

Мониторинг безопасности информации в приложении к задачам управления качеством инфотелекоммуникационных сетей

Monitoring of information security applied to quality control problems of infotelecommunication networks

Ключевые слова: безопасность информации – information security; инфотелекоммуникационная сеть – infotelecommunication network; мониторинг – monitoring; менеджмент качества – quality management; цикл управления – control cycle; валидация – validation; верификация – verification.

В статье рассмотрены место и роль мониторинга как взаимоувязанного процесса наблюдения, оценивания и прогнозирования состояния безопасности информации в рамках задач управления качеством инфотелекоммуникационных сетей, анализируются подходы к формированию модели системы менеджмента качества объекта – системы безопасности информации, приведены основные понятия, используемые при описании пространства состояний безопасности информации.

The article considers the place and the role of monitoring as a coupled process of surveillance, evaluation and forecasting information security state within the tasks of infotelecommunication networks quality management, analyzes the approaches to forming an object quality management system model – an information security system, the main notions, used in the information security state space description.

Системный подход к методологии мониторинга безопасности информации (МБИ) инфотелекоммуникационных сетей (ИТКС) предопределяет как рассмотрение данного процесса в рамках метасистемы, так и учет форм, закономерностей и факторов развития (технической эволюции) мониторинга безопасности параллельно с системами связи, кибернетической составля-

ПАРАЩУК / PARASCHUK I.

Игорь Борисович

(shchuk@rambler.ru)
доктор технических наук, профессор,
заслуженный изобретатель РФ,
профессор кафедры Автоматизированных систем
специального назначения,
Военная академия связи,
г. Санкт-Петербург

ющей которых он является. Исходя из предпосылки, что ИТКС может быть представлена как производственная структура, рассмотрим процесс МБИ ИТКС с системных позиций – рассмотрим взаимосвязь МБИ ИТКС и мониторинга системы связи в целом с точки зрения стандартизованных понятий управления (менеджмента) качеством и с учетом тенденций технической эволюции (ТЭ) и особенностей этапов жизненного цикла (ЖЦ) сетей такого класса. Это даст нам возможность взглянуть на МБИ ИТКС как на комплексный, системный и эволюционирующий процесс наблюдения, оценивания и прогнозирования состояния и качества системы безопасности информации (СБИ) сети, позволит обосновать новизну и актуальность исследований, ориентированных на эволюционные изменения в оценке состояния и качества безопасности информации современных и перспективных ИТКС.

Иерархия процессов мониторинга в рамках системы связи предопределяет взгляд на МБИ ИТКС как на систему наблюдения, оценивания и прогнозирования состояния и качества всех объектов системы безопасности информации сети и процессов, реализуемых ими. Мониторинг безопасности информации должен пронизывать все уровни системы связи и представлять собой единый взаимоувязанный процесс на различных уровнях управления системой связи. Структура понятий МБИ ИТКС должна быть ориентирована на отечественные [1, 2] и международные [3–5] стандарты в области менеджмента качества.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Ключевыми понятиями здесь являются понятия маркетинга, мониторинга и менеджмента качества.

Как и в любой другой производственной структуре, заказчикам и потребителям необходима продукция ИТКС – безопасные инфотелекоммуникационные услуги, характеристики которых удовлетворяли бы их потребности и ожидания. Эти потребности и ожидания отражаются в технических условиях заказчика (для этапов проектирования, разработки и производства), руководящих документах по организации связи (для этапа эксплуатации) и обычно считаются требованиями потребителей. Требования по безопасности информации могут быть установлены потребителями услуг ИТКС или определены вышестоящим органом управления системы связи.

В любом случае, приемлемость продукции – инфотелекоммуникационных услуг с точки зрения безопасности, в конечном счете, устанавливает потребитель услуг ИТКС. Поскольку потребности и ожидания потребителей меняются, система связи (СС) в целом, и ИТКС в частности, испытывают давление, обусловленное необходимостью в безопасных услугах, адекватных современным условиям технической эволюции, СС и ИТКС должны постоянно совершенствовать свою продукцию (услуги) и свои процессы с точки зрения безопасности информации.

Системный подход к менеджменту качества ИТКС побуждает разработчиков и производителей систем связи (на этапах проектирования, разработки и производства) и инженеров-администраторов ИТКС (на этапе эксплуатации) анализировать требования заказчиков и пользователей (маркетинг) с точки зрения безопасности информации, наблюдать, оценивать и прогнозировать выполнение требований к качеству (мониторинг качества) СБИ ИТКС, определять процессы, способствующие получению и предоставлению услуг, приемлемых для потребителей с точки зрения безопасности информации, а также поддерживать эти процессы в управляемом состоянии (менеджмент качества СБИ).

