СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Обеспечение надежной защиты информации от несанкционированного доступа (НСД) со стороны нарушителей и воздействия вредоносного кода при ее обработке, хранении и передаче с использованием средств вычислительной техники является важнейшим направлением деятельности специалистов в сфере информационной безопасности.

По этой причине в содержании ФГОС направлений подготовки и специальностей, относящихся к УГСНП «Информационная безопасность», изучение дисциплины «Программно-аппаратные средства защиты информации» или родственных ей «Программно-аппаратные средства обеспечения информационной безопасности», «Программно-аппаратная защита информации» является обязательным.

В процессе изучения этих дисциплин, наряду с обязательным рассмотрением теоретических вопросов, значительное внимание должно уделяться приобретению навыков использования средств программно-аппаратной защиты информации.

В книге, предлагаемой вниманию читателя, подробно описываются практические аспекты применения сертифицированных ФСТЭК РФ продуктов – средства защиты информации от несанкционированного доступа (СЗИ от НСД) Dallas Lock 8 и средства антивирусной защиты (САВЗ) Kaspersky Endpoint Security 10 для Windows.

В процессе изучения работы с СЗИ от НСД Dallas Lock 8 рассматриваются вопросы настройки механизмов авторизации, контроля и аудита доступа пользователей к объектам файловой системы и внешним устройствам. Исследуются особенности настройки механизмов гарантированной очистки информации и замкнутой программной среды, использования криптографических методов защиты информации, контроля целостности, мандатного доступа пользователей к объектам файловой системы и съемным носителям, работы приложений в сессиях с различными уровнями конфиденциальности.

Проблематика обеспечения защиты информации от воздействия вредоносных программ и сетевых атак рассмотрена с использованием средства антивирусной защиты информации Kaspersky Endpoint Security 10 для Windows.

Поскольку специалист в области информационной безопасности должен знать положения основных нормативных документов, регулирующих его деятельность, в практикум добавлена работа, посвященная изучению положений Постановления Правительства РФ от 01.11.2012 № 1119, Приказов ФСТЭК РФ № 21 от 18.02.2013, № 17 от 11.02.2013 и ряда других документов.

Практикум может быть использован для обучения студентов высшего образования:

– направления подготовки бакалавриата «Информационная безопасность» при изучении дисциплины «Программно-аппаратные средства защиты информации»;

– специальностей «Информационная безопасность телекоммуникационных систем» и «Информационная безопасность автоматизированных систем» при изучении дисциплины «Программно-аппаратные средства обеспечения информационной безопасности»;

– специальностей «Информационно-аналитические системы безопасности» и «Компьютерная безопасность» при изучении дисциплин, рассматривающих вопросы применения средств программно-аппаратной защиты информации;

– специальности «Безопасность информационных технологий в правоохранительной сфере» при изучении дисциплины «Программно-аппаратная защита информации».

Также использование материалов лабораторного практикума возможно в процессе преподавания дисциплины «Информационная безопасность» или родственных ей, для студентов высшего образования, обучающихся по следующим специальностям и направлениям подготовки: «Информатика и вычислительная техника», «Информационные системы и технологии», «Прикладная информатика», «Программная инженерия», «Бизнес-Информатика», «Экономическая безопасность».

Изложенный в книге материал способствует выполнению трудовых функций профессиональных стандартов специалистов, чьей сферой деятельности являются:

1) обеспечение информационной безопасности объектов информатизации;

2) проектирование, разработка и обслуживание информационных систем.

