иявляется отличным средством автоматизации учёта рабочего времени на любом предприятии.

Е. В. Рафалова
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **А. И. Кучеров,** ст. преподаватель

ИСПОЛЬЗОВАНИЕ ПРОГРАММНЫХ СРЕДСТВ МОНИТОРИНГА ПОЛЬЗОВАТЕЛЬСКОЙ АКТИВНОСТИ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

На современном этапе развития информационных технологий, практически все рабочие места оснащены вычислительной техникой. При этом проблемы администрирования и обеспечения информационной безопасности являются очень актуальными.

Деятельность человека, нарушающая конфиденциальность или уровень доступа к данным может оцениваться как вторжение в информационную систему. Вторжения, которые происходят внутри организации, приносят наибольший ущерб, поскольку атака осуществляется злоумышленником, который имеет непосредственный доступ к файловой системе организации.

В системах обнаружения вторжений чаще всего используется сигнатурный метод, который представляет собой сравнение записей о событиях с шаблонами атак. Проблема таких систем состоит в невосприимчивости к новым угрозам, пока эксперт не опишет новые шаблоны атак. В свою очередь, специалист должен анализировать журналы аудита и приложений, собранные системой, для обеспечения достаточной степени защиты информации. Информацию такого рода собирают с помощью специализированных инструментов.

Инструменты мониторинга пользовательской активности в сети должны обеспечивать сбор и анализ статистики работы пользователей и приложений, позволять визуализировать модели поведения пользователей, а также выявлять внутренние угрозы.

При анализе инструментов для мониторинга пользовательской активности в сети были выявлены основные три класса программных продуктов:

– различные программные средства с открытым исходным кодом, в основном распространяются бесплатно, но требуют более тонкой настройки для решения отдельных задач;

– программные решения, входящие в состав продуктов определенных производителей, которые могут работать «из коробки», но имеют ограничения на взаимодействие с отдельными видами инструментов;

– специализированные средства для мониторинга и диагностики сети (NPMD-решения). Это продукты для глубокого анализа сетевой инфраструктуры.

Данные инструменты используются для автоматизации контроля над событиями, которые протекают в информационной системе, а также для анализа этих событий с целью поиска признаков угроз безопасности. В связи с тем, что количество различных способов и видов несанкционированных вторжений в информационные сети увеличивается, системы обнаружения вторжений являются неотъемлемой частью организации информационной безопасности.

Е. В. Рафалова
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **А. И. Кучеров,** ст. преподаватель

ПРИМЕНЕНИЕ МОДУЛЬНОГО ТЕСТИРОВАНИЯ В ПРОЕКТЕ МОНИТОРИНГА ПОЛЬЗОВАТЕЛЬСКОЙ АКТИВНОСТИ

Оценка качества приложения достигается с помощью применения различных видов и техник тестирования. В данном проекте применяются техники модульного, интеграционного и системного тестирования.

Модульное тестирование приложения заключалось в запуске небольших частей приложения и оценки результата их работы. Программный продукт разрабатывался по методологии TDD. Написание тестов предшествовало разработке самого кода.

В таком случае требования к приложению были разбиты на небольшие логические блоки, которые, после реализации, явились точками входа для модульного тестирования. Это увеличило покрытие кода тестами, что, в свою очередь, уменьшило количество ошибок в работе приложения.

Для разработки модульных тестов необходимо придерживаться некоторых принципов: тесты не должны быть громоздкими, они должны