УДК 004.056
DOI: 10.15827/2311-6749.19.185

ПРОГРАММНЫЙ КОМПЛЕКС РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.Б. Дроботун, к.т.н., докторант; Д.В. Козлов, курсовой офицер;
А.С. Марковский, курсант
(Военная академия воздушно-космической обороны им. Маршала Советского Союза Г.К. Жукова, ул. Жигарева, 50, г. Тверь, 170022, Россия, vavko@mil.ru)

Аннотация. В работе приводится вариант построения программного комплекса расследования случаев нарушений правил и политик информационной безопасности в информационно-вычислительных системах на базе операционной системы семейства Windows. Определены требования к составу и возможностям этого программного комплекса. Приведены описания общей структуры программного комплекса, а также его отдельных составных элементов.

Ключевые слова: *информационная безопасность, инцидент информационной безопасности, политика информационной безопасности, реагирование на инцидент информационной безопасности.*

Расследование инцидентов *информационной безопасности* (ИБ) является неотъемлемой и одной из важнейших задач обеспечения ИБ организации или предприятия, цель которой – не только изучение и исследование всех обстоятельств и деталей свершившегося факта для установления круга лиц, причастных к инциденту ИБ, но и выработка рекомендаций по недопущению такого рода событий в дальнейшем. Зачастую именно по качеству и эффективности реагирования, а также по расследованию произошедших в компании инцидентах ИБ руководство, потенциальные партнеры и клиенты оценивают состояние безопасности и организацию управляющих или производственных процессов в компании.

Само понятие «инцидент ИБ» (в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М.: Стандартинформ, 2009) можно определить как появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ. В свою очередь, под событием ИБ понимается идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ, отказ защитных мер или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

К инцидентам ИБ (по ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных систем. М.: Стандартинформ, 2007) можно отнести следующие:

– утрата услуг, оборудования или устройства;
– системные сбои или перегрузки;
– ошибки пользователей;
– несоблюдение политик или рекомендаций;
– нарушение физических мер защиты;
– неконтролируемые изменения системы;
– сбои программного обеспечения и отказы технических средств;
– нарушение правил доступа.

Инциденты ИБ могут быть преднамеренными или случайными (например, являться следствием какой-либо ошибки или природного явления) и вызваны как техническими, так и нетехническими средствами. Последствиями инцидентов ИБ могут быть несанкционированное раскрытие или изменение информации, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам организации или их хищение.

Расследование инцидентов ИБ является частью процесса реагирования на них и предполагает решение следующих задач:

– подтверждение или опровержение факта инцидента ИБ;
– детальное изучение всех обстоятельств произошедшего инцидента ИБ;
– сбор доказательств и формирование доказательной базы;
– обеспечение неизменности, целостности и сохранности доказательств;
– определение причастных к инциденту ИБ лиц;
– предоставление детализированного отчета о произошедшем инциденте ИБ;
– хранение и защита материалов расследования.

Наибольшую сложность при проведении расследований инцидентов ИБ представляют сбор доказательств и формирование доказательной базы, а также обеспечение неизменности, целостности и доказательств. Это связано с тем, что, как правило, в случаях расследования инцидентов ИБ большая часть доказательств представляет собой информацию, хранящуюся в информационной системе на накопителях информации или в оперативной памяти в виде каких-либо данных, файлов, записей в БД или служебных областях операционной системы. Всю эту информацию достаточно легко случайно либо умышленно уничтожить. Часто ее довольно легко подделать, поскольку поддельная информация, хранящаяся в цифровом виде, ничем не отличается от подлинной. При этом фальсификацию таких доказательств приходится выявлять либо по смысловому содержанию информации, либо по оставленным в иных местах следам, тоже информационным. Цифровые доказательства нельзя воспринимать непосредственно органами чувств человека, а только посредством сложных аппаратно-программных средств. Не всегда просто обеспечить неизменность следов при их хранении. И не только обеспечить, но и доказать эту неизменность [1].

Все это требует определенного набора средств (прежде всего программных) для извлечения требуемой информации из исследуемой компьютерной системы и представления этой информации в виде, пригодном для анализа.

Определение требований к программному комплексу расследования инцидентов ИБ

Исходя из возможных мест нахождения информации, представляющей интерес для расследования инцидентов ИБ, и возможных способов действий ее нарушителей, программный комплекс должен включать в себя следующие элементы (рис. 1):

– средство анализа технических компонентов системы;

– средство поразрядного копирования накопителей информации;

– средство анализа файловой системы на предмет возможного восстановления удаленной информации;

– средство анализа реестра Windows;

– средство анализа посещенных интернет-страниц;

– средство поиска зашифрованных данных;

– средство формирования отчетов;

– средство анализа стойкости паролей (по словарю);

– средство анализа системы на наличие индикаторов вредоносной активности;

– средство поиска информации по шаблонам (в том числе и с использованием регулярных выражений);

– средство анализа сетевого трафика.

