V.S. Oladko

Monitoring and Auditing Residual Information on the User's Computer

Key words: residual information, monitoring, audit, risk, information leaks

This paper considers the problem of violation of information security components such as confidentiality and availability in the event of a computer user's residual information. Analyze the requirements of regulators and mechanisms to be applied in the organization to monitor the residual information or its destruction.Approach to monitoring and auditing residual information on the user's computer, which allows monitoring the residual information in certain areas proposed. Approach allows us to identify the detected information and rank it according to the degree of criticality, as well as calculate the risk of leakage and its potential to develop recommendations aimed at its reduction. The proposed approach is formally described and automated in a software system.

В.С. Оладько

МОНИТОРИНГ И АУДИТ ОСТАТОЧНОЙ ИНФОРМАЦИИ НА КОМПЬЮТЕРЕ ПОЛЬЗОВАТЕЛЯ

Введение

Основу любой информационной системы (ИС) предприятия и организации составляют компьютеры, представляющие собой сервера и автоматизированные рабочие места пользователей, которые предназначены для реализации ключевых бизнес-процессов организации. В то время, когда пользователь работает на компьютере, в нем постоянно фиксируется различная информация о его деятельности, накапливаются лишние данные, которые могут быть как конфиденциальной информацией, персональными данными пользователей, так и временными файлами, необходимыми для работы различных приложений и программ. Со всеми этими данными связаны две основные проблемы:

- возможность несанкционированной утечки конфиденциальных данных, несущая непосредственный ущерб информационной безопасности организации;
- нерациональное использование ресурсов системы, поскольку остаточная информация содержащая «мусор» занимает лишнее место на жестком диске, не позволяет использовать объем жесткого диска по максимуму, увеличивает время доступа к информации и, в общем, замедляет систему.

Таким образом, контроль над наличием остаточной информации на компьютерах ИС предприятия, ее своевременном удалении и уничтожении является одной из актуальных задач при обеспечении таких ключевых составляющих информационной безопасности организации, как конфиденциальность и доступность информации.

Под остаточной информацией в рамках данной работы автором будет пониматься информация на запоминающем устройстве, оставшаяся от формально удалённых операционной системой данных, или временные файлы, создаваемые прикладными программами в процессе работы.

Остаточная информация и причины ее появления

Остаточная информация появляется на компьютерах ИС (рабочих станциях пользователей, серверах) в результате работы пользователей при выполнении своих долж-

ностных обязанностей, при функционировании ОС и различного рода программных приложений. Остаточная информация обычно представляет собой как удаленные данные и файлы пользователей, так и служебную информацию, полученную в результате работы прикладного (СУБД, браузеры и т.п.) и системного ПО (ОС), а также специализированных служб. Одна информация может иметь конфиденциальный характер, другая просто занимать ресурсы ИС и приводить к нарушению работоспособности и доступности элементов ИС.

Анализ литературных источников [1, 2] показывает, что основными видами остаточной информации являются: удаленные файлы пользователей; ключи реестра (списки запускавшихся приложений, результаты поиска, информация о подключенных сетевых дисках и внешних устройствах, сведения о работе разнообразных установленных программ.); лог-файлы; история посещений сайтов;cookie;временные файлы в кеше; временные файлы о работе системы, сохраненные в dat файлах.пароли для доступа к вебсайтам.

Причины появления и накопления остаточной информации на компьютерах пользователей в ИС заключаются в первую очередь в том, что многие ОС, файловые менеджеры и другое ПО предоставляют возможность не удалять файл немедленно, а перемещать файл в корзину. Это делается для того, чтобы пользователь мог исправить свою ошибку в случае неумышленного удаления информации. Но даже если возможность обратимого удаления явно не реализована, или пользователь не применяет её, большинство ОС, удаляя файл, не удаляют содержимое файла непосредственно, а просто удаляют запись о файле из директории файловой системы. Содержимое файла – реальные данные – остаётся на запоминающем устройстве. Данные существуют до тех пор, пока ОС не использует заново это пространство для новых данных. Во множестве систем остаётся достаточно системных метаданных для несложного восстановления при помощи широко доступных утилит. Даже если восстановление невозможно, данные, если они не были перезаписаны, могут быть прочитаны ПО, читающим сектора диска напрямую. Программно-техническая экспертиза часто применяет подобное ПО.

