КОМПЛЕКСИРОВАНИЕ ИЗМЕРИТЕЛЬНОЙ ИНФОРМАЦИИ В МНОГОДАТЧИКОВЫХ СИСТЕМАХ НАБЛЮДЕНИЯ

Д.С. Шарак А.В. Хижняк

Важнейшим элементом разведывательной деятельности государства является использование технических средств разведки, существенно расширяющих возможности в отображении воздушной обстановки.

Анализ существующих систем наблюдения показывает, что комплексирование координатной информации от нескольких разнородных датчиков, работающих с различными физическими полями, позволяет повысить одновременно помехозащищенность, точность и достоверность управляющих воздействий.

Оптимальное решение задачи повышения эффективности таких систем состоит в комплексном объединении всех доступных результатов измерений координатной информации об объектах наблюдения от нескольких датчиков в единый вектор измерений с комплексной многомерной оптимальной обработкой информации.

Разработка нового специального программного обеспечения по комплексированию измерительной информации требует глубоких аналитических исследований, а также наличие материально-технической базы для проведения научных исследований. С этой целью в Военной академии Республики Беларусь был разработан и запатентован учебно-стационарный комплекс автоматизированных систем управления (УСК АСУ), который представляет собой совокупность учебно-боевых командных пунктов тактического, оперативно-тактического и оперативно-стратегического звеньев управления военно-воздушных войск и войск противовоздушной обороны, а также оперативного объединения Сухопутных войск. Компактность расположения комплекса, наличие структурной избыточности по каналам связи и другие достоинства способствует оперативному проведению всех необходимых проверок разрабатываемого программного обеспечения.

Таким образом, созданный в Военной академии УСК АСУ позволяет проводить апробацию разработки новых технических решений (в т.ч. комплексирование измерительной информации в многодатчиковых системах наблюдения) с последующей оценкой их эффективности.

Литература

1. Хижняк А.В. // Наукоемкие технологии. 2014. № 5. С. 56–61.

ОПТИМИЗАЦИЯ ПОСЛЕДОВАТЕЛЬНЫХ УСЕЧЕННЫХ ПРОЦЕДУР ОБНАРУЖЕНИЯ

А.С. Шеин Е.И. Хижняк

Задачи обнаружения сетевых атак являются актуальными при обеспечении защиты информации. Часто такие задачи могут быть представлены в байесовской постановке. При этом они характеризуются зависимостью возможных потерь от времени с момента начала атаки до ее обнаружения, а также необходимостью ограничения времени на принятие решения. Для указанных условий в классической теории статистических методов обнаружения получено решение только для минимизации текущего среднего риска, связанного с каждым шагом наблюдения. В данном случае вопрос нахождения абсолютно оптимального решения, связанного с минимизацией среднего риска остается открытым.

Для разрешения указанной проблемы предлагается использование k-этапных последовательных процедур. В публикациях Российских ученых, И.Г. Сосулина и К.Ю. Гаврилова подробно освещен вопрос применения k-этапных процедур для оптимизации условно-экстремального критерия и лишь упоминается возможность оптимизации байесовского риска. При оптимизации байесовского риска правило принятия решения сохраняется общим для k-этапных процедур, при этом ограничения на используемую статистику не налагаются. Однако вопрос выбора оптимальных порогов остается нераскрытым. Для решения задачи оптимизации порогов предлагается использовать

численный метод а алгоритм поиска оптимальных значений порогов реализовать на основе принципа динамического программирования Беллмана.

Таким образом, в докладе предложен алгоритм поиска порогов k-этапных процедур принятия решения, квазиоптимальный по критерию минимума среднего риска. Предлагаемый алгоритм основывается на численных методах поиска экстремума функции. При этом для значительного уменьшения вычислительной сложности численного поиска применен метод динамического программирования Беллмана. Использование принципа Беллмана позволило избавиться от экспоненциальной зависимости итераций поиска от k, возникающей при полном переборе всех возможных комбинаций.

Литература

1. Шеин А.С., Хижняк А.В., Белый А.С. Методика многоканальной квазиоптимальной по критерию полного среднего риска k-этапной обработки радиолокационной траекторной информации для обнаружения факта наведения истребителя противника на свой самолет / Доклады БГУИР 2013г. №3(73) стр. 94.

ЗАЩИТА ДИНАМИЧЕСКИХ ВЕБ-САЙТОВ С ПОМОЩЬЮ ПРОДУКЦИИ КОМПАНИИ CHECKPOINT НА ПРИМЕРЕ МЕЖСЕТЕВОГО ЭКРАНА CHECKPOINT R77

А.О. Хмельницкий, О.В. Бобков, Т.А. Пулко

Угрозы безопасности постоянно меняются, и средства защиты для компаний различных размеров усложняются. Множество систем безопасности на сегодня являются системами поиска совпадений (сигнатур) и моделей поведения уже известных угроз. Они бессильны против новых атак, на которые ещё нет сигнатур и патчей от производителя. Для решения обозначенных проблем предлагается использование демилитаризованной зоны (ДМЗ), представляющей собой сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных. Основной целью ДМЗ является добавление дополнительного уровня безопасности в локальной сети, позволяющего минимизировать ущерб в случае атаки на один из общедоступных сервисов: злоумышленник имеет внешний прямой доступ только к оборудованию в ДМЗ.

В нашем случае в демилитаризованной зоне находится только статическая часть сайта, содержащая компоненты, которые при атаке на них и выводе из строя не наносят критического ущерба всему веб-сайту. Динамическую часть мы вынесли в ядро системы. Статическая и динамическая части разделены межсетевым экраном CheckPoint R77, который является новой версией своей архитектуры программных блейдов. CheckPoint R77 характеризуется новым сервисом ThreatCloud Emulation, технологей обеспечения высокой производительности Check Point HyperSpect, программным блейдом Check Point Compliance, новыми средствами централизованного управления устройствами, улучшенной системой аутентификации пользователей на основе интеграции RADIUS и IF-MAP, а также усовершенствованной унифицированной операционной системой Check Point GAiA.

Современные угрозы информационной безопасности вынуждают не только изменять существующие архитектурные решения, но и внедрять новые аппаратные решения.

Литература

http://www.checkpoint.com/r77/index.html.

ПРОВЕРКА КАЧЕСТВА РАБОТЫ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ

Ярук А.М., Киевец Н.Г., Корзун А.И.

В информационной системе безопасности для получения надежных криптографических ключей используют качественные генераторы случайных чисел (ГСЧ). Оценка качества работы ГСЧ осуществляется путем использования статистических методов тестирования. Целью данной работы является проверка качества работы физического ГСЧ.

Одной из наиболее используемых систем тестирования является система стандарта FIPS140-2[1], которая включает следующие статистические тесты: монобитный тест, тест