Лабораторный практикум может использоваться как в процессе проведения аудиторных занятий, так и при осуществлении самостоятельной работы студентов. Для выполнения заданий требуется следующее программное обеспечение:

1) VMware Player (предпочтительнее) или Virtual Box для запуска виртуальных машин, работающих под управлением операционных систем семейств Windows. Также задания практикума можно выполнять на обычных компьютерах без использования технологии виртуализации;

2) желательно наличие принтера, при его отсутствии можно использовать виртуальные принтеры;

3) учебная или коммерческая версии СЗИ от НСД Dallas Lock 8.0 редакций «К» или «С». Редакция «С» требуется для выполнения последней работы;

4) средство антивирусной защиты Kaspersky Endpoint Security 10 для Windows с постоянной или временной (trial) лицензией;

5) пакет офисных программ MS Office или Open Office;

5) свободно распространяемый сетевой сканер Nmap;

6) средство просмотра pdf файлов Adobe Acrobat Reader или другое.

Для выполнения некоторых лабораторных работ потребуется развернуть локальную сеть в соответствии с одной из схем, приведенных в приложении. По этой причине использование виртуальных машин является наиболее удобным вариантом.

Элементы графического интерфейса программных продуктов Kaspersky Endpoint Security 10 для Windows и Dallas Lock 8.0 могут иметь незначительные отличия от представленных в книге рисунков.

Материалы, изложенные в книге, могут быть полезны практическим работникам, чьей сферой деятельности является обеспечение информационной безопасности.

Свои пожелания или критические замечания относительно приведенного в книге материала можно высылать на электронный ящик автора:
yaroslav-prokushev2@mail.ru

Лабораторная работа 6. Настройка аудита доступа к объектам файловой структуры и внешним устройствам в Dallas Lock (фрагмент)

Цель работы: получение навыков настройки подсистемы аудита доступа пользователей к файловым объектам и используемым внешним устройствам на защищаемом Dallas Lock 8 компьютере. Получение навыков анализа действий пользователей на защищаемом Dallas Lock 8 компьютере.

Теоретическая информация

При рассмотрении функциональных возможностей семейства операционных систем Windows было показано, что используемая в них модель разграничения доступа к объектам файловой системы и внешним устройствам не в полной мере соответствует предъявляемым требованиям. Такая же картина наблюдается и при рассмотрении возможностей, которые предоставляет Windows для обеспечения аудита действий пользователей. Так, например, подсистема аудита в Windows имеет следующие недостатки:

1) крайне тяжело отследить подключение внешних устройств. Об их использовании лишь можно догадываться по наличию некоторых событий в операционной системе. Понять, какая информация была скопирована на внешние устройства, весьма затруднительно;

.....

4) В журналах Windows достаточно тяжело искать записи о событиях.

Поэтому использование добавочных средств защиты, позволяющих в полной мере обеспечить требования к аудиту действий пользователей, необходимо. В подсистеме аудита действий пользователей в Dallas Lock указанных недостатков не наблюдается. Предусмотрено несколько журналов, события в которые записываются в зависимости от типа (вход в систему, печать документа, запуск программы, доступ к файлу и т.п.), что облегчает поиск интересующей администратора безопасности информации (рис. 39):

– входов в систему. Регистрирует входы и выходы в защищаемую систему, доступ к сетевым ресурсам, попытки входа на защищаемый компьютер:

– управления учетными записями;

– ресурсов;

– печати;

– управления политиками;

– процессов;

– из сохраненного ранее файла.

