Сорокин Дмитрий Анатольевич
347922, г. Таганрог, пер. Украинский, д. 21, кв. 30.
E-mail: jotun@inbox.ru.
Тел.: 88634393820.
Научный сотрудник.

Дордопуло Алексей Игоревич
Учреждение Российской академии наук «Южный научный центр РАН».
E-mail:scorpio@mvs.tsure.ru.
347900, г. Таганрог, 10-й переулок, 114/1, кв. 6.
Тел.: 88634368651.
К.т.н.; с.н.с. отдела ИТ и ПУ.

Levin Ilya Israilevich
Kalyaev Scientific Research Institute of Multiprocessor Computer Systems at Southern Federal University.
E-mail: levin@mvs.tsure.ru.
224/1, Lenin Street, Ap. 65, Taganrog, 347922, Russia.
Phone: +78634623226.
Deputy Director of Science; Dr. of Eng. Sc.

Sorokin Dmitry Anatolievich
E-mail: jotun@inbox.ru.
21, Ukrainskiy Lane, Ap. 30, Taganrog, 347922, Russia.
Phone: +78634393820.
Scientific Associate.

Dordopulo Alexey Igorevich
Southern Scientific Centre of the Russian Academy of Sciences.
E-mail: scorpio@mvs.tsure.ru.
114/1, 10th Lane, Ap. 6, Taganrog, 347900, Russia.
Phone: +78634368651.
Senior Staff Scientist; Cand. of Eng. Sc.

УДК 004.08

А.М. Максимов, Е.Н. Тищенко

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ НОСИТЕЛЕЙ ИНФОРМАЦИИ В ЗАЩИЩЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

В современных защищённых информационных системах общий уровень защищенности определяется уровнем защищенности самого слабого звена. Одним из таких звеньев являются накопители данных. Распространение, удешевление и увеличение объёмов накопителей вынуждает делать больше затрат для контроля за носителями данных, чтобы сохранить защищённое состояние информационной системы в целом. Дополнительные проблемы в этом направлении создаются с появлением, развитем и распространением накопителей данных, созданных по новым технологиям. К таким накопителям уже мало применимы, или же в принципе не применимы подходы, использующиеся в настоящее время, что требует поиска новых решений по защите информационных систем.

Информационная система; накопители данных; магнитные накопители данных; твердотельные накопители данных; программно-техническая экспертиза.

A.M. Maksimov, E.N. Tishchenko

ESPECIALLY THE USE OF MEDIA IN THE PROTECTED INFORMATION SYSTEMS

In a modern secure informational systems the overall level of protection depends on level of protection of the weakest element. One of this elements are data storage devices. Spreading, reduction in price and volume increasing of data storage devices increasing cost of control of data storage devices to save protected state of informational system as a whole. Additional problems in this area are created by the emergence, development and spread of data storage devices, created with new technologies. These current used approaches have little applying or not be applied to these drives. So this require to look for new solutions to protect informational systems.

Information system; data storage device; magnetic storage; solid state drives; computer forensics.

Широкое распространение, удешевление и увеличение объёмов накопителей несомненно облегчило жизнь большинства пользователей в плане хранения и переноса данных. Однако же, именно этот факт широкого распространения подобных носителей во всех сферах деятельности вызывает и беспокойство различных специалистов.

Носители данных в информационной системе (так же, впрочем, как и средства их обработки) могут быть стационарными и мобильными. Помимо этого носители информации могут быть составной частью оборудования, выполняющего также и обработку данных. Также они могут быть носителями в собственном смысле слова – устройствами, с помощью которых информацию переносят, и во время того, как ее носят, она там хранится. Потом, когда информацию перенесли, она обрабатывается с помощью какого-либо другого оборудования. И вновь сохраняется на носитель, чтобы быть перенесенной куда-то еще.