Рис. 1. Общая структура программного комплекса расследования инцидентов ИБ

Для обеспечения функционирования некоторых средств программного комплекса (в частности средства анализа стойкости паролей Windows и средства анализа системы на наличие индикаторов вредоносной активности) в его состав дополнительно необходимо включить БД (словарь) паролей, индикаторов вредоносной активности, контрольных сумм (хэшей) общесистемных файлов.

Средство анализа технических компонентов системы должно иметь возможность получать максимально полную информацию о технических компонентах системы и представлять эту информацию в удобном для восприятия виде.

Введение в состав программного комплекса средства поразрядного копирования накопителей информации вызвано необходимостью обеспечения сохранности, целостности и неизменности данных, хранящихся на устройствах внешней памяти исследуемой компьютерной системы, в связи с чем целесообразно проводить анализ и исследование этих данных в виде копии, снятой с «оригинального» устройства внешней памяти [1]. Для обеспечения полной идентичности снятой копии оригиналу данное средство должно иметь возможность копирования информации на самом низком (системном) уровне, а не на уровне файловой системы. Данное средство должно иметь следующие возможности:

– поразрядное (посекторное) копирование информации с источника (исследуемого накопителя) на дублирующий накопитель всей информации (включая служебные данные, загрузочные сектора, скрытые разделы, области, помеченные как неисправные, и т.п.);

– возможность снятия копий как с физических разделов накопителей, так и с логических;

– логирование процесса снятия копий;

– фиксация всей служебной информации из накопителя (серийный номер, объем, производитель и т. п.).

Средство анализа файловой системы на предмет возможного восстановления удаленной информации должно обладать следующими возможностями:

– анализ всех файловых систем, используемых в операционных системах семейства Windows;

– поиск и восстановление удаленных (штатными средствами операционной системы) файлов;

– поиск информации в скрытых и системных областях накопителя информации;

– поиск информации в альтернативных потоках (при использовании файловой системы NTFS);

– взаимодействие со средством анализа системы на наличие индикаторов вредоносной активности.

Средство анализа реестра Windows должно обладать следующими возможностями:

– анализ записей в областях автозагрузки (поиск программ, запускающихся одновременно с загрузкой операционной системы);

– анализ и извлечение информации о подключенных внешних накопителях информации (в том числе и о предоставлении данных об истории таких подключений);

– извлечение информации о паролях и учетных записях (для обеспечения функционирования средства анализа стойкости паролей);

– извлечение и предоставление информации о настройках политик безопасности.

Средство анализа посещенных интернет-страниц должно обладать возможностями:

– извлечение и предоставление истории посещенных сайтов всех браузеров, установленных в системе;

– извлечение и предоставление информации о произведенных загрузках файлов;

– извлечение информации о паролях и учетных записях.

Средство поиска зашифрованных данных на исследуемой компьютерной системе должно иметь следующие возможности:

– поиск областей на накопителе информации, предположительно, содержащих зашифрованную информацию (путем анализа значения энтропии этих областей);

– поиск и определение вида криптоконтейнеров различных программ шифрования (TrueCrypt, BestCrypt, PGP и т.п.);

– анализ файла гибернации на предмет присутствия в нем ключевой информации от криптоконтейнеров и ее извлечение;

– анализ файла дампа оперативной памяти (при его наличии) на предмет присутствия в нем ключевой информации от криптоконтейнеров и ее извлечение;

– анализ файлов изображений на предмет наличия внедренной в них информации с помощью методов стеганографии.

Средство анализа стойкости паролей должно обладать следующими возможностями:

– извлечение информации об учетных записях и хэшей паролей из реестра Windows;

– анализ стойкости паролей от учетных записей путем подбора пароля по словарю, определенному лицом, производящим расследование;

– анализ файла дампа оперативной памяти (при его наличии) на предмет присутствия в нем информации о зарегистрированных пользователях системы и паролей, а также извлечение этой информации и паролей.

Средство анализа системы на наличие индикаторов вредоносной активности должно позволять:

– поиск атомарных индикаторов (IP-адреса, URL, e-mail-адреса) вредоносной активности (в том числе и в файле дампа памяти);

– поиск вычисляемых индикаторов (контрольные суммы файлов вредоносных и потенциально вредоносных программ, ключи реестра Windows, сигнатуры участков памяти и файлов, различные объекты, создаваемые операционной системой (каталоги, файлы, мьютексы, службы, процессы и т.п.)) вредоносной активности (в том числе и в файле дампа памяти);

– возможность ручного указания индикатора вредоносной активности для поиска.

