УДК 004.621:681.14

Чернишев А.Н.

КОНЦЕПЦИЯ И ПРОБЛЕМЫ МОНИТОРИНГА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТЕЙ.

В статье рассматривается проблема мониторинга обеспечения безопасности сетей, который должен базироваться на широком применении современных математических методов и методов анализа данных, новых информационных, а также интелектуальных технологий и средств телекоммуникаций.

Ключевые слова: мониторинг, метод, синтез, информация, событие, модель, прогноз, информационное пространство, несанкционированный доступ.

Для количественного определения уровня устойчивого получения информации для развития и функционирования государства необходимо создание интегрированной системы сбора, накопления, анализа и интерпритации информации о ходе и тенденциях развития общества и мирового сообщества, отличной от традиционной системы статистической информации [1]. Следовательно, без системы мониторинга не обойтись. Разработка методологического и методического обеспечения этой деятельности должна в определенном смысле составить новое и относительно самостоятельное направление в науке – теорию мониторинга.

Термин «мониторинг», согласно Статистическому словарю – «специально организованное систематическое наблюдение за состоянием каких-либо объектов» [2]. Эта формулировка может стать основой для определения понятия мониторинг информационных и телекоммуникационных сетей при условии уточнения целей такого наблюдения и смысла понятия «объект».

Мониторинг должен базироваться на объединении различных видов мониторинга. В системном анализе такому объединению соответствует понятие целого, приобретающего в результате объединения определенных элементов новое системное качество, не присущее этим элементам порознь (свойство эмерджентности).

На сегодняшний день существуют различные подходы к классификации мониторинга информационной сферы:

- по характеру решаемых задач;
- по уровню организации (локальные, региональные и глобальные сети);
- по природной среде, за которой ведутся наблюдения.

Блок-схема системы мониторинга приведена на рис. 1.

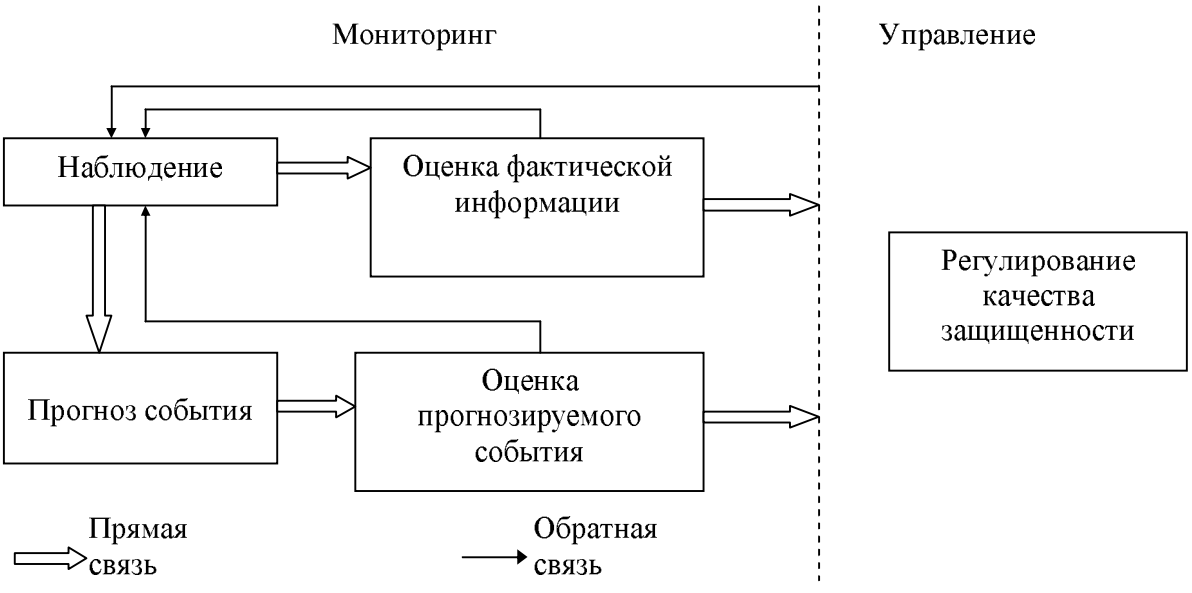

Рис. 1. Блок-схема системы мониторинга.

Поскольку информационное пространство представляет собой единую систему, информационные процессы неразрывно связаны с функционированием пространства, то оценки прогнозируемых событий не могут быть получены без использования данных мониторинга.

Концепции мониторинга информационного пространства [3]:

- целевая (мониторинг - проблемно-ориентированная система, перекрывающая определенную сферу информационных потребностей);
- инструментальная (выделяемая среди других систем обработки информации по типу используемых средств и методов);
- интеграционная (результат перегруппировки традиционных информационно-управляющих функций и т.д.).

В данной работе предлагается концепция мониторинга, базирующаяся на трех приведенных концепциях.

Под мониторингом безопасности сетей как частью системы управления безопасностью будем понимать специально организованное целевое непрерывное (систематическое) наблюдение и прогнозирование (краткосрочное) хода дальнейших событий с целью их анализа, идентификации и выявления круга регулируемых фактов, для подготовки противодействия и принятия решений.