Тезис о том, что защищенность различных элементов информационных систем обеспечивается разными способами, очевиден. Он объясняется тем, что защищенность – понятие относительное, и она тем выше, чем более прямое отношение имеет именно к тем атакам, осуществление которых наиболее вероятно по отношению к данному элементу системы. В качестве обыденного аналога данного утверждения можно рассмотреть спасательный круг, который существенно повысит защищенность на воде, но совершенно не повысит ее при пожаре или морозе.

Что это означает применительно к вопросу защищенности носителей информации?

Носители информации являются частью информационной системы, и, значит, существенно большая их защищенность по отношению к остальным ресурсам системы не имеет смысла. Она никак не усилит общую защищенность данных, и переплачивать за нее нецелесообразно. Давно доказано и стало очевидным, что общий уровень защищенности определяется уровнем защищенности самого слабого звена. Нет практического смысла использовать сверхзащищенный носитель данных в незащищенной системе.

Однако даже для того, чтобы защищенность носителя информации соответствовала уровню защищенности самоой простой системы, не оборудованной ничем, кроме антивируса, этот носитель должен находиться в пределах этой системы – и нигде, кроме неё, – и должна быть каким-то образом защищена от возможного воздействия вирусов. Теоретически это достижимо с помощью организационных мер. Владелец носителя, который, в свою очередь, используется только внутри информационной системы для переноса информации между несколькими защищенными от вирусов компьютерами, может быть спокоен: данный носитель не снижает общей защищенности его системы.

Наивно полагать, что существуют абсолютно защищённые системы, используя которые можно оградиться от угроз безопасности раз и навсегда. Именно поэтому зачастую принимается ряд мер и действий, которые помогут хотя бы снизить ущерб в случае, если злоумышленник смог обойти систему безопасности каким-либо путём. Порой известен только сам факт действий злоумышленника, при этом остаётся неизвестно, что произошло, какая информация была похищена, какие воздействия были осуществлены на защищаемый объект, в каком месте было осуществлено воздействие и т.д. Возможно, ущерб удалось бы минимизировать, если б стало известно, какие данные оказались скомпрометированы, какие опасные и вредоносные воздействия были осуществлены.

Самая главная особенность мобильных носителей состоит в том, что они подвержены дополнительным угрозам, связанным с тем, что контур системы для них проницаем. Они могут не только выноситься за пределы системы, но и использоваться там. Что приводит к утечкам информации из системы и к притоку вредоносного ПО в систему. То есть помимо механизмов защиты, которые на сегодняшний день хорошо развиты (например, через организационные меры, программно-аппаратное обеспечение) для информационных систем, следует также развивать и механизмы минимизации ущерба, если меры защиты были всё же каким-либо образом пройдены.

В информационной безопасности есть интересное направление, которое зачастую обходится стороной. Это так называемая программно-техническая экспертиза, так же известная как и компьютерная экспертиза, computer forensic, digital forensic [1]. Основной интерес подобной экспертизы – отыскать различного рода доказательства, скрытые и удаленные файлы, логи действий на компьютере, историю браузера, действий, журналы событий и происшествий и всё, что может косвенно быть полезным или подтвердить какие-то факты. Тема эта довольно обширная и интересная. Многое в этой тематике совсем не так очевидно, как может показаться на первый взгляд.

Суть такой экспертизы следует из её названия. Эксперт может получить доказательства и полезные для пострадавшей стороны материалы несколькими путями.

