СТРУКТУРНО-ИНФОРМАЦИОННЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ СЛОЖНЫХ СИСТЕМ

Л.С. СТРИГАЛЕВ

В современных условиях резко возросла актуальность создания высокоэффективных систем и средств безопасности. Необходим анализ и обновление традиционной парадигмы безопасности. Безопасность — неотъемлемое эмерджентное свойство сложной системы; это свойство структуры системы в ее четверке: система, структура, цель, технология [1]. Чем выше качество безопасности, тем более устойчива структура системы. В структуре системы заложена ее цель, порождающая технологию системы; угрозу представляет все то, что способно причинить вред структуре системы. Безопасность, как и у живых организмов, должна охватывать все структурные уровни.

У человека, например, сеть «датчиков» контролирует все жизненно важные органы, которые имеют многочисленные проекции (на коже такие проекции используются в акупунктуре и акупрессуре). Дополнительная, интеллектуальная безопасность человека, связана с тремя уровнями целеполагания: генетическим, неосознанным (условный и каузальный рефлексы; ментальность, привычка) и осознанным. Заметим, что именно неосознанному уровню в значительной степени обязаны, техногенные катастрофы.

В заключение отметим, что важен не только «охват» структуры защищаемой системы «нервной сетью», но и обеспечение заданного качества функционирования такой сети. В этой связи необходимы соответствующие методы и средства оценки качества информационного метаболизма. Ограничения на объем тезисов не позволяют детализировать данный аспект, который является достаточно хорошо проработанным в рамках информационного подхода применительно к системам обнаружения объектов.

Литература

1. Стригалев Л.С. // Экономическое развитие общества: инновации, информатизация, системный подход: Материалы Междунар. научно-экономической конф. 22–23 апреля 2008 г. Минск, 2008 С. 257–226.

КРИТЕРИИ ОЦЕНКИ КАЧЕСТВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Л.С. СТРИГАЛЕВ

Оценка качества средств защиты информации занимает далеко не последнее место в проблемной среде индустрии компьютерной безопасности. Такие оценки необходимы при разработке и оптимизации средств защиты информации, а также при выборе средств защиты для реализации политики безопасности.

Стандарты в области компьютерной безопасности отображают вопросы методологии, менеджмента, включая управление и контроль рисков, но не содержат критерии оценки качества средств безопасности. Последнее обстоятельство способствует маркетинговым играм. Например, как отмечается в ряде источников, манипулируя критериями и условиями проведения эксперимента можно практически любой антивирус представить как наилучший. Подобное возможно для всех средств и систем, работа которых связана с двумя видами ошибок: ложное обнаружение и пропуск объекта. Более того иногда количественные оценки результатов машинных и даже натурных экспериментов могут превышать предельные возможности исследуемых систем (результат «подгонки» под требования ТЗ при отсутствии оценки предельных возможностей системы).

Для разрешения обсуждаемой проблематики представляется целесообразным использовать информационные меры, в частности, дивергенцию Кульбака-Лейблера, которая представляет собой математическое ожидание логарифма отношения правдоподобия и обладает свойством аддитивности. Данное свойство позволяет, например, в области систем обнаружения оценивать предельные возможности средств обнаружения, а также путем введения информационных КПД оценивать потери информации при ее поэтапной обработке (включая оценку качества работы человека-оператора) и осуществлять оптимизацию, как в цепи поэтапной обработки информации, так и системы обнаружения в целом.

АНАЛИЗ ПРОСТОЕВ СЕРВЕРА INTEL SERVER BOARD S5520UR ПО ПРИЧИНАМ ИХ ВОЗНИКНОВЕНИЯ

В.И. ПАЧИНИН, Т.Г. ТАБОЛИЧ, Д.В. ШЕРЕМЕТ

Отказы программно-аппаратной части является одной из важнейших техногенных угроз информационной безопасности сервера [1]. Парированием этой угрозы могут быть наблюдения за работой сервера во время эксплуатации [2-5]. Результаты наблюдений не только помогают [2–4] уменьшить простои сервера и потери во время простоев обрабатываемой сервером информации, но и дают возможность количественно оценить показатели надёжности сервера и уровень потерь информации во время отказов [2, 5]. Однако фактические данные об отказах серверов практически не публикуются, поэтому в [6] проанализированы результаты наблюдений в течение 2,1 года за надёжностью высокопроизводительного сервера Intel Server Board S5520UR (процессор Intel Xeon CPU E5620 x2, RAM 26 Gb, HDD 2x2 Тб). Коэффициент готовности (КГ) этого сервера (без разделения отказов на конструктивные, производственные и эксплуатационные) составил 0,999406, коэффициент технического использования (КТИ) 0,999340, процент потерь информации (ПИ) за счёт простоев 0,066%.

Если проанализировать простои сервера и разделить их по причине возникновения, то два простоя можно отнести к эксплуатационным. Таким образом, повышая качество эксплуатации, этих отказов можно было бы избежать. Простой в связи с обновлением версии операционной системы также относится к эксплуатационным отказам. Избежать данного вида отказов не возможно по причине неосуществимости ликвидации существующего объективно морального старения программного обеспечения. Оставшиеся простои (замена планки памяти 4 Гб Memory Module Kit на планку большего объёма и замена винчестера на винчестер большего объёма с целью увеличения дискового пространства сервера) также невозможно отнести к конструктивным или производственным отказам — замена комплектующих во время эксплуатации не требовалась бы, при условии приобретения более дорогостоящего сервера с планкой и винчестером большего объёма.

Таким образом, фактическая безотказность (средняя наработка на отказ относительно отказов, которых нельзя было избежать) сервера Intel Server Board S5520UR оказалась не ниже 18 тысяч часов, фактический КТИ не ниже 0,9999445, а фактический процент ПИ не более 0,00445 %.

Литература

1. Гайдук В.Ю., Пачинин В.И., Сечко Г.В., Таболич Т.Г. // Материалы 13-й МНТК «Современные средства связи» 7–9 октября 2008 г., Минск. Минск: ВГКС, 2008. С. 194.

2. Бахтизин В.В., Николаенко Е.В., Сечко Г.В., Таболич Т.Г. Модели отказов и наблюдения за отказами: лаб. практикум по курсу «Надёжность программного обеспечения (НПО)» для студ.