Лингур Л.Н., Есина О.Г.

ПРОГРАММНЫЕ ПРОДУКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕСА

Одесский национальный политехнический університет, Одесса

Современный бизнес и государственный аппарат сегодня уже невозможно представить без применения информационных технологий. Автоматизация процесса сбора, хранения, обработки и использования информации, комплексная автоматизация управленческой деятельности стала закономерным этапом развития государственных и коммерческих структур.

Стремительное увеличение информационного потока, повышение динамики бизнеса и постоянно растущие требования современного общества диктуют необходимость модернизации существующих и внедрения новых высокотехнологичных систем, предназначенных для оптимизации бизнес-процессов в области управления предприятия.

Проблема информационной безопасности является в настоящее время одной из ключевых составляющих деятельности любого предприятия. При этом важнейшими являются вопросы внутренней безопасности. Решать эти задачи непросто, т.к. сотрудникам предприятия для выполнения производственных задач предоставляется доступ к информационным ресурсам компании, в том числе и к конфиденциальной информации.

Санкционированные мониторинговые программные продукты используются администратором безопасности вычислительной системы для обеспечения ее наблюдаемости. Именно это свойство, в зависимости от качества его реализации, позволяет в той или иной мере контролировать соблюдение сотрудниками предприятия установленных правил безопасной работы на компьютерах и политики безопасности.

Для чего используются мониторинговые программы?

Их применение позволяет специалисту, ответственному за информационную безопасность предприятия:

- определить (локализовать) все случаи попыток несанкционированного доступа к конфиденциальной информации с точным указанием времени и сетевого рабочего места, с которого такая попытка осуществлялась;
- определить факты несанкционированной установки программного обеспечения;
- проконтролировать возможность использования персональных компьютеров в нерабочее время и выявить цель такого использования;
- определить все случаи несанкционированного использования модемов в локальной сети путем анализа фактов запуска несанкционированно установленных специализированных приложений;
- определить все случаи набора на клавиатуре критичных слов и словосочетаний, подготовки каких-либо критичных документов, передача которых третьим лицам приведет к материальному ущербу;
- определить факты нецелевого использования персональных компьютеров:
- получить достоверную информацию, на основании которой будет разрабатываться политика информационной безопасности предприятия;
- контролировать доступ к серверам и персональным компьютерам;
- контролировать контакты собственных детей при серфинге в сети Интернет;
- проводить информационный аудит;
- исследовать и расследовать компьютерные инциденты;
- проводить научные исследования, связанные с определением точности, оперативности и адекватности реагирования персонала на внешние воздействия;

- определить загрузку компьютерных рабочих мест предприятия;
- восстановить критическую информацию после сбоев компьютерных систем;
- и т.д.

Наиболее популярными среди руководителей предприятий и системных администраторов являются следующие программные продукты.

Большинство мероприятий мониторинга можно проводить с помощью одного программного комплекса: LanAgent- хорошо показал себя при работе с 300 рабочими станциями, что доказывает хорошую масштабируемость этого программного комплекса.

Особенно стоит отметить специальные возможности, предоставляемые программным комплексом LanAgent, такие как мониторинг подключений и отключений запоминающих устройств, контроль набираемых на клавиатуре и копируемых в буфер текстов, которые являются инструментом для выявления утечек важной информации. Средства составления отчетности позволяют распечатывать отчеты, конвертировать их в различные типы, что позволяет составлять статистику по работе пользователей и использование её в служебных целях.

Security Curator – это система обеспечения информационной безопасности нового поколения, объединяющая в себе возможность наблюдения за деятельностью сотрудников, контроля их действий и блокировки потенциально опасных путей утечки информации.

Security Curator выполняет практически все виды мониторинга и логирования персональных компьютеров сотрудников. А именно:

- Контроль основных путей утечки конфиденциальной информации и эффективности работы сотрудников.
- Возможность отключения либо блокировки запуска приложений, процессов, операций с файлами, сайтов и общения в чатах.
- Система уведомлений о нарушении политики безопасности.
- Генерация детализированных статистических отчетов об использовании компьютеров организации.
- Удобная система поиска и фильтрации данных по ключевым словам.