Программный метод [2]. Исследуются различные журналы историй, логи, остающиеся в операционных системах. Кроме того, исследуются сами операционные системы на наличие файлов, помогающих установить действия злоумышленника и их масштаб, используемые для этих действий инструменты, так как большинство программ имеют тенденцию оставлять в системах после своей работы много следов. Также исследуются файловые системы, находящиеся на дисках, на наличие данных, которые могли быть удалены из системы. При этом следы таких данных остаются на диске, что зачастую позволяет установить характер этих данных, а порой и целиком восстановить такие данные. Наглядным примером может служить ситуация, когда пользователь случайно удаляет свои данные, а потом, осознав ошибочность своих действий, восстанавливает эти самые данные при помощи некоторых утилит и инструментов. Более того, в случае удачного восстановления существует вероятность получить ещё больше информации о злоумышленнике, так как некоторые файлы способны хранить гораздо больше информации, чем это кажется на первый взгляд, а именно – метаданные. В них может быть сохранена история перемещений файлов, история о тех, кто пользовался этим файлом и т.п. в зависимости от приложения, создающего и работающего с такими файлами. Всё это возможно благодаря особенностям работы жёстких дисков и различных твердотельных сменных накопителей.

Аппаратный метод [3]. С помощью него выясняются настройки устройств, серийные номера, информация об устройстве. Также производится, в случае необходимости, дублирование данных на другой носитель, с которым уже и будет работать эксперт.

Однако при проведении всех этих действий существует вероятность нежелательных изменений данных в исследуемой системе и оборудовании. Например, изменение каких-то настроек, естественная для файловой системы работа с жёсткими дисками и накопителями, изменение штампов времени и контрольных сумм. Этот момент учитывается экспертами, и для предотвращения таких негативных влияний используются различные блокираторы (как программные, так и аппаратные), производится резервное копирование исследуемых носителей. Программы, проводящие такое резервирование, как правило, ещё и создают специальный файл истории, в котором подробно документируется весь процесс копирования, обязательно документируются данные носителя, например, серийные номера и марки производителя.

С этого момента и начинают проявляться новые проблемы. Если все обозначенные методы применимы к уже хорошо изученным видам носителей данных (HDD, flash (в том числе SD, MMC и т.д.), CD/DVD), то их применение может вызвать проблемы относительно накопителей, которые только-только развиваются и входят в употребление. В частности, таким видом накопителей являются SSD-накопители.

Использование накопителей, построенных на использовании энергонезависимой памяти (так называемые NAND SSD) способно породить ряд проблем, вызванных их конструктивными особенностями.

При всех преимуществах твердотельных накопителей (отсутствие подвижных частей (как следствие шума и охлаждающих систем), скорость чтения до 740 МБ/с и записи до 730 МБ/с, низкая потребляемая мощность, высокая механическая стойкость, широкий диапазон рабочих температур, стабильность времени считывания файлов вне зависимости от их расположения или фрагментации, малые габариты и вес) есть недостатки, которые при некоторых обстоятельствах могут нанести серьезный ущерб информационной системе.

При проведении исследований (которые были представлены на Международной конференции Usenix FAST 11 в Калифорнии в конце февраля 2011 г.), имеющих важные результаты для всех банков, фирм и компаний по безопасности, ученые обнаружили, что файлы, хранимые на твердотельных накопителях, иногда невозможно удалить при помощи традиционных способов удаления информации.

Даже если такие устройства по хранению информации показывают, что файлы были удалены, большой объём информации (зачастую более 50–70 %), содержащийся в них, может по-прежнему находиться в основанных на flash-памяти накопителях. В некоторых случаях SSD неправильно показывают, что файлы были "надежно удалены", даже несмотря на то, что дубликаты файлов остались в запасных хранилищах. Подобная проблема наблюдается не только с этим развивающимся типом накопителей, но и с уже довольно широко распространенными и давно использующимися flash-носителями различных форматов.

Сложность надежного удаления с твердотельных накопителей связана с их внутренним устройством. Они используют чипы для хранения информации, а также технологию FTL (flash translation later) для управления данными. Когда информация модифицирована, FTL часто записывает новые файлы в различные области и обновляет карту для отображения изменения.

В процессе, остаточная информация из старого файла, которую авторы доклада на Usenix FAST называют цифровыми остатками, продолжает находиться в накопителе. Возникает такая проблема как раз из особенностей устройства твердотельных накопителей, а именно: запись информации на накопитель не по порядку, а в различные области памяти.