Средство поиска информации по шаблонам поиска должно обладать следующими возможностями:

– поиск информации по различным шаблонам (текстовая строка, последовательность байт в явном виде и в виде регулярных выражений, сигнатуры в виде хэш-сумм) на уровне файловой системы;

– поиск информации по различным шаблонам на уровне секторов и разделов накопителей информации;

– поиск информации по различным шаблонам в архивированных файлах;

– поиск информации по различным шаблонам в системных областях операционной системы;

– взаимодействие со средством анализа системы на наличие индикаторов вредоносной активности.

БД (словарь) паролей должна обеспечивать хранение массива наиболее часто употребляемых паролей (к примеру, один из вариантов такого массива представлен в [2]), а также возможность пополнения этой БД пользователем системы.

БД индикаторов вредоносной активности должна обеспечивать хранение всех видов индикаторов вредоносной активности (как атомарных, так и вычисляемых), а также возможность добавления индикаторов пользователем и обновление (пополнение) содержимого этой базы актуальной информацией.

БД контрольных сумм общесистемных файлов должна обеспечивать хранение контрольных сумм (в виде MD5-хэшей) файлов, в которых поиск информации должен быть исключен.

Средство анализа сетевого трафика должно позволять проводить анализ сетевого трафика (если требуется оперативный анализ).

Структура программного комплекса расследования инцидентов информационной безопасности

Общая структура программного комплекса

Общая структурная схема программного комплекса (со всеми взаимосвязями между элементами) представлена на рисунке 2.

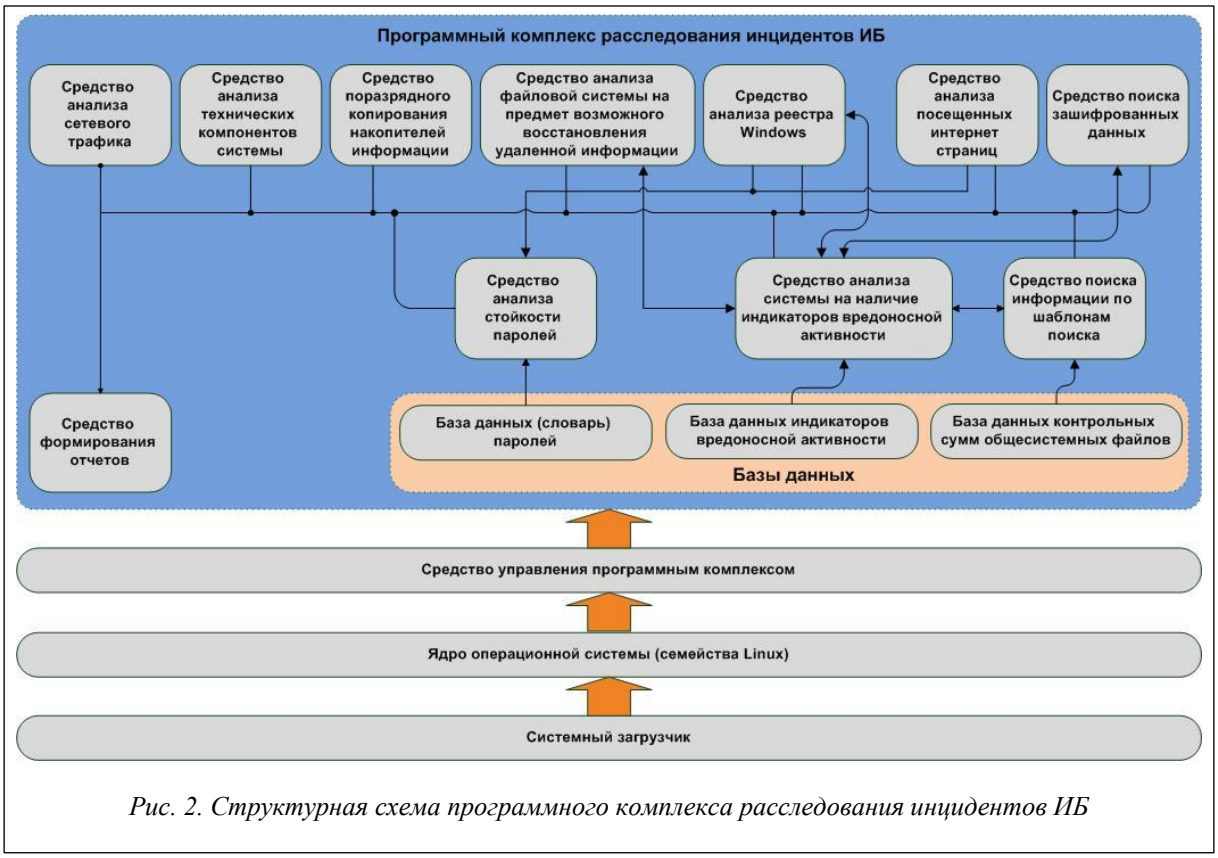

Рис. 2. Структурная схема программного комплекса расследования инцидентов ИБ

Помимо перечисленных средств, в состав комплекса необходимо также включить средство управления программным комплексом и системный загрузчик с ядром операционной системы.