Boss Everyware – логирует все программы, которые запускает пользователь и учитывает время, которое он потратил на них. Программа записывает все напечатанные пользователем символы, позволяя владельцу компьютера или сетевому администратору ответить на вопросы по созданной корреспонденции. Boss Everyware регистрирует время простоя компьютера, уведомляет администратора сети об установленных программах, какое программное обеспечение было использовано и какие веб - сайты были посещены.

Boss Everyware может предупреждать пользователя о том, что запускаемое приложение или программа относятся к запрещённым для этого компьютера. Или может полностью скрыться из обзора и секретно вести лог - файл использования компьютера. Данная программа защищена паролем и к ней имеет доступ только сетевой администратор.

StaffCop Standard - система корпоративной информационной безопасности.

StaffCop Standard контролирует все действия сотрудников за рабочими компьютерами и позволяет получать данные о работе каждого из них как в режиме on-line, так и в виде наглядных отчётов за любой период времени.

На основе собранной информации о действиях пользователей на компьютерах, руководитель или администратор сети может оптимизировать рабочий график сотрудников, а также своевременно выявить и устранить утечки конфиденциальной информации, проанализировав, что именно делал сотрудник, и сколько это заняло времени.

Основные функции программы:

Мониторинг социальных сетей;

Возможность просматривать все поисковые запросы работников в Яндексе, Google, Рамблер и многих других поисковых системах;

Генерация детальных отчётов о действиях сотрудников за компьютером: диаграммы работы с программами и играми, диаграммы посещения сайтов и общения в ICQ.

Сохранение снимков экрана – что работник видел на экране монитора;

Доступна вся переписка в ICQ, Mail.Ru агенте и других онлайн пейджерах;

Клавиатурный шпион;

Логируются все действия с файлами, история напечатанных документов, подключенные USB устройства, установленные программы и многое другое.

Внедрение StaffCop Standard позволяет оценить и повысить эффективность работы организации, а также способствует повышению уровня корпоративной безопасности. Программа позволяет отследить переписку, в которой сотрудник может раскрыть конфиденциальную информацию и определить какие файлы были скопированы на съемные носители информации. Также наблюдению подвергаются практически все действия персонала за компьютерами, что позволяет оценить эффективность его работы.

Система мониторинга персонала «ГЛОСАВ» – услуга, сочетающая в себе удобство и передовые информационные технологии – дает возможность существенно повысить эффективность работы предприятия и его конкурентоспособность.

Персональный мониторинг является мощным альтернативным механизмом повышения эффективности работы персонала. Наличие достоверной информации о местонахождении сотрудников дает возможность эффективно планировать график работ, увеличить производительность, снизить затраты, повысить качество обслуживания.

Система мониторинга персонала «ГЛОСАВ» отличается высокой производительностью и масштабируемостью и в сочетании с гибкими возможностями настройки позволяет достичь максимальной эффективности при управлении персоналом.

В приведенной таблице вы можете сравнить возможности ряда распространенных программ мониторинга:

	Lan Agent	Security Curator	Boss EveryWare	Staff Cop Standart	ГЛОСАВ
Мониторинг запоминающих устройств	+				
Блокировка запуска различных приложений	+	+			
Формирование отчетов разного типа	+	+	+	+	+
Экспорт отчетов в популярные форматы данных	+	+	+	+	+
Разграничение прав доступа к собираемой информации	+	+	+	+	+
Определение графика рабочего времени		+	+	+	+
Мониторинг соц. сетей			+	+	+

Список литературы:

1. Н.Д. Красноступ, Д.В. Кудин. Шпионские программы и новейшие методы защиты от них. Электронный ресурс http://bozza.ru/art-75.html, 12.04.2013
2. А.Жмерик. Boss – EveryWare Описание программного продукта Электронный ресурс: http://www.softsoft.ru/security-privacy/covert-surveillance/7922.htm, 8.04. 2013
3. Описание программного продукта LanAgent. Электронный ресурс: http://www.lanagent.ru/lanagent_func.html 20.04. 2013
4. Система мониторинга персонала ГЛОСАВ. Электронный ресурс: http://www.glosav.ru/glosav.html 6.05.2013