Это так называемая техника «Wear leveling», которая применяется для продления сроков службы накопителей путём заноса данных в менее используемые области (опять же, это вызвано спецификой твердотельных накопителей, которые поддерживают примерно от 10 (самые распространенные) до 100 тысяч (дорогостоящие) циклов перезаписи).

Существующие схемы работы с твердотельными накопителями могут потенциально привести к опасному расхождению между ожиданиями пользователя и реальным поведением накопителя. Обладатель SSD или flash-накопителя может применить какую-либо технику обработки носителя, ошибочно полагая, что это поможет безвозвратно удалить информацию. По факту же, информация может оставаться (и как правило остаётся) на накопителе и для ее удаления требуются более изощренные методы [4].

С другой стороны, в результате исследований учёных из австралийского университета Мердока в SSD была выявлена целая ветвь проблем с восстановлением данных. Проблем, совершенно не свойственных магнитным дискам и вызванных алгоритмами очистки или "сбора мусора", применяемыми для поддержания твердотельных накопителей на уровне максимальной производительности.

Под действием этих алгоритмов важные для следствия данные, хранимые на современных SSD, зачастую становятся объектом процесса, получившего среди криминалистов название "самокоррозия". Результатом этого процесса становится то, что улики на SSD непрерывно стираются или загрязняются посторонними данными – таким способом, который совершенно не свойственен носителям на базе жёстких магнитных дисков. И, что принципиально важно, все эти перемены с информацией происходят при отсутствии каких-либо команд от пользователя или от компьютера [5].

Результаты австралийских исследователей неизбежно порождают сомнения в целостности и достоверности тех файлов, которые изолируют криминалистическими методами (например, устройствами блокировки записи на накопители) и извлекают из устройств хранения. Можно даже сказать, что обозначилась отчётливая угроза окончания того "золотого века" в сборе цифровых улик, что был обеспечен особенностями хранения данных на магнитных носителях.

Результатом работы индустрии над повышением эффективности памяти SSD стало то, что большинство современных флэш-драйвов имеют встроенные в прошивку программы, которые регулярно и автоматически выполняют процедуры "самоочищения" или "сбора мусора". В результате этих санитарных процедур происходят постоянное затирание, изменение и перенос тех файлов, которые помечены системой как уничтоженные. Причем процесс этот начинается без всякого уведомления и очень быстро, почти сразу после подачи на чип питания. От пользователя не требуется никаких команд, а флэш-драйв при этом не издает никаких звуковых или световых сигналов, чтобы проинформировать пользователя о начале процедуры очистки.

При тестировании конкретного образца, после того как он был подвергнут быстрому форматированию, исследователи ожидали, что утилита очистки начнёт работать примерно минут через 30–60, полагая, что этот процесс должен происходить с SSD перед тем, как новые данные начнут записываться в блоки, прежде занятые файлами. К их удивлению, зачистка произошла всего три минуты спустя, после чего всего лишь 1 064 файла улик от общего числа 316 666 остались доступными для восстановления с диска [6].

Решив проследить этот процесс дальше, ученые вынули флэш-диск из компьютера и подключили его к блокиратору записи – аппаратному устройству, специально предназначенному для изоляции от всех процедур, способных изменить

содержимое носителя. Но и здесь всего через 20 минут после подключения почти 19 процентов всех файлов было затёрто из-за внутренних процессов, которые инициирует прошивка самого SSD без каких-либо внешних команд. Для сравнения можно отметить, что на эквивалентном магнитном жёстком диске все данные после аналогичного форматирования оставались восстановимыми вне зависимости от прошедшего времени – как и ожидалось исследователями.

Эта проблема является результатом механизма TRIM – команда, позволяющая опреационной системе уведомить твердотельный накопитель о том, какие блоки данных больше не используются и могут быть очищены накопителем самостоятельно.