Также при форматировании, переразбиении на разделы или восстановлении образа системой не гарантируется запись по всей поверхности, хотя диск и выглядит пустым или, в случае восстановления образа, на нём видны только файлы, сохранённые в образе. Кроме того, если запоминающее устройство перезаписывается, физические особенности устройств делают возможным восстановление информации при помощи лабораторного оборудования благодаря, например, явлению остаточной намагниченности. Кроме того, помимо доступа к остаточной информации и файлам пользователей на жестком диске злоумышленник для получения несанкционированного доступа может использовать информацию браузера о паролях и страницах, которые посетил пользователь.

Анализ методов защиты, применяемых при присутствии остаточной информации на компьютере

Поскольку присутствие на компьютерах остаточной информации может стать причиной нарушения информационной безопасности в ИС предприятия, то возникает необходимость в использование специализированных средств и методов защиты, направленных на контроль за присутствием остаточной информации на компьютере и ее своевременное удаление в случае необходимости. Выбор конкретного метода также зависит от уровня секретности информации, подвергаемой уничтожению. Например, для предприятий ИС, которые обрабатывают информацию открытого доступа и конфи-

денциальные данные, использование методов гарантированного уничтожения не является обязательным. В автоматизированных системах, аттестованных по классам защищенности 3А, 2А, 1А, 1Б, 1В и 1Г, в соответствии с требованиями, определенными в стандартах и руководящих документах ФСТЭК России [3, 4], должна производиться очистка внешней памяти путем двукратной произвольной записи или путем записи в нее маскирующей информации.

Таким образом, все направления по обеспечению информационной безопасности при наличии на компьютере остаточной информации разделяются на три группы:

- методы выявления и контроля над остаточной информацией на компьютере, реализуемые средствами аудита и мониторинга;
- методы перезаписи информации на носителях и оперативной памяти;
- методы уничтожения носителя информации.

Первый метод, основанный на мониторинге и аудите остаточной информации, в основном направлен на поиск, классификацию и выявление в определенных областях остаточной и вспомогательной информации, полученной в результате работы пользователей и приложений, после чего выявленная остаточная информация может быть по выбору пользователя удалена. Данный метод может применяться в ИС любых предприятий отдельно от других методов либо в комбинации со вторым и третьим. Как показывает анализ [2], к средствам мониторинга и аудита остаточной информации на компьютере, которые могут использоватьсякак для домашнего использования, так и в ИС предприятий, не обрабатывающих секретную информацию, относятся Wide 2-13 Build, Ccleaner, RegCleaner, R-Wipe & Clean другие.

Второй и третий методы направлены на гарантированное уничтожение и/или многократную перезапись информации, расположенной на носителях, и являются обязательными для АИС, обрабатывающих секретную информацию начиная с 3-го класса защищенности. В соответствии с [1, 4] методы гарантированного уничтожения информации делятся на физические, программные, аппаратные, механические, термические, радиационные и другие. Как правило, средства, реализующие программно-аппаратные методы, поставляются в виде отдельных систем – СГУ-2, «Стек-НС1в», «ФИКС», TERRIER 3.0 или входят в состав сертифицированных ФСТЭК России программно-аппаратных средств защиты информации, например, таких как SecretNet, Dallas Lock, Аккорд и другие.

В рамках данной работы при разработке подхода к мониторингу и аудиту остаточной информации будут рассматриваться ИС небольших предприятий, обрабатывающие только конфиденциальную информацию, в которых не требуется использовать сертифицированные ФСТЭК России средства гарантированного уничтожения информации на носителях.

Подход к мониторингу и аудиту остаточной информации на компьютере пользователя

Для повышения уровня безопасности в компьютерах ИС предприятия и защиты от внутреннего злоумышленника, авторомпредлагается подход к мониторингу и аудиту остаточной информации на компьютере, обеспечивающий выполнение следующих функций на трех этапах, представленных в табл. 1.