Основная функция средства управления программным комплексом – диалоговое взаимодействие с пользователем программного комплекса, выбор для работы необходимых средств, ввод параметров (например шаблонов поиска, областей поиска информации), а также отображение и сохранение результатов работы.

Для обеспечения целостности и неизменности информации на накопителях исследуемой компьютерной системы программный комплекс должен быть выполнен в виде оптического диска (или образа такого диска) с возможностью загрузки исследуемой компьютерной системы непосредственно с этого диска, а не с собственного системного накопителя (то есть программный комплекс должен быть выполнен в виде так называемого Live-CD диска). Данный диск может быть реализован на базе какого-либо дистрибутива Linux (поскольку использование для этих целей компонентов операционной системы Windows запрещено лицензией) и системного загрузчика Grub.

Средство анализа технических компонентов системы

Структурная схема анализа технических компонентов системы приведена на рисунке 3.

Рис. 3. Структурная схема средства анализа технических компонентов системы

Блок определения типа процессора определяет тип процессора, идентификатор, производителя, тактовую частоту, количество ядер, характеристики кэш-памяти и наличие дополнительных возможностей (аппаратный DEP и аппаратная виртуализация). Реализация данного блока возможна на базе команды cpuid, предусмотренной в процессорах архитектуры X86 [3]. После получения всей информации о процессоре исследуемой системы блок определения типа процессора передает ее на вход блока формирования отчета.

Основная задача блока определения характеристик оперативной памяти – предоставление информации о типе, общем объеме оперативной памяти, количестве модулей, их типе, объеме, частоте шины и временных характеристик. Вся полученная информация также выдается на вход блока формирования отчета.

Блок определения характеристик внешних накопителей информации служит для определения количества внешних накопителей информации, подключенных к системе на момент проверки, их типа, объема, типа файловой системы, идентификатора (серийного номера) и производителя внешнего накопителя информации.

Блок определения характеристик материнской платы предназначен для получения информации о производителе и чипсете материнской платы, характеристик «южного» и «северного» мостов, версии BIOS (UEFI), а также серийного номера. Вся полученная информация передается в блок формирования отчета.

Блок определения типов и характеристик внешних интерфейсов служит для предоставления информации о типах (COM и LPT-порты, USB-порты, сетевые интерфейсы, беспроводные интерфейсы, слоты для карт памяти) и их количестве. Результаты работы данного блока также передаются в блок формирования отчета.

Блок определения характеристик видеоадаптера необходим для получения информации о количестве и типах видеоадаптеров, установленных в исследуемой системе, а также информации о производителе, серийном номере, объеме памяти и поддерживаемых видеорежимах. Вся информация, полученная в результате работы этого блока, передается в блок формирования отчета.

Средство поразрядного копирования накопителей информации

Структурная схема средства поразрядного копирования накопителей информации изображена на рисунке 4.

Рис. 4. Структурная схема средства поразрядного копирования накопителей информации

Блок определения характеристик накопителя «оригинала» служит для определения объема накопителя, используемой в нем файловой системы (NTFS или FAT-32), размеров секторов и кластеров, а также серийного номера накопителя.

Буфер для хранения считанной информации необходим для промежуточного хранения данных, считанных из очередного сектора перед их записью на накопитель-«дубликат» с помощью блока посекторной записи. Размер буфера определяется исходя из размера сектора, который используется в файловой системе накопителя-«оригинала» (обычно 4096 КБ).

Весь процесс создания копии с помощью блока логирования процесса снятия копии сохраняется в лог-файл, который может служить подтверждением корректности копии и ее полного соответствия «оригиналу».

Средство анализа файловой системы на предмет возможного восстановления удаленной информации

Средство анализа файловой системы на предмет возможного восстановления удаленной информации состоит из блоков определения файловой системы, анализа служебных областей накопителя, посекторного считывания информации, восстановления информации и блока логирования процесса восстановления информации (рис. 5).