Этот кажущийся парадокс можно объяснить.

Один из непосредственных участников австралийского исследования, Грэм Белл сделал заключение.

Прежде данные на дисках традиционно зачищали вручную, т.е. в явном виде отдавая компьютеру команду, чтобы он велел приводу записать что-то другое поверх прежних данных. Если такой команды на перезапись не поступало, то в магнитных носителях данные продолжали сохраняться. Однако если тот же самый трюк пытаться применять к SSD, то он может не срабатывать. Тот логический адрес памяти, что вы пытаетесь перезаписать, мог быть уже перераспределён на лету, так что ваша команда "перезаписать" идет к какой-нибудь другой физической ячейке памяти, а не к той, которая хранила данные раньше. С логической точки зрения всё это выглядит так, будто перезапись сработала: вы уже не сможете больше получить доступа к этим данным через ОС вашего компьютера. Однако с точки зрения самого флэш-драйва – эти данные всё ещё там, находящиеся в какой-нибудь физической ячейке, которая в данное время не используется, если подразумевать соответствующий логический сектор. Однако какая-нибудь новая прошивка или специалист, в принципе, может получить доступ к этим данным.

Однако в угоду повышения производительности твердотельные накопители могут использовать некоторые собственные функции. Такой функцией и является озвученная функция TRIM, которая заключается в заблаговременном затирании ячеек памяти, в которых содержатся данные, более уже не учитываемые файловой системой. В этом случае привод сам активно пытается непрерывно очищать с диска всё, что только может. Причём делает это всё исключительно по собственной инициативе – просто ради ускорения будущих операций записи, предоставляя заранее заготовленный пул доступных и ни подо что не задействованных ячеек.

Вызваны эти проблемы также и особенностями существующих операционных систем с накопителями. ОС ориентированы в основном на работу с магнитными накопителями (так сложилось исторически), и поэтому работа с твердотельными накопителями не всегда соответствует ожиданиям конечного пользователя. Так, например, исследователи обнаружили, что около 70 % информации, хранимой в файле, остается даже после того, как он был удален с SSD с использованием опции безопасного удаления информации, предлагаемой компанией Apple в ОС Mac OS X (которая по заявлениям производителя, поддерживает полноценную работу с SSD).

У других ОС ситуация не лучше. Windows-системы оставляют почти всю информацию, затирая лишь заголовки и начала файлов. Linux-системы также оставляют почти всю информацию на носителе.

Другие операции по затиранию информации – которые безопасно удаляют файлы путем повторной переписи информации, хранимой в определенном месте на диске – оказались безуспешными с такими же большими показателями при их использовании для удаления отдельного файла с SSD. При осуществлении псевдослучайных операций над данными, например, осталось около 75 % информации, в то время как британская техника HMG IS5 имеет немногим лучшие результаты – 58 %.

Техники по очистке всего диска работают немногим лучше. В случае форматирования SSD в различных файловых системах проблема остаётся. Данные по прежнему остаются на диске. Исследователи на конференции назвали несколько случаев полного удаления данных с SSD. Накопители смогли надежно удалить свои данные после двух попыток полной перезаписи диска, но на операцию потребовалось в различных случаях от 58 до 121 часа для осуществления одного цикла перезаписи, что делает технику нежизнеспособной в большинстве случаев.

Таким образом, получается ситуация, явно показывающая, что современность носителя данных может сыграть злую шутку с безопасностью в информационной системе (кому бы она не принадлежала – коммерческой компании, финансовому заведению, или государственной организации), и что необходимо попрежнему искать решения озвученной проблемы, так как затронутые вопросы по прежнему остаются открытыми.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Сотов А.* Директор по безопасности. – 2011. – № 10. – С. 30.
2. *Warren G. Kruse; Jay G. Heiser*. Computer forensics: incident response essentials. Addison-Wesley, 2002. – С. 16.
3. Eoghan Casey. ed. Handