УДК 004.056:378(06)

ВИРТУАЛЬНОЕ МЕСТО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Фадин А.А. и Щербина С.А.

(Всероссийская конференция «БИТ», МГТУ им.Н.Э.Баумана, 2010 г.)

В современном мире IT-инфраструктура проникла практически в каждую организацию, и все они сталкиваются с набором как внешних, так и внутренних угроз в области информационной безопасности. В зависимости от размеров этой организации, характера её деятельности и других факторов – в том или ином виде определяются цели и задачи по обеспечению конфиденциальности, целостности и доступности обрабатываемой информации. Формируется политика информационной безопасности.

Но этот документ останется ничего не значащей бумагой, если нет людей, ответственных за контроль её внедрения и обеспечения. Среди них одну из важных ролей занимает администратор информационной безопасности.

Следует указать, что согласно руководящему документу Гостехкомиссии России наличие отдельного места (терминала) администратора безопасности в АС является обязательным условием оценки соответствия и ввода в эксплуатацию системы [1]. В тоже время данная задача имеет особое актуальное значение в связи с обязательными требованиям по использовании систем анализа защищенности (а не только тестирования [2, 3]) в распределенных системах защиты персональных данных [4].

1. Администратор информационной безопасности (защиты). Задачи и направления деятельности. Инструменты системного администратора.

В соответствии с определением, приведенном в руководящем документе Гостехкомиссии России «Защита от несанкционированного доступа к информации: Термины и определения», администратор защиты – это субъект доступа, ответственный за защиту автоматизированной системы (АС) от несанкционированного доступа (НСД) к информации.

Как обеспечить эту защиту? Если речь идёт о технической защите информации, то здесь мы сталкиваемся с целым комплексом различных программных и программно-аппаратных средств защиты информации.

Помимо таких широко известных и распространенных средств как межсетевые экраны (МЭ), антивирусы, средства доверенной загрузки и создания доверенной среды, а также системы обнаружения вторжений (СОВ) – однако требуются и средства другого рода, обеспечивающие проверку работы всех вышеперечисленных продуктов.

Необходимы средства, которые администратор информационной безопасности сможет использовать для тестирования защищенности, как сети, так и отдельных автоматизированных рабочих мест (АРМов).

Рассмотрим типовой набор операций, относящийся к анализу защищенности АС. Администратору безопасности необходимо:

- получать оперативную информацию о составе и структуре сети, открытых сервисах;
- проводить тестирование на предмет наличия известных уязвимостей (penetration testing);

- осуществлять контроль стойкости используемых паролей;
- контролировать целостность критически важной информации;
- контролировать и при необходимости изучать сетевой трафик между выбранными узлами сети;
- тестировать систему гарантированной очистки информации;
- проводить системный аудит ЭВМ из состава АС (аппаратная, программная конфигурация, журнал).

2. Требования к месту администратора информационной безопасности.

Перечислим основные требования к среде и месту работы администратора информационной безопасности системы:

1) Защита от НСД к информации, обрабатываемой администратором безопасности на рабочем месте (пароли, ключи, результатов аудита АС и др.)

Данное требование может быть обеспеченно доверенной средой, в которой работает администратор и применением одним из двух механизмов к защите данной информации – либо гарантированная очистка данных по завершению работы, либо их шифрование при хранении.

2) Мобильность (переносимость) места администратора безопасности (возможность подключиться к произвольному сегменту сети и выполнить локальную проверку каждого АРМ).

3) Полнота инструментария – важно, когда все необходимые для работы средства доступны «из коробки», а операция по их развертыванию (deployment) требует минимум времени и усилий со стороны администратора.

4) Сертификация – для работы в средах, обрабатывающих информацию с ограниченным доступом администратору безопасности необходимо использовать сертифицированные средства защиты

3. Мобильное место администратора безопасности на примере средства анализа защищенности «Сканер-ВС»

В качестве примера мобильного средства (а точнее комплекса средств) по анализу защищенности рассмотрим продукт «Сканер-ВС» компании ЗАО «НПО «Эшелон».

Он представляет собой носитель, в зависимости от поставки или загрузочный компакт-диск (LiveCD), или USB-флэш (LiveFlash), который запускает свою собственную среду для работы, операционную систему (производная от Linux), данный подход позволяет нам выполнить первые два требования, поскольку данный носитель может быть установлен фактически в любой x86-совместимый компьютер, не нарушая целостности его программной среды, а вся обрабатываемая администратором информация хранится лишь в оперативной памяти, что гарантирует её очистку по завершению работы (по желанию администратора отчеты и другие данные могут быть сохранены на внешний носитель).

Данный продукт выполняет требование №4, поскольку имеет сертификаты соответствия Минобороны России и ФСТЭК России.

В соответствии с пунктом 3 рассмотрим функционал Сканера-ВС, помимо других продуктов в него входит:

1) Сетевой сканер.
2) Сканер безопасности, средство поиска уязвимостей в сети.
3) Аудитор паролей.
4) Контроль целостности файлов, папок, секторов на диске и др. объектов.

5) Анализатор трафика, средство перехвата (снифинга) сетевого трафика и контроля передаваемой информации.

6) Общесистемный анализатор.

7) Средство проверки системы гарантированной очистки.

Список литературы

1. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (Гостехкомиссия, 1992 г.) - http://www.fstec.ru/_docs/doc_3_3_004.htm

2. Марков. А.С., Щербина. С.А. Испытания и контроль программных ресурсов // Information Security - 2003 - № 6. - http://www.egovernment.ru/attachments/insec01-2004/25.pdf

3. Выбор сетевого сканера для анализа защищённости сети / А.С. Марков, С.В. Миронов, В.Л. Цирлов // Byte - 2005 - №6.

4. Информационный портал по защите персональных данных ИСПДн.ру – http://www.ispdn.ru