Таблица 1. Функции мониторинга и аудита остаточной информации на компьютере

Функции	Этапы аудита
Формирование списка файлов и ключевых слов, по которым будет осуществляться поиск остаточной информации на компьютере Формирование списка областей для поиска остаточной информации на компьютере пользователя	Этап 1 – Сбор данных (мониторинг)
Поиск остаточной информации по сформированному списку в указанных областях компьютера Идентификация обнаруженной остаточной информации	
Ранжирование выявленной остаточной информации по степени важности и оценка рисков от потенциальной утечки	Этап 2 – Анализ данных аудита
Формирование отчета по результатам аудита и выдача рекомендаций администратору безопасности	Этап 3 – Выработка рекомендаций и формирование аудиторского отчета

Формально данный подход можно представить в виде следующей функции:

$$SysAMRI = RPT(RI, RISK, RECOM) = RPT(RI(I, O), RISK(CL, I), RECOM(MP, TR, RI)) \quad (1)$$

где

RI – функция идентификации остаточной информации, указывающая на обнаруженную в ходе мониторинга остаточную информацию;

RISK – функция риска, позволяющая оценить риск утечки остаточной информации по потенциальным каналам;

RECOM – функция рекомендаций, описывающая мероприятии, которые необходимо провести для снижения рисков от выявленной остаточной информации;

I – остаточная информация;

O – области компьютера;

CL – множество каналов утечки информации;

MP – множество мероприятий по снижению рисков;

TR – множество требований.

Остаточная информация *I* представляет собой множество данных, обнаруженных в ходе поиска по заданным параметрам и ключевым словам в указанных областях компьютера. Каждый элемент $I_x \in I$ описывается следующим вектором $I_x=(Type, lev)$, где

Type – тип остаточной информации с множеством базовых значений *Type* ={*DF, KR, LF, CO, TF, PW*}, здесь DF – удаленные файлы пользователей, *KR* – ключи реестра, *LF* – лог-файлы, *CO* – cookie, *TF* – временные файлы, *PW* – пароли к веб-сайтам;

lev – уровень важности с множеством базовых значений *lev*={0, 1, 2}, где 0 – низкий уровень важности, 2 – высокий.

Множество *O* – множество областей компьютера пользователя, где будет осуществляться поиск остаточной информации, описывается множеством базовых значений *O* = {*basket, conductor, cache, browser_history, register*}.

Функция идентификации остаточной информации на компьютере$RI(I,O)$ формируется по результатам выполнения первого этапа аудита и позволяет идентифицировать обнаруженную по заданным параметрам поиска в указанных областях остаточную информацию и задать связь между обнаруженной информацией и областью компьютера. Связь задается посредством матрицы бинарных отношений где 1 – указывает, что данная информация обнаружена в данной области памяти, а 0 – что ее нет. Формально представляется в следующем виде:

$$RI(I_x, O_y) = \begin{cases} 1, \text{если } x \text{ информация } I \text{ присутсвует в } y \text{ области } O, \\ 0, \text{если } x \text{ информация } I \text{ не присутсвует в } y \text{ области } O. \end{cases} \quad (2)$$

Следующим этапом при проведении мониторинга и аудита остаточной информации является ранжирование выявленной остаточной информации по степени важности и оценка рисков от потенциальной утечки. С учетом подходов, изложенных в [4], в данной работе использовался количественно-качественный подход к оценке рисков. В соответствии с данным подходом для оценки общего риска от утечки обнаруженной остаточной информации используется следующая формула:

$$RISK(CL, I) = \frac{1}{k}\sum_{I=1}^{k} R_I, \quad (3)$$

где k – количество единиц обнаруженной остаточной информации. Для каждой единицы обнаруженной остаточной информации риск определяется по формуле $R_I = P_I L_I CLP_I$, где P_I – вероятность утечки I остаточной информации, задаваемая уровнем, который определяется экспертно и описывается множеством базовых значений $P_I \in \{0,0.5,1\} = \{\text{низкий, средний, высокий}\}$; L_I – величина ущерба при утечки i-й остаточной информации, определяется критичностью (уровнем важности) остаточной информации, измеряется в уровнях. CLP_I – наличие канала утечки информации, принимает значение 0 или 1, 0 – канал утечки отсутствует, 1 – канал утечки имеется.

