УДК 004
ББК 32.81

ПОДХОД К ПОСТРОЕНИЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

А.М. Цыбулин

Повышение эффективности управления информационной безопасностью предприятия за счет сочетания централизованного (автоматизированного рабочего места администратора) и децентрализованного (комплекс интеллектуальных агентов) мониторинга и аудита управления информационной безопасностью предприятия; выработки множества решений и синтез оптимального решения по повышению уровня информационной безопасности

Ключевые слова: *автоматизированная система управления информационной безопасностью предприятия, система обнаружения атак, информационная безопасность, многоагентные системы, язык моделирования многоагентных систем.*

Анализ состояния дел в области информационной безопасности показывает, что в ряде развитых учреждений и предприятий сложилась и успешно функционирует вполне устоявшаяся инфраструктура системы информационной безопасности, то есть системы мер, обеспечивающей такое состояние конфиденциальной информации, при котором исключаются ее разглашение, утечка, несанкционированный доступ (внешние угрозы), а также искажение, модификация, потеря (внутренние угрозы).

Тем не менее, как свидетельствует реальность, злоумышленные действия над информацией не только не прекращаются, а имеют достаточно устойчивую тенденцию к росту. Опыт показывает, что для успешного противодействия этой тенденции уже недостаточно стройной и управляемой системы обеспечения безопасности информации, созданной уникальным системным администратором или специалистом по защите информации на основе опыта и интуиции. В своей работе они сталкиваются с современными проблемами информационной безопасности. Остановимся на трех из них.

Первая проблема – большое количество разнородных устройств безопасности:

- 90 % – используют межсетевые экраны и антивирусы;
- 40 % – используют системы обнаружения вторжений (IDS);
- растет число сетевых устройств;
- растущее число оборудования обусловливает возрастающую сложность систем.

Вторая проблема – резкое увеличение событий безопасности:

- Один межсетевой экран может генерировать за день более 1 Гб данных в Log-файле.
- Один сенсор IDS за день может выдавать до 50 тыс. сообщений, до 95 % ложных тревог.
- Сопоставить сигналы безопасности от разных систем безопасности практически невозможно.

Третья проблема, являющаяся следствием первой и второй, – существенное увеличение вероятности ошибок при конфигурировании аппаратного и программного обеспечения и анализе инцидентов безопасности в современных информационных системах (ИС) в ограниченное время.

Комплексное решение указанных проблем невозможно без построения автоматизированной системы управления информационной безопасностью предприятия.

Модель целей управления в виде дерева целей строится в соответствии со стратегическими и оперативными целями функционирования предприятия на основании ряда правил [1]. Например. Достижение пяти целей управления позволяет минимизировать остаточный риск информационной безопасности, а именно:

- минимизировать несанкционированный доступ к информационным ресурсам (ИР);
- защитить от вредоносного программного обеспечения (ПО);
- рационально использовать внутренний трафик;
- рационально использовать внешний трафик;
- рационально конфигурировать аппаратное и программное обеспечение.

Дерево целей для автоматизированной системы управления приведено в таблице.

Таблица

Дерево целей для автоматизированной системы управления

Номер узла	Описание цели
0	Минимизация остаточного риска информационной безопасности
1	Минимизация несанкционированного доступа к информационным ресурсам
1.1	Минимизация числа попыток доступа к информационным ресурсам (ИР) с неавторизованных рабочих мест
1.2	Минимизация числа попыток доступа к ИР с неавторизованным ПО
1.3	Минимизация числа прочих попыток несанкционированного доступа к ИР
1.3.1	Минимизация числа попыток перебора и подбора паролей
1.3.2	Минимизация числа попыток применения эксплоитов и атак на ИР
1.4	Минимизация числа нарушений регламента работы с ИР
1.4.1	Минимизация числа нарушений правил эксплуатации ИР
1.4.2	Минимизация случаев вмешательства в работу ИР и прикладного ПО для доступа к ИР
1.4.2.1	Обнаружение умышленного вмешательства
1.4.2.2	Обнаружение неумышленного вмешательства (установка несовместимого ПО и т.п.)
2	Защита от вредоносного ПО
2.1	Исключение вредоносных программ на ПК пользователей
2.2	Исключение потенциально опасных и запрещенных программ
2.3	Исключение потенциально опасных и запрещенных программ
2.3.1	Исключение сбоев по вине пользователя
2.3.2	Исключение сбоев по причине активного заражения компьютера вирусами
2.3.3	Исключение сбоев по техническим причинам, не зависящим от пользователя
3	Рациональное использование внутреннего трафика
3.1	Минимизация аномалий в локальном трафике КВС
3.2	Минимизация самовольных подключений сетевых устройств к ПК или КВС
3.3	Минимизация самовольного изменения сетевых настроек
4	Рациональное использование внешнего трафика
4.1	Минимизация аномалий и нарушений работы Интернета и борьба с ними
4.2	Своевременное обнаружение аномалий и нарушений в работе электронной почты и борьба с ними
5	Рациональное конфигурирование аппаратного и программного обеспечения
5.1	Минимизация случаев самовольной установки ПО
5.2	Минимизация случаев самовольного изменения аппаратной

Алгоритмы автоматизированной системы управления информационной безопасностью на основе данных мониторинга (событий безопасности), поступающих от множества агентов мониторинга [2], внедренных в компоненты ИС, вырабатывают множество управляющих воздействий для множества агентов управления, обеспечивающих достижение целей.