Применительно к терминам Государственного стандарта [1], под менеджментом качества СБИ ИТКС целесообразно понимать скоординированную деятельность по руководству и управлению безопасностью информации сети применительно к качеству.

Использование стандартизованных понятий, изложенных в документах [1–5] и обобщенных в работе [6], применительно к процессам управления СБИ ИТКС позволяет определить роль

и место МБИ ИТКС, которые достаточно ярко прослеживаются при рассмотрении модели системы менеджмента качества объекта, основанной на процессном подходе. Действительно, функционирование СБИ ИТКС можно рассматривать как любую деятельность, направленную на преобразование ресурсов в результат (входов в выходы) [1], т.е. как процесс.

Чтобы результативно функционировать, СБИ ИТКС должны определять и управлять многочисленными взаимосвязанными и взаимодействующими процессами, причем выход одного процесса часто образует непосредственно вход следующего. Систематическая идентификация и менеджмент применяемых СБИ ИТКС процессов и обеспечение их взаимодействия могут считаться «процессным подходом» [1].

В процессе мониторинга в рамках системы менеджмента качества ГОСТы [1–5] много внимания уделяют терминам «качество» и «оценение». Интерпретируя понятия, введенные в данных руководящих документах, для нужд конкретного исследования, можно определить качество СБИ ИТКС как степень соответствия присущих СБИ ИТКС характеристик требованиям.

Применительно к качеству СБИ ИТКС, оценивание, по аналогии со стандартизованными в РФ понятиями, является основой получения объективного свидетельства, получения данных, подтверждающих или опровергающих наличие требуемого качества СБИ ИТКС в конкретных условиях функционирования. Важными понятиями, нашедшими свое отражение в [1–4], относящимися к мониторингу в целом и к оцениванию качества СБИ ИТКС в частности, являются, на наш взгляд, понятия верификации и валидации.

Под верификацией понимается подтверждение на основе представления объективных свидетельств того, что установленные требования по безопасности ИТКС были выполнены [1]. Под валидацией понимается подтверждение на основе представления объективных свидетельств того, что установленные требования по безопасности ИТКС, предназначенные для конкретного использования или применения, были выполнены [1]. Сущность данных понятий в рамках МБИ ИТКС необходимо рассматривать, отталкиваясь от понятий «составление безопасности информации ИТКС» и «качество безопасности информации ИТКС». Анализируя такой многофункциональный и изменяющийся в динамике ТЭ, ЖЦ и эксплуатации объект как ИТКС, нетрудно заметить, что уровень качества его безопасности информации напрямую связан с традиционными классами

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

состояния, а определение (оценивание) состояния безопасности информации, и, особенно, получение подтверждения того факта, что состояние (качество) безопасности информации удовлетворяет требованиям (которые тоже изменяются в ходе ТЭ, ЖЦ, эксплуатации) представляет собой одну из задач МБИ – задачу валидации-верификации. При этом этапам (циклам) МБИ ИТКС соответствует определенный уровень решения задачи валидации-верификации.

Таким образом, верификация в рамках МБИ ИТКС представляет собой симбиоз решения задачи получения подтверждения о том, что установленные требования по безопасности информации, ориентированные на конкретное использование или применение ИТКС, были выполнены (валидации) и решения задачи получения подтверждения, что установленные требования по безопасности информации ИТКС будут выполнены в измененных, например, критических условиях, как сейчас, так и в будущем.

Анализ показывает, что решение задачи верификации включает валидацию и, кроме того, связано с задачей прогнозирования состояния (качества) безопасности информации ИТКС, определяет возможности СБИ ИТКС достигать цели функционирования всегда, в любых условиях, и служит главной составляющей при принятии информационного решения в рамках цикла управления безопасностью ИТКС.

Очевидно, что на МБИ ИТКС, на процесс оценивания состояния (качества) СБИ сети оказывает непосредственное влияние ряд факторов, главными из которых, на наш взгляд, являются факторы, характеризующие этапы ТЭ, ЖЦ и условия эксплуатации (функционирования и применения).

