**КОНТРОЛЬ СОСТОЯНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И НАСТРОЕК ОПЕРАЦИОННОЙ СИСТЕМЫ**

**Аннотация.** Цель статьи заключается в рассмотрении проблем, связанных с проведением контроля соответствия настроек средств защиты информации и компонентов операционной системы.

**Ключевые слова:** аудит, информационная безопасность, средства защиты информации, компьютерная атака.

Информационные системы (ИС), на которых обрабатывается информация ограниченного доступа, должны соответствовать требования нормативных, руководящих и методических документов. В нормативных документах предъявляются требования к средствам защиты информации, классам АС. Контроль за соблюдением требований руководящих документов осуществляет администратор безопасности (АБ) информации. В настоящее время проверка соответствия конфигурации требованиям руководящих документов проводится вручную. Принимая во внимание влияние человеческого фактора, есть вероятность ошибки первого и второго рода.

Программное обеспечение (ПО) входящее в состав ИС можно разделить на несколько классов:

– операционная система (ОС) и ее компоненты;

– специализированное ПО;

– прикладное ПО.

Операционная система состоит из ядра и драйверов, которые реализуют базовые функции ИС. Проведение успешной компьютерной атаки на ОС позволяет злоумышленнику обойти или отключить все средства защиты работающее на данном уровне и более высоких уровнях. Для проведения атак злоумышленник может использовать уязвимости в коде ОС. Своевременная установка обновлений позволяет устранить известные уязвимости кода, поэтому наличие критических обновлений является важным параметром защищенности ИС. Конфигурация ОС по умолчанию, часто является недостаточной для обеспечения требуемого уровня защищенности и требует дополнительной настройки со стороны АБ. При настройке ОС следует обратить внимание на следующие настройки системы:

– настройка сетевых сервисов и служб;

– настройка общих ресурсов;

– параметры аутентификации и идентификации;

– параметры разграничения доступа;

– настройки СЗИ.

Одним из основных алгоритмов обнаружения угроз современного антивирусного ПО является сигнатурный анализ, использующий для работы базы сигнатур вредоносного ПО. Компании, разрабатывающие САВЗ, добавляют сигнатуры в базы по мере выявления новых атак, поэтому эффективность САВЗ зависит от наличия актуальных баз вирусных сигнатур. Кроме обновления на безопасность ИС также влияют настройки компонентов антивирусного ПО. Пользователи в целях достижения личного блага вносят изменения в настройки конфигурации СЗИ, что снижает уровень защищенности ИС. С другой стороны, «жесткая» настройка СЗИ, может привести к снижению доступности данных, обрабатываемых ИС.

Класс прикладного ПО достаточно разнообразен и включает в себя текстовые и графические редакторы, браузеры, программы для просмотра изображений и документов, почтовые клиенты и т.п. Главным параметром, определяющим безопасность использования прикладного ПО, является версия, используемого ПО. Использование неактуальных версий ставит под угрозу безопасность ИС из-за наличия в них известных уязвимостей.

Основной трудностью при контроле параметров настроек ПО и СЗИ требованиям нормативных документов является то, что они расположены в различных каталогах, ветках реестра и имеют различный формат хранения. Что совместно с огромным количеством настроек, требует огромного служебного времени АБ.

В настоящее время контроль настроек СЗИ проводится АБ вручную: администратор просматривает параметры и настройки на исследуемой системе и проверяют их на соответствие требованиям руководящих документов. При этом возникают следующие проблемы:

– вероятность пропустить ряд параметров из-за невнимательности, либо из-за недостаточной квалификации специалистов

– неправильная трактовка текстов документов;

– большие временные затраты из-за необходимости искать и просматривать каждый параметр.

Исходя из вышеуказанного, следует что необходимо разработать алгоритм автоматизации действий администратора при проведении аудита настроек ПО и СЗИ.

Разработка алгоритмов имеет следующие этапы:

1. Сбор информации о системе. На этом этапе производится считывание значений всех параметров, которые могут влиять на защищенность ИС, и сохранение их в едином формате.
2. Сравнение значений параметров. После сбора информации происходит сравнение значений параметров с эталоном. Под эталоном понимается сохранение значений параметров, собранных с ИС, настройки которой соответствуют требованиям руководящих документов.
3. Анализ расхождений. Для параметров значение которых отличается от эталонного значения, вычисляется уровень опасности.
4. Формирование отчета. На данном этапе производится формирование и сохранение отчета в требуемой форме.

В настоящее время при проведении аудита настроек ПО и СЗИ производятся АБ вручную. Это приводит к возникновению ошибок, связанных с человеческим фактором. Также из-за большого количества параметров и различных способов хранения параметров проверка занимает продолжительное время АБ. Поэтому целесообразно разработать программный комплекс, позволяющий автоматизировать сбор, анализ информации и формирование отчета, а также упростить работу АБ, и как следствие снизить человеческий фактор.

Список литературы:

1. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК от 18 февраля 2013 г. №21
2. ГОСТ Р 50922-96. Защита информации. Основные требования и определения.
3. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. ГОСТ Р ИСО/МЭК 15408-2-2002

© В.А. Варганов, Ю.А. Кузнецов, Д.В. Домрачев