства живучести.

Это необходимо учитывать при разработке систем безопасности и строить защиту не в рамках классических методов защиты информации, на основе модели «крепости», по классической схеме «защиты от», а с учетом неопределенности условий функционирования, которая возникает при использовании глобальных сетей для передачи данных и организации удаленного доступа к информационным ресурсам, например, через Интернет, по схеме «что, если».

Такая схема организации защиты позволит не только отражать атаки и противостоять возникновению нештатных ситуаций, но и поддерживать нормальное функционирование распределенной компьютерной системы или осуществить безопасный останов без потери наиболее важных информационных ресурсов, или восстановить нормальное функционирование системы при возобновлении штатных условий.

Наличие разнообразных средств адаптации также дает возможность улучшить организацию систем безопасности за счет перехода на модель адаптивного управления безопасностью. Так называемые адаптивные компоненты уже сегодня используются в различных технологиях, поддерживающих политики сетевой безопасности, например, для усовершенствования подсистем выявления атак, анализа защищенности, поиска уязвимостей, для управления динамической реконфигурацией межсетевых экранов, маршрутизаторов, коммутаторов и других средств для отражения атаки в реальном масштабе времени.

Расходы на обеспечение живучести являются одновременно и расходами на повышение безопасности, т.к. наличие механизмов обеспечения живучести позволяет еще до анализа причин нарушения безопасности среагировать на неблагоприятное воздействие и перевести систему или ее отдельные ресурсы в безопасное состояние; значительно улучшить мониторинг системы; не прекращая функционирование, осуществлять реконфигурацию программного и аппаратного обеспечения, адекватную возникающим угрозам.

Разработку систем с учетом требований по живучести можно одновременно рассматривать как развитие и внедрение элементов принципиально новой системы безопасности, ориентированной на функционирование компьютерных систем в динамичной сетевой среде, формулируя задачу защищенности информации и технологий работы с нею не как задачу ограничения доступа к ресурсам, а как задачу прогнозирования критических ситуаций и ликвидации их последствий за счет гибкой адаптации структуры и поведения системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Додонов А.Г., Кузнецова М.Г., Горбачик Е.С.* Введение в теорию живучести вычислительных систем.– К.: Наук. думка, 1990. – 184 с.

2. *Додонов А.Г., Кузнецова М.Г., Горбачик Е.С.* Живучесть и надежность сложных систем. Методическое пособие. - Международный научно-учебный центр ЮНЕСКО/МПИ информационных технологий и систем, 2001. – 163 с.

3. *Додонов А.Г., Горбачик Е.С., Кузнецова М.Г.*, Современные технологии и проблемы информационной безопасности // Сб. научн. трудов «Информационные технологии и безопасность». – К.:ИПРИ НАН Украины, 2006. - Вып.9.– С.51–59.

4. *Robert J. Ellison*, *David A. Fisher*, *Richard C. Linger*, *Howard F. Lipson*, *Thomas A. Longstaff*, *Nancy R. Mead* “Survivable Network Systems: An Emerging Discipline” // http://www.cert.org\research\97tr013.pdf

5. *Robert J. Ellison*, *David A. Fisher*, *Richard C. Linger*, *Howard F. Lipson*, *Thomas A. Longstaff*, *Nancy R. Mead* “Survivability: Protecting Your Critical Systems” // http://www.cert.org\archive\html\protect-critical-systems.html