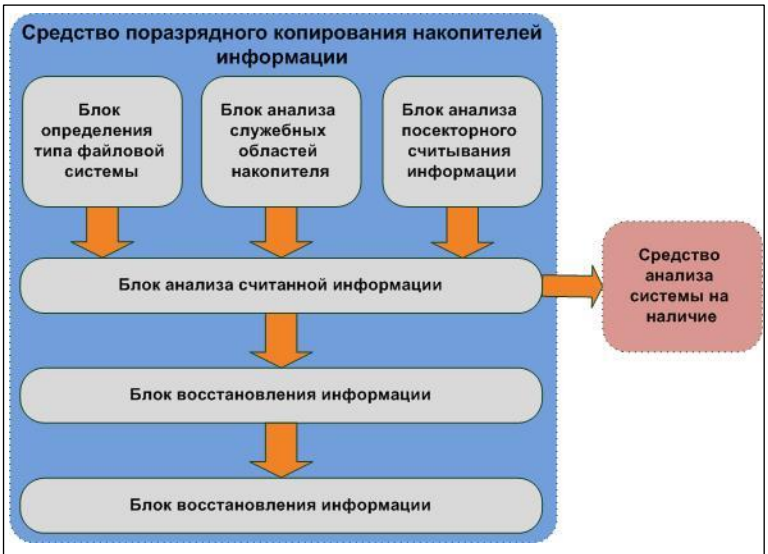

Рис. 5. Структурная схема средства анализа файловой системы на предмет возможного восстановления удаленной информации

Блок определения типа файловой системы передает информацию о типе файловой системы (NTFS или FAT-32) в блок анализа файловой системы, и в зависимости от типа файловой системы блок анализа служебных областей производит анализ либо таблицы расположения файлов (в случае FAT-32), либо файла метаданных (в случае NTFS). Далее на основе информации, полученной при анализе служебных областей, и данных, считанных из секторов накопителя, помеченных как свободные, осуществляется восстановление информации. Более подробно процессы восстановления информации изложены в [4–6]. Весь процесс восстановления информации записывается в лог-файл с помощью блока логирования процесса восстановления.

Помимо этого, блок анализа считанной информации предоставляет информацию для средства анализа системы на наличие индикаторов вредоносной активности, для поиска этих индикаторов в областях накопителя, помеченных как свободные.

Средство анализа реестра Windows

Средство анализа реестра Windows состоит из блока анализа областей автозагрузки, блока анализа истории подключения внешних устройств и блока анализа информации об учетных записях и паролях (рис. 6).

Блок поиска параметров реестра осуществляет поиск информации по заданным параметрам для средства анализа системы на наличие индикаторов вредоносной активности.

Блок анализа областей автозагрузки осуществляет поиск программ, которые запускаются вместе со стартом операционной системы. В большинстве случаев это следующие ветки реестра:

– HKLM\Software\Microsoft\Windows\CurrentVersion\Run;
– HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run;
– HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce;
– HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce;

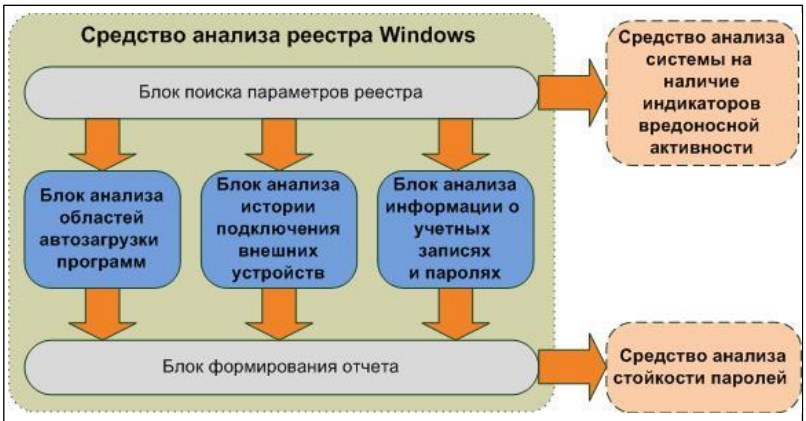

Рис. 6. Структурная схема средства анализа реестра Windows

Блок анализа истории подключения внешних устройств осуществляет извлечение информации обо всех USB-устройствах, когда-либо подключаемых к исследуемой системе, а также о времени и дате подключения и отключения этого устройства.

Блок анализа информации об учетных записях и паролях извлекает имена учетных записей и хэши паролей из ветки HKLM\SAM\SAM\Domains\Account\Users\[RID]\V (где RID – идентификатор пользователя). Данная ветка реестра содержится в файле SAM, который, как правило, находится в каталоге %WinDir%/System32/config. В версиях Windows до Vista пароли к учетным записям хранятся в виде двух контрольных сумм – так называемых LM- и NT-хэшей; в версиях от Vista и выше в файле SAM сохраняется только контрольная сумма в виде NT-хэша [7, 8]. Информация об учетных записях и значения хэш-сумм паролей передаются в блок анализа стойкости паролей.

Средство анализа посещенных интернет-страниц

В состав данного средства входят блок определения браузеров, установленных в системе, блок анализа истории посещенных страниц, блок анализа истории загруженных файлов и блок анализа информации об учетных записях и паролях интернет-сервисов (рис. 7).