Таким образом, графа оценки риска определяется следующим образом:

$$R_I = \begin{cases} 4, \text{риск высокий}; \\ 2, \text{риск средний}; \\ < 2, \text{риск низкий}. \end{cases}$$

В идеале риск от утечки остаточной информации на компьютере пользователя должен $RISK(CL, I) \to 0$, т.е. либо остаточная информация должна отсутствовать, либо потенциальные каналы утечки должны быть полностью перекрыты механизмами защиты.

Целью этапа формирования отчета по результатам аудита и выдачи рекомендаций является анализ результатов аудита и выработка рекомендаций, направленных на устранение выявленных недостатков и снижение рисков от умышленных и неумышленных утечек остаточной информации на компьютерах ИС организации. Формально данный этап описывается функцией $RECOM = RECOM(MP, TR, RI)$. При выработке рекомендаций учитываются возможные механизмы, которые могут использоваться для воздействия на остаточную информацию, требования организации к безопасности ИС в случае наличия в ней остаточной информации, а также вид и критичность выявленной в ходе мониторинга и аудита остаточной информации.

На последнем этапе формируется отчет, содержащий информацию о виде, критичности остаточной информации, ее местонахождении на компьютере ИС, уровне риска в случае ее утечке, а также рекомендациях, направленных на его снижение.

Программный комплекс мониторинга и аудита остаточной информации на компьютере пользователя в ИС организации

Для автоматизации процедуры мониторинга и аудита остаточной информации на компьютере пользователя в ИС организации был разработан программный комплекс, который имеет модульную архитектуру и пользовательский интерфейс. Каждый модуль реализует близкие по своему назначению функции (рис.1).

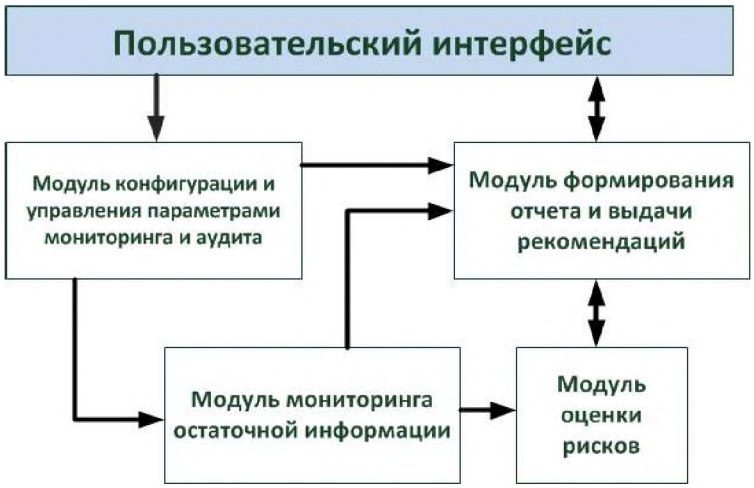

Рис. 1. Архитектура программного комплекса мониторинга и аудита остаточной информации на компьютере пользователя

Пользовательский интерфейс имеет графический вид и предназначен для организации взаимодействия пользователя с программой аудита и мониторинга, ввода входных данных и вывода результата (рис. 2).

