Тип работы: Научно-исследовательская работа

Предмет: Информационные системы и процессы

Оглавление

Введение

В связи с увеличением объемов информации, циркулирующих в локальных вычислительных сетях (ЛВС) и расширением спектра задач, решаемых с помощью информационных систем (ИС), возникает проблема, связанная с ростом числа угроз и повышением уязвимости информационных ресурсов.

Существует ряд факторов, действие которых влияет на это. Рссмотрим эти факторы:

- расширение спектра задач, решаемых ИС;
- повышение сложности алгоритмов обработки информации;
- увеличение объемов обрабатываемой информации;
-усложнение программных и аппаратных компонентов ЛВС, и соответственно - повышение вероятности наличия ошибок и уязвимостей;
- повышение агрессивности внешних источников данных (глобальных сетей);
- появление новых видов угроз.

От функционирования информационной системы и целостности информационных систем зависит функционирование предприятий и роль на рынке.

Исходя из этого, возрастают требования к системам защиты ЛВС, которые должны обеспечивать не только пассивное блокирование несанкционированного доступа к внутренним ресурсам сети предприятия из внешних сетей, но и осуществлять обнаружение успешных атак, анализировать причины возникновения угроз информационной безопасности и, по мере возможности, устранять их в автоматическом режиме.

Поэтому основным качеством системы защиты можно считать адаптивность.

Адаптивность – это способность или готовность меняться в соответствии с различными условиями, анализировать информацию и менять конфигурацию.

Анализ существующих подходов к реализации систем обнаружения атак показывает, что большинство программных продуктов, присутствующих в настоящее время на рынке, ориентируется на использование формальных

описаний системной активности (сигнатур).
Функции обнаружения и регистрации новых видов атак возлагаются в подобных системах на разработчика, выпускающего новые сигнатуры.
Данный метод защиты является ненадежным, т.к. он ставит защищенность ИС в зависимость от действий внешнего неконтролируемого источника.
Несмотря на то, что разработка адаптивных систем защиты информации ведется уже достаточно длительное время, ни одно подобное решение не получило сколько ни будь широкого распространения в силу сложности и малоэффективное используемых алгоритмов, отсутствия в большинстве случаев адекватных инструментов их развертывания и администрирования, а также - пользовательской документации.
Проанализировав работы, ведущиеся в данной области, мы пришли к выводу что проблема требует дальнейшего изучения. А так же требует реализации эффективных алгоритмов обнаружения атак и принятия решений.
Объект исследований - система защиты информации корпоративной информационной системы.
Предмет исследований - алгоритмическое и программное обеспечение защиты информации.
Цель работы - повышение эффективности обнаружения атак и принятия решений на основе оперативной оценки риска функционирования ИС с использованием динамических моделей на основе нечетких когнитивных карт.

5
1. Информационная атака

Информационная безопасность — это состояние информации, информационных ресурсов и информационных систем, при котором обеспечивается защита информации или данных от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования информации и т.п.
Для начала нужно определить что такое атака. И только потом можно обсудить способы выявления атак
Итак, информационная атака (вторжение) — совокупность действий нарушителя, направленная на реализацию угрозы информационной безопасности АС.
Результатом успешной атаки может стать, например, несанкционированный доступ нарушителя к информации, хранящейся в ИС, потеря работоспособности системы или искажение данных в ИС.
В качестве целей атаки могут рассматриваться серверы, рабочие станции пользователей или коммуникационное оборудование ИС.
При организации информационных атак злоумышленники часто используют специализированное ПО, позволяющее автоматизировать действия, выполняемые на различных стадиях атаки.

1.1. Стадии обнаружении атак
Обычно, любая атака делится на четыре стадии (рис. 1).

6
Рис.1. Жизненный цикл типовой атаки

Рекогносцировка.
Эта стадия характеризуется получением информации об объекте применения атаки. Для дальнейшего планирования злоумышленником этапов

дальнейшего вторжения. Цель нарушителя получить максимальное количество информации.
Этим целям может служить, например,
-информация о типе и версии ОС,
- установленной на хостах ИС;
-список пользователей, зарегистрированных в системе;
-сведения об используемом прикладном ПО и т. д.
Вторжение.
На этой стадии нарушитель получает несанкционированный доступ к ресурсам тех хостов, на которые совершается атака.
Атакующее воздействие.
Эта стадия характеризуется действием, т.е. реализацией поставленных целей злоумышленников. Целью можно считать, например, кража данных или модификация системы.

1. Технические обзоры интернет ресурс: https://selectel.ru/blog/ips-and-ids/
2. Политическая лингвистика. 6 (66)'2017 интернет ресурс file:///C:/Users/Пользователь /Downloads/informatsionnaya-ataka-ponyatie-i-ontologicheskie-svoystva.pdf
3. Безопасность интернет ресурс https://www.bytemag.ru /articles/detail.php?ID=9036
4. Библиофонд Системы обнаружения атак интернет ресурс https://www.bibliofond.ru/view.aspx?id=785519
5. Сетевая система обнаружения вторжений интернет ресурс https://ru.wikipedia.org/wiki/Сетевая_система_обнаружения_вторжений
6. Все об Open Source интернет ресурс https://www .igromania.ru/article/3956/Vse_ob_Open_Source._Plyusy_i_minusy_programm _s_otkrytymi_ishodnymi_kodami.html#