Рис. 7. Структурная схема средства анализа посещенных интернет-страниц

Блок определения типов браузеров определяет количество и типы браузеров (помимо InternetExplorer), установленных в системе. Необходимость введения в состав средства анализа посещенных интернет-страниц вызвана различиями в хранении и расположении файлов, содержащих историю посещенных интернет-страниц и загруженных файлов, кэша браузера (временных файлов Интернета, в которых хранятся копии просмотренных веб-страниц), т.н. cookie-файлов, в которых содержится информация о настройках для определенных веб-сайтов, а также могут храниться учетные записи и пароли от различных интернет-сервисов.

В зависимости от типа установленного браузера блок истории посещенных интернет-страниц производит анализ нужного файла (см. таблицу), в котором хранится эта история, и предоставляет полученную информацию в блок формирования отчета.

Блок истории загруженных файлов анализирует папку загрузок и также выдает полученные после анализа данные в блок формирования отчета.

Файлы хранения истории для разных браузеров

Браузер	Файл истории	Местонахождение файла
Opera	global_history.dat	C:\Users\имя пользователя\AppData\ Roaming\Opera\Opera\
Chrome	history	C:\Users\имя пользователя\AppData\ Local\Google\Chrome\UserData\Default\
Mozilla	places.sqlite	C:\Users\имя пользователя\AppData\ Roaming\Mzilla\FireFox\Profiles\
InternetExplorer	index.dat	C:\Users\имя пользователя\AppData\ Local\Microsoft\Windows\History\

Блок анализа информации об учетных записях и паролях производит поиск учетных записей и паролей от различных интернет-сервисов в файлах настроек браузера и в cookie-файлах и выдает полученную информацию на блок анализа стойкости паролей для их дальнейшего анализа, а также на блок формирования отчета.

Средство поиска зашифрованных данных

Структурная схема средства поиска зашифрованных данных приведена на рисунке 8.

В основу работы данного средства положено сравнение энтропии «подозрительного» участка с заранее определенным значением, и, если значение энтропии анализируемого участка превышает этот установленный порог, принимается решение о том, что в этой области (секторе или файле) находится зашифрованная информация [9].

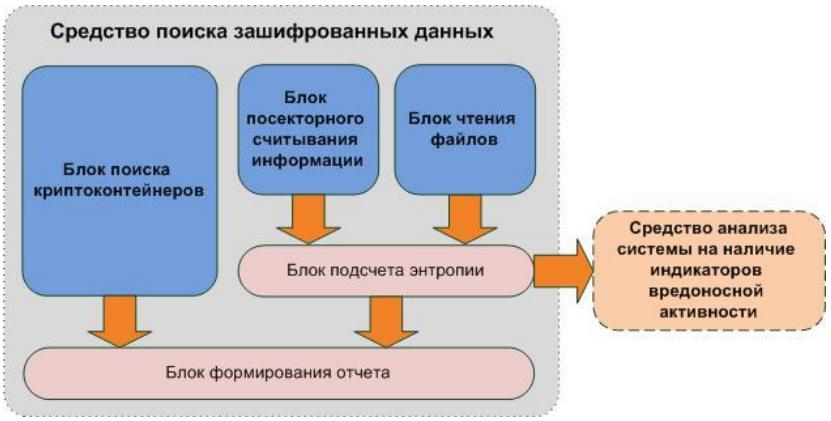

Рис. 8. Структурная схема средства поиска зашифрованных данных

Помимо поиска зашифрованных областей, на основе анализа значения энтропии с помощью блока поиска криптоконтейнеров возможен поиск информации, зашифрованной посредством некоторых распространенных программ шифрования, таких как TrueCrypt, BestCrypt, PGP и т.п. Это производится на основе известной информации о форматах криптоконтейнеров и характерных сигнатур.

Информация о возможном наличии зашифрованных данных и об участке, где находятся эти данные, передается на средство анализа системы на наличие индикаторов вредоносной активности (в случае поиска зашифрованных компонентов вредоносных программ), а также на блок формирования отчета для представления полученной информации в наглядном виде.

Средство анализа стойкости паролей

Основная функция средства анализа стойкости паролей – проверка паролей к учетным записям Windows, а также различных интернет-сервисов на устойчивость к взлому по словарю.

Структурная схема этого средства представлена на рисунке 9.

При анализе стойкости паролей к учетным записям Windows блок вычисления хэш-суммы пароля производит вычисление контрольной суммы для каждого пароля, содержащегося в словаре паролей; далее все вычисленные хэш-суммы поочередно сравниваются с хэш-суммами паролей к учетным записям Windows, извлеченных из реестра средством анализа реестра Windows. В случае совпадения сравниваемых хэш-сумм принимается решение о подборе пароля к учетной записи Windows.