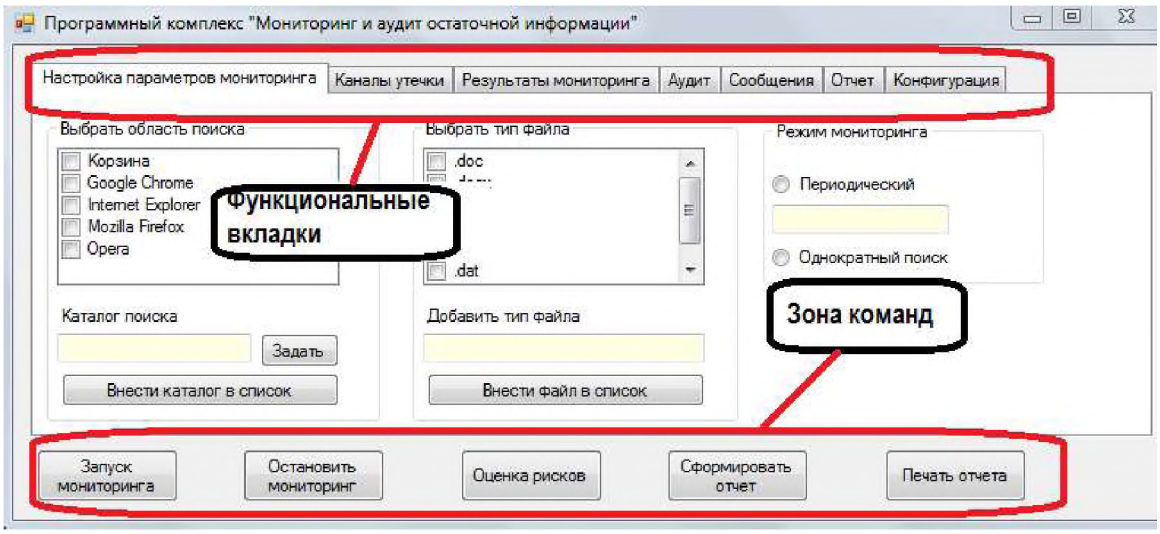

Рис. 2. Пользовательский интерфейс программного комплекса мониторинга и аудита остаточной информации (экранная копия)

Заключение

Разработанный программный комплекс может применяться в качестве вспомогательного инструментального средства поддержки принятия решений при проведении внутреннего аудита информационной безопасности в корпоративных ИС предприятий, в части мониторинга остаточной информации на компьютерах пользователей ИС и для оценки величины потенциального риска от ее утечки.

СПИСОК ЛИТЕРАТУРЫ:

1. Малюк А.А., Горбатов В.С., Королев В.И. и др. Введение в информационную безопасность: учебное пособие – М.: Горячая линия–Телеком, 2011, 288 с.
2. Щеглов А., Щеглов К. Компьютерная безопасность. Часть 10. Дополнительная защита информационных ресурсов методами криптографической защиты и гарантированного удаления остаточной информации// Daily.Sec.Ru. URL: http://daily.sec.ru/2005/05/17/print-ASHeglov-KSHeglov-Komputernaya-bezopasnost-CHast-10-Dopolnitelnaya-zashita-informatsionnih-resursov-metodami-kriptograficheskoy-zashiti-i-garantirovannogo-udaleniya-ostatochnoy-informatsii.html (дата обращения 24.01.2014).
3. Аверченков В.И. Аудит информационной безопасности: учебное пособие для вузов. – М.: Горячая линия – Телеком, 2011, 300 с.
4. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – М.: Гостехкомиссия РФ, 1992.
5. Машкина И.В. Сенцова А.Ю. Методология экспертного аудита в системе облачных вычислений//Безопасность информационных технологий. 2013. №4. С. 63-70.

REFERENCES:

1. Malyuk A.A., Gorbatov V.S., Korolev V. I. i dr. Vvedeniye v informatsionnuyu bezopasnost': uchebnoye posobiye – M.: Goryachaya liniya–Telekom, 2011, 288 s.
2. Shcheglov A., Shcheglov K. Komp'yuternaya bezopasnost'. Chast' 10. Dopolnitel'naya zashchita informatsionnykh resursov metodami kriptograficheskoy zashchity i garantirovannogo udaleniya ostatochnoy informatsii// Daily.Sec.Ru. URL: http://daily.sec.ru/2005/05/17/print-ASHeglov-KSHeglov-Komputernaya-bezopasnost-CHast-10-Dopolnitelnaya-zashita-informatsionnih-resursov-metodami-kriptograficheskoy-zashiti-i-garantirovannogo-udaleniya-ostatochnoy-informatsii.html (data obrashcheniya 24.01.2014).
3. Averchenkov V.I. Audit informatsionnoy bezopasnosti: uchebnoye posobiye dlya vuzov. M.: Goryachaya liniya – Telekom, 2011, 300 s.
4. Rukovodyashchiy dokument. Avtomatizirovannyye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii. – M.: Gostekhkomissiya RF, 1992.
5. Mashkina I.V. Sentsova A.YU. Metodologiya ekspertnogo audita v sisteme oblachnykh vychisleniy//Bezopasnost' informatsionnykh tekhnologiy. 2013. №4. S.63-70.