Таким образом, можно сделать выводы о том, что МБИ ИТКС – иерархический, комплексный (системный) и эволюционирующий процесс наблюдения, оценивания и прогнозирования состояния (качества) сети с точки зрения безопасности информации. Мониторинг безопасности информации ИТКС должен охватывать все пространство состояний сети с учетом всего диапазона факторов, влияющих на состояние (качество) СБИ ИТКС, и быть адаптивным – способным изменять свои режимы (алгоритмы наблюдения, уровни, объем, номенклатуру контролируемых параметров) в зависимости от активности тех или иных факторов.

Литература

1. ГОСТ Р ИСО 9000-2001. Системы менеджмента качества. Основные положения и словарь. – М.: Госстандарт России, 2001. – 26 с.
2. ГОСТ Р ИСО 9004-2001. Системы менеджмента качества. Рекомендации по улучшению деятельности. – М.: Госстандарт России, 2001. – 46 с.
3. Международный стандарт ISO 9000-1-94. Общее руководство качеством и стандарты по обеспечению качества. Часть 1. Руководящие указания по выбору и применению. – М.: ИПК Издательство стандартов, 1998. – 32 с.
4. Международный стандарт ISO 9004-1-94. Управление качеством и элементы системы качества. Часть 1. Руководящие указания. – М.: ИПК Издательство стандартов, 1998. – 41 с.
5. Международный стандарт ISO/IEC 27001:2005. Системы менеджмента информационной безопасности. Требования. ИСО/МЭК 2005. – М.: Технорматив, 2006. – 48 с.
6. Парашук И.Б., Хасан Т.М. Мониторинг информационной безопасности: от общесистемного к частному. // Information Security / Информационная безопасность. – 2006. – № 5. – С. 8–9.

НОВОСТИ НАУКИ

23–25 апреля 2014 г. компания «Совзонд» проводит II Международный Форум «Интеграция геопространства — будущее информационных технологий»

Журнал «Информация и Космос» является информационным партнером Второго Международного форума «Интеграция геопространства — будущее информационных технологий» и совместно с организаторами приглашает принять участие в мероприятии.

Как и в предыдущий год, участники предстоящего Форума ознакомятся с новыми технологиями и проектами, перспективами развития геоинформационной отрасли. О новейших разработках расскажут руководители и специалисты министерств, ведомств, крупных компаний, успешно внедряющих геоинформационные системы и геопорталы. Появление программных средств автоматизированного дешифрирования и обработки космических снимков, совершенствование геоинформационного программного обеспечения и программно-аппаратных комплексов визуализации пространственных данных, развитие технологии облачных вычислений — все это кардинально меняет взаимоотношения поставщиков и заказчиков на рынке геоинформационных услуг. Появился и активно развивается такой сегмент геоинформатики, как геоинформационные онлайн-сервисы, своим опытом использования и внедрения таких сервисов поделятся представители ведущих участников рынка. О новинках программного обеспечения и технических средств расскажут мировые лидеры геоинформационного сектора и космической отрасли.

Международный форум «Интеграция геопространства — будущее информационных технологий», собравший в прошлом году более 300 участников из 17 стран мира, является одним из самых заметных событий отрасли. Он предоставляет специалистам и руководителям отличную площадку для обмена опытом и получения новых знаний.

Деловая программа Форума:

- VIII Международная конференция «Космическая съемка — на пике высоких технологий»
- II Международная конференция «ГИС — интеграционные решения будущего»
- Отраслевые круглые столы и семинары
- Обучающие мастер-классы
- Конкурс «Лучшие проекты в области ГИС и ДЗЗ»
- Выставка «Техника и технологии»

Актуальные темы Форума

- Региональные инфраструктуры пространственных данных
- Региональные ГИС и геопорталы
- Муниципальные ГИС
- Геоинформационные онлайн-сервисы на базе данных ДЗЗ и облачных технологий
- Отраслевые ГИС (в сельском и лесном хозяйстве, нефтегазовой отрасли и т.д.).
- Перспективы развития ГИС в здравоохранении и социальной сфере (ГИС «Доступная среда»)
- ГИС в системах обеспечения безопасности жизнедеятельности (ГИС «Система 112»)
- Новые зарубежные и отечественные системы космического мониторинга. Перспективы развития глобальной группировки спутников ДЗЗ
- Использование результатов космической деятельности в регионах РФ
- Новинки программных решений обработки и анализа данных ДЗЗ
- Применение малых спутников ДЗЗ для оперативной съемки
- Перспективы видеосъемки из космоса группировками микро- и наноспутников
- Новейшие источники получения геопространственных данных, в том числе БПЛА

Оформить заявку на участие можно на официальном сайте Форума www.sovzondconference.ru.