При анализе стойкости паролей к учетным записям интернет-сервисов вычисление хэш-сумм паролей из словаря не производится (поскольку пароли и информация об учетных записях в cookie-файлах хранится в открытом виде). Блок сравнения поочередно сравнивает пароли из словаря с паролями, полученными с помощью средства анализа посещенных интернет-страниц. В случае совпадения также принимается решение о подборе пароля.

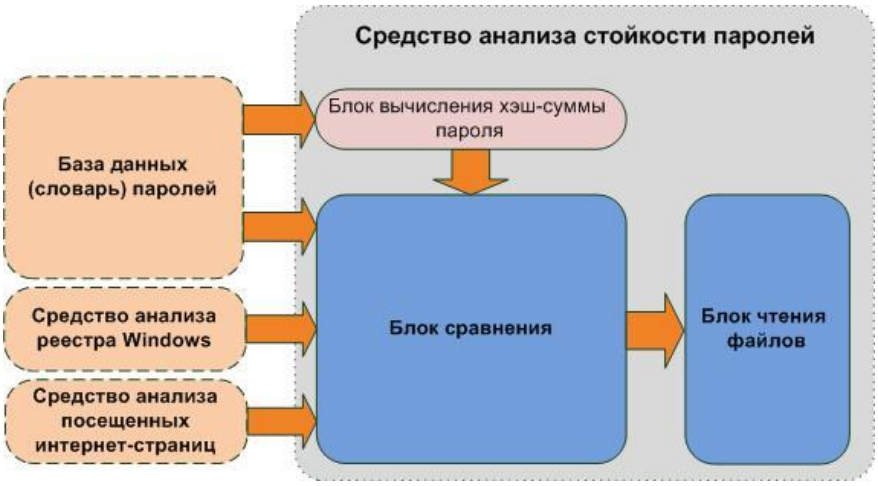

Рис. 9. Структурная схема средства анализа стойкости паролей

Средство анализа системы на наличие индикаторов вредоносной активности

Средство анализа системы на наличие индикаторов вредоносной активности служит для обнаружения воздействия на систему с помощью вредоносных программ. Основной принцип работы этого средства заключается в поиске на носителях информации исследуемой системы (жестких магнитных дисках, SSD-накопителях, съемных флэш-накопителях информации) характерных следов воздействия вредоносных программ в виде определенных файлов и записей на носителе информации в виде записей в реестре Windows, конфигурационных и других системных файлов, которые выступают в роли индикаторов вредоносной активности [10].

В состав данного средства входят блок расчета вычисляемых индикаторов, блок сравнения информации и блок формирования отчетов (рис. 10). Поиск индикаторов вредоносной активности производится во всех возможных областях накопителей информации системы с помощью средств анализа файловой системы на предмет возможного восстановления удаленной информации, поиска зашифрованных данных, поиска информации по шаблонам поиска и средства анализа реестра Windows. При поиске и обнаружении атомарных индикаторов блок расчета вычисляемых индикаторов никаких расчетов не производит.

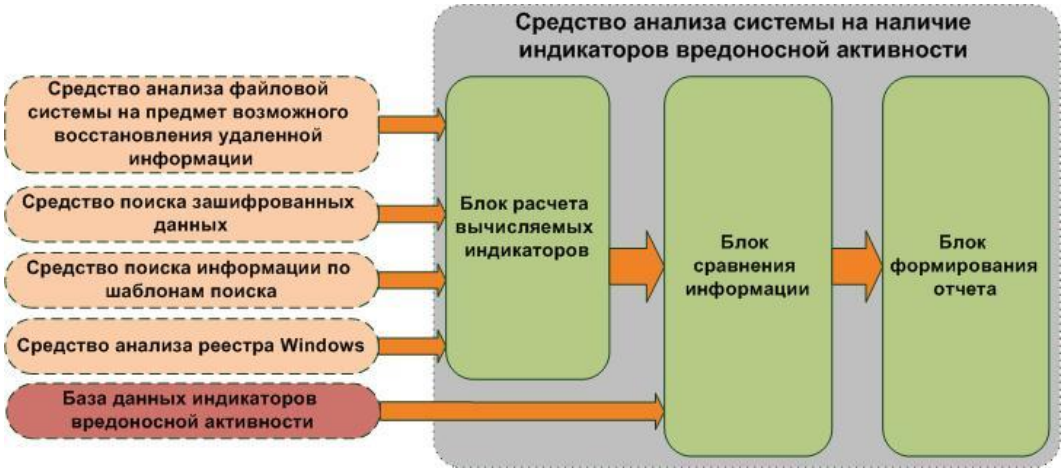

Рис. 10. Структурная схема средства анализа системы на наличие индикаторов вредоносной активности

При поиске вычисляемых индикаторов с помощью данного блока рассчитываются контрольные суммы нужных областей и участков носителей информации и памяти.