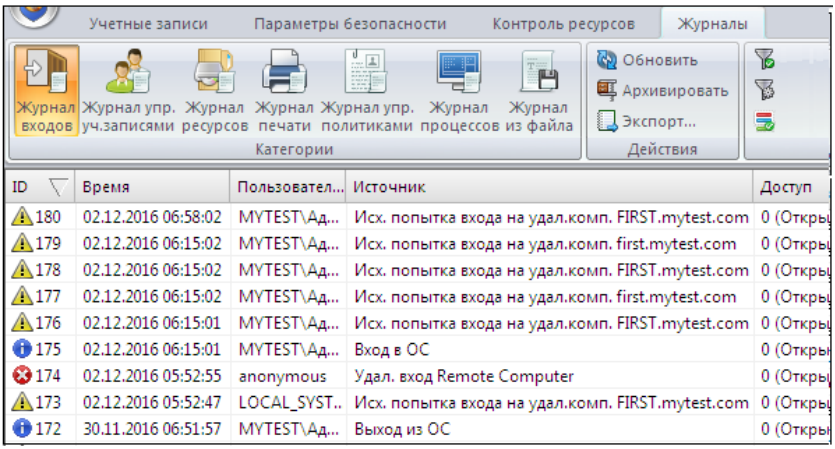

Рис. 39. *Журналы учета работы пользователей*

По умолчанию в журналах хранится до 20000 записей о событиях. После переполнения журнал архивируется и помещается в специальный каталог «C:\DLLOCK80\Logs». Действующие журналы хранятся в каталоге «C:\ DLLOCK80\Jrn». Файлы журналов и их архивы хранятся в зашифрованном виде и недоступны для просмотра или изменения со стороны обычных пользователей. Чтобы события вносились в журналы аудита, в системе защиты необходимо установить соответствующие настройки. Для этого надо открыть вкладку «Параметры безопасности», а в ней закладку «Аудит» (рис. 40).

Чтобы настройки аудита позволяли отслеживать наиболее существенные действия пользователей в защищаемой системе, а также соответствовали требованиям, предъявляемым к защите персональных данных, следует включить аудит следующих событий [8]:

– входов пользователей в систему;
– доступа пользователей к ресурсам;
– управления политиками безопасности и учетными записями;
– печати (с целью контроля утечки информации с помощью ее вывода на твердую копию);
– запуска и завершения процессов;
– запуска и остановки операционной системы;
– исходящие попытки входа на удаленные компьютеры;
– запуска и остановки модулей администрирования Dallas Lock;

– устройств (включать необходимо, поскольку неконтролируемый вывод информации на внешние носители, как правило, приводит к утечке значительного объема защищаемой информации);

– создавать теневые копии распечатываемых документов. Этот параметр позволяет контролировать вывод информации пользователями, поскольку появляется возможность анализа содержимого выведенных на печать файлов. «Теневые копии» помещаются в специальный каталог «C:\ DLLOCK80\Logs\PrintCopy», где их могут просмотреть пользователи, обладающие соответствующими правами;