Главная цель мониторинга безопасности - сбор, изучение и подготовка информации для принятия и анализа решений на различных уровнях управления. Мониторинг безопасности как инструмент для принятия обоснованных решений противодействия включает: ведение единой базы данных мониторинга; визуализацию и анализ данных; построение моделей безопасности; прогноз развития различных атакующих ситуаций и действий; формирование управляющих решений на основе моделирования и прогноза.

Как система сбора и обработки информации мониторинг безопасности сети имеет две особенности: целевая направленность информационных процессов и объективность получаемых выводов на каждой стадии обработки данных.

Основные задачи мониторинга:

1. Начальная и текущая идентификация процесса безопасности сети. Мониторинг должен базироваться на системной классификации процессов обеспечения безопасности. Поскольку состав и номинальные характеристики процессов обеспечения безопасности меняются и попытки несанкционированного получения информации меняются, мониторинг позволяет накапливать данные для пересмотра и коррекции самой структурной схемы таких процессов.

2. Анализ взаимосвязей, наблюдаемых и ненаблюдаемых процессов попыток несанкционированного получения информации и выявление круга управляемых переменных, определяющих течение одного из них. Динамично развивающие эти процессы характеризуются не только количественно изменяющимися выходами и входами, но и меняющимся набором факторов.

3. Прогнозирование протекания наблюдаемого процесса. Интерпретация текущего значения наблюдения возможна только при условии, когда оно рассматривается связующим звеном между прошлым и будущим, а не просто завершающим элементом прошедшего периода.

В зависимости от источников и потребителей информации по уровню агрегирования можно выделить 4 уровня мониторинга: локальный, региональный, государственный и глобальный.

По направлениям мониторинг безопасности можно разделить на следующие алгоритмы, согласно рис. 2.

Мониторинг безопасности сетей должен базироваться на широком применении современных математических методов и методов анализа данных, новых информационных технологий и средств телекоммуникаций.

Так как предмет мониторинга безопасности (в соответствии с изложенным) - процессы обеспечения безопасности сетей, то требуется разработка моделей процессов обеспечения безопасности, предназначенных для решения аналитических и прогнозных задач.

Рис. 2. Структурная схема алгоритмов мониторинговых исследований.

Особенности моделирования определяются следующим:

1. Предмет изучения и моделирования - процессы мониторинга безопасности. Потребности мониторинга требуют включения когнитивной базы в предметную область моделирования, поскольку система мониторинга претерпевает изменения в процессе развития процессов мониторинга, которые могут характеризоваться нестабильностью. Для них характерно не только непостоянство механизмов трансформации входных воздействий и выходных, но и изменчивость самого состава факторов.

2. В сферу мониторинга безопасности входит не только функциональное, но и целевое пространство. Моделирование целевого пространства, отражающего интересы безопасности,

затруднено из-за не наблюдаемости его элементов и недостаточной математической разработки [4].

3. Интегрирующая роль мониторинга безопасности требует интегрированного учета в моделях разнородной количественной и качественной информации об контролируемых процесах. По мере накопления мониторинговых количественных данных возникает задача переработки их в данные качественные т.е. знания [5].

4. Прикладной характер, мониторинга безопасности делает процедуру интерпретации результатов моделирования весьма ответственной. Вопрос о том, какие именно показатели модели можно интерпретировать как реальные, а какие носят промежуточный и не интерпретируемый характер – далеко не прост [6].

Многие из перечисленных проблем моделирования процессов безопасности актуальны не только в задачах мониторинга безопасности.

Для решения недостаточно разработанной на сегодня методологии моделирования процессов безопасности имеется фундамент в виде различных моделей [7].

Таким образом, математическое обеспечение мониторинга безопасности информационных и телекоммуникационных сетей требует разработки и адаптации инструментария моделирования, отвечающего задачам мониторинга безопасности. В частности должна быть разработана методология построения моделей процессов обеспечения безопасности с переменным составом факторов; методы интегрированного анализа данных, методы анализа и графического представления пространственно привязанных данных.

ЛИТЕРАТУРА

1. Хорошко В.А. Информационная безопасность Украины: основные проблемы и перспективы. /Хорошко В.А.// Захист інформації, Спец. випуск, 2008.-с.6-9.
2. Статистический словарь. – М.: Финансы и статистика, 1989. – 654с.
3. Мухин В.И. Мониторинг состояний информационных ресурсов для реализации адаптивного управления защищенностью компьютерных систем/Мухин В.Е., Волокита А.Н., Павленко Е.К.//Штучний інтелект, №3,2006.-с.773-783.
4. Вальков К.И. Введение в теорию моделирования/Вальков К.И.-Л.:Изд. ЛИСИ, 1974.-152с.
5. Катренко А.В. Теорія прийняття рішень/Катренко А.В., Пасічник В.В., Пасько В.П.-К.:Вид. група BHV, 2009/-448с.
6. Хелман О. Введение в теорию оптимального поиска/Хелман О.-М.: Наука, 1985.-248с.
7. Мухин В.Е. Риск-ориентированная информационная безопасность/Мухин В.Е.-К.: НТУУ «КПІ», 2011.-291с.

Надійшла: 25.01.2012

Рецензент: д.т.н., доц. Толюпа С.В.