Схема взаимодействия автоматизированной системы управления информационной безопасностью и информационной системой предприятия представлена на рисунке.

ряда факторов. К ним относятся: сложность современных предприятий, нередко работающих во многих странах мира; быстро меняющиеся возможности бизнеса; изощренность и высокая скорость распространения сетевых угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Стоянова, О. В. Метод дерева целей для оценки эффективности использования информационных ресурсов / О. В. Стоянова, О. В. Зайцев // Программные продукты и системы. – 2009. – № 3. – С. 15–18

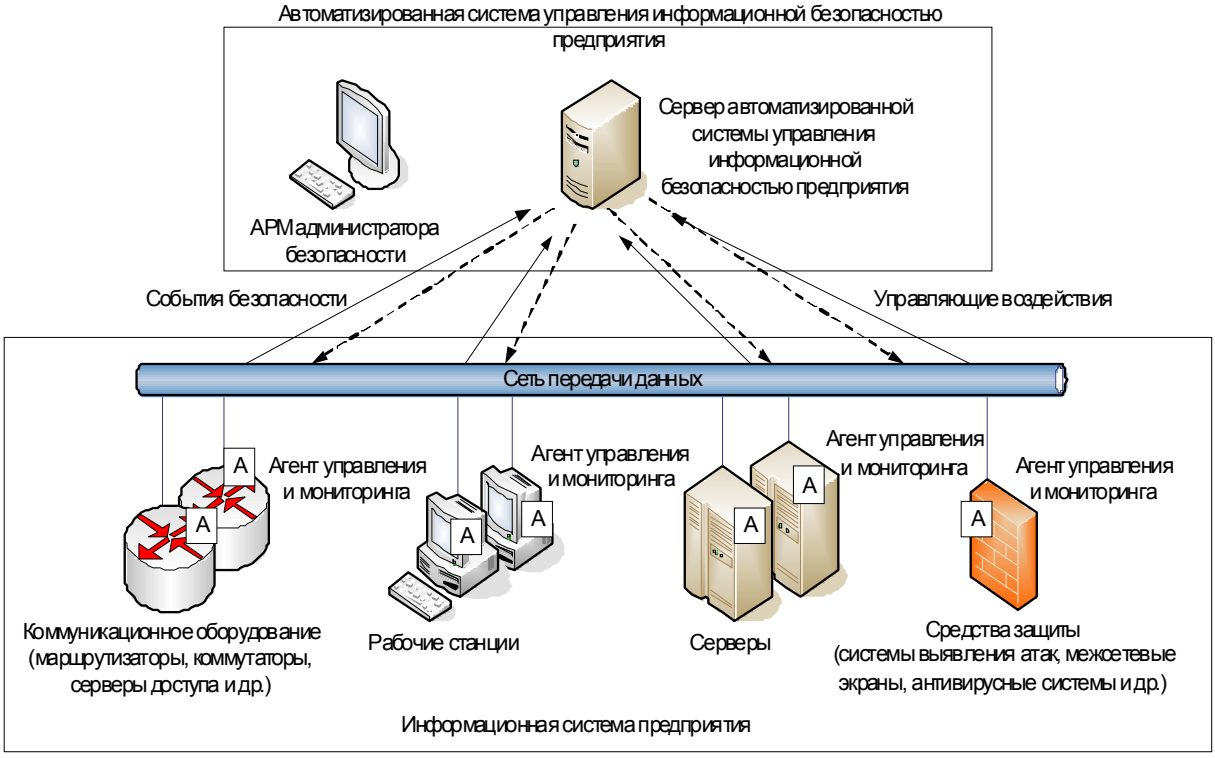

Схема взаимодействия автоматизированной системы управления информационной безопасностью и информационной системой предприятия

В настоящее время разрабатываются целевые алгоритмы автоматизированной системы управления информационной безопасностью предприятия.

Активный упреждающий подход к управлению системами безопасности является необходимостью для предприятий ввиду целого

2. Цыбулин, А. М. Исследование противоборства службы безопасности и злоумышленников на многоагентной модели / А. М. Цыбулин, А. В. Никишова, М. Ю. Умницын // Известия ЮФУ. Технические науки. Тематический вып. Информационная безопасность. – Таганрог : Изд-во ТТИ ЮФУ, 2008. – № 8 (85). – С. 94–99.

THE CONSTRUCTING APPROACH TO THE ENTERPRISE'S AUTOMATED INFORMATION SECURITY MANAGEMENT SYSTEM

A.M. Tsybulin

Increasing the information security management by centralized (automated administrator workplace) and decentralized (the intelligent agents complex) combining of monitor and audit of information security management at the enterprise; the development of a solutions set and synthesis of optimal solutions for improving information security.

Key words: *automated information security management system of enterprise, Intrusion Detection system, information security, multi-agent system, agent-based system modeling language.*