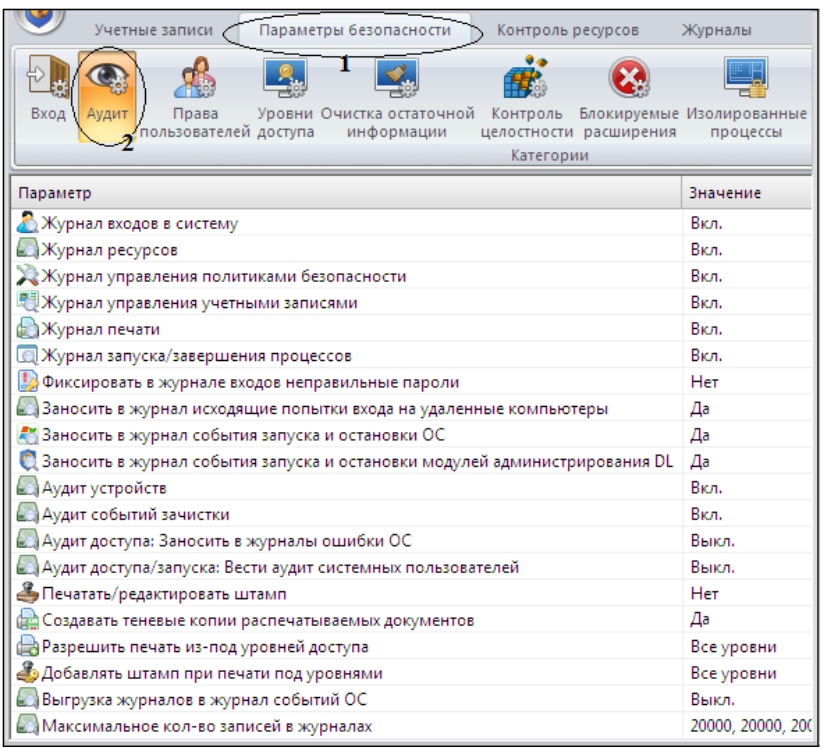

Рис. 40. *Настройка учета событий по категориям*

– разрешать печать из-под уровней доступа. Этот параметр имеется только в версии Dallas Lock 8C. С его помощью можно установить или запретить печать документов определенной степени важности. Например, если используется система управления потоками, то можно заблокировать печать персональных данных

Внесение в журнал событий операционной системы, аудит системных пользователей можно не включать. Учет событий операционной системы, как правило, требуется при анализе противоречий в настройках систем безопасности Windows и Dallas Lock. Например, доступ к каталогу был разрешен в Dallas Lock, но пользователь не может его открыть. В этом случае следует внимательно рассмотреть права, назначенные в Windows.

Аудит системных пользователей, к которым относятся такие учетные записи, как System, Local Service, Network Service и пр., требуется, если в работе приложений и служб (например, таких как MS SQL Server), стартующих под этими учетными записями, происходят сбои.

Печать штампа чаще всего не требуется.

Выгрузка журналов Dallas Lock в журнал событий ОС также обычно не требуется. Аудит в Dallas Lock организован лучше, поэтому более вероятным будет решение обратной задачи.

Параметр «максимальное количество записей в журналах» устанавливается для каждого журнала индивидуально. Корректировать начальное значение, равное 20000, обычно не следует.

Задание 1. Самостоятельно настроить параметры аудита действия пользователей на компьютере KADR так, как показано на рисунке 41.

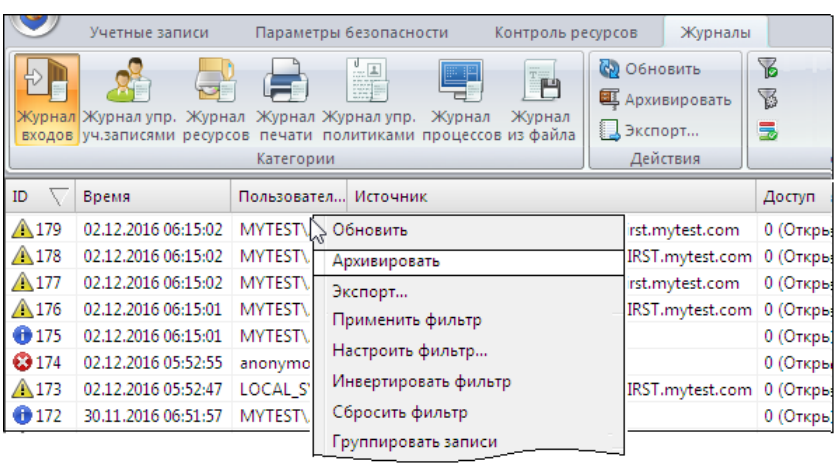

Рис. 41. *Архивация журналов аудита Dallas Lock*

Задание 2. Выполнить архивацию (аналог очистки) всех журналов, кроме журнала управления учетными записями. Архивация в данном

случае выполняется в учебных целях, чтобы в дальнейшем при выполнении заданий можно было легче искать требуемую информацию.

Архивированные журналы помещаются в каталог «C:\DLLOCK80 \Logs».

Задание 3. Подготовить отчет о действиях с учетными записями.

Чтобы составить отчет, необходимо выполнить следующую последовательность действий:

1. Открыть закладку журнала управления учетными записями. В нем должны отображаться все изменения, связанные с настройкой учетных записей пользователей.

2. Нажать на кнопку «Экспорт», расположенную справа на вкладке журнала.

.....