Средство поиска информации по шаблонам поиска

Данное средство включает в себя блоки чтения файлов (начинает работу при поиске на уровне файловой системы), посекторного чтения (начинает работу при поиске на системном уровне), сравнения информации и блок формирования отчета (рис. 11) и служит для поиска на накопителях информации текстовых строк или последовательности байтов в соответствии с заданным шаблоном поиска. Для снижения времени поиска предусмотрена возможность исключения из поиска общесистемных файлов (в большинстве случаев поиск в этих файлах нецелесообразен). Для этого в состав программного комплекса введена БД контрольных сумм общесистемных файлов. Перед поиском в файле вычисляется контрольная сумма этого файла; в случае совпадения вычисленной суммы с контрольной суммой из БД поиск в этом файле не производится и осуществляется переход к следующему файлу.

Рис. 11. Структурная схема средства поиска информации по шаблонам поиска

Данное средство также используется при работе средства анализа системы на наличие индикаторов вредоносной активности.

Средство анализа сетевого трафика

Данное средство анализа необходимо, если в сети наблюдался подозрительный трафик. Анализаторы протоколов, встроенные в программу, организуют процесс разделения трафика на пакеты для облегчения анализа и получения информации, позволяющей отыскать проблемы в сетевых приложениях или в неверно сконфигурированных рабочих станциях. В средство анализа сетевого трафика входят фильтры, позволяющие выделить специальную информацию при больших сетевых потоках; фильтры захвата, выбирающие из всей захваченной информации ту, которая необходима; и триггеры, позволяющие системе выполнять определенные действия с данными, содержащимися в пакетах.

Вспомогательные БД

Для обеспечения функционирования средств анализа стойкости паролей, анализа системы на наличие индикаторов вредоносной активности и средства поиска информации по шаблонам в состав программного комплекса включены вспомогательные БД.

БД (словарь) паролей используется при анализе паролей от учетных записей Windows и от учетных записей различных интернет-сервисов и представляет собой файл с набором наиболее часто употребляемых паролей в текстовом виде.

БД индикаторов вредоносной активности используется при поиске признаков воздействия на систему вредоносных программ и представляет собой файл с набором записей, в каждой из которых содержатся индикаторы, характерные для одного вида вредоносных программ.

БД контрольных сумм общесистемных файлов может использоваться при поиске данных по шаблонам поиска в случае необходимости сокращения времени поиска и представляет собой файл, содержащий контрольные суммы системных файлов Windows в виде MD5-хэшей.

Таким образом, использование предлагаемого программного комплекса расследования инцидентов ИБ позволит проводить расследования случаев нарушения правил и политик ИБ при использовании информационно-вычислительных систем в различных организациях. При этом в ходе расследования возможны сбор и исследование различных данных, свидетельствующих об обстоятельствах произошедшего инцидента, сбор доказательств, а также обеспечение их целостности, неизменности и сохранности.

Комплексирование различных средств сбора и анализа данных об инциденте в виде программного комплекса, представляющего собой загрузочный диск с собственным загрузчиком и ядром операционной

системы, и включение в его состав средства управления позволят сделать более удобной работу со средствами сбора доказательств, а также сократить время на расследование инцидента и реагирование на него.

Литература

1. Федотов Н.Н. Форензика – компьютерная криминалистика. М.: Юридический мир, 2007. 432 с.
2. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1996. 336 с.
3. Intel Corporation. Intel 64 and IA-32 Architectures Software Developer‘s Manual. 2014, vol. 1–3.
4. Кэрриэ Б. Криминалистический анализ файловых систем. СПб: Питер, 2007. 480 с.
5. Касперски К. Восстановление данных: практич. руководство; [пер. с англ.]. СПб: БХВ-Петербург, 2006. 352 с.
6. Дроботун Е.Б. О сложности безвозвратного удаления данных на SSD-накопителях // Перспективы развития информационных технологий: докл. 3-й Всерос. науч.-практич. конф. Новосибирск, 2011. С. 5–8.
7. Хранение и шифрование паролей MicrosoftWindows. URL: habrahabr.ru/post/114150 (дата обращения: 13.11.2015).
8. Получение в открытом виде паролей пользователей, авторизованных в Windows. URL: winitpro.ru/index.php/2013/12/24/poluchenie-v-otkrytom-vide-parolej-polzovatelej-avtorizovannyx-v-windows/ (дата обращения: 13.11.2015).
9. Матвеева В. Криптография и вредоносные программы // InformationSecurity – информационная безопасность. 2015. № 1. С. 35–38.
10. Лукацкий А. Эффективное распределение информации об угрозах // BIS Journal – информационная безопасность банков. 2015. № 4 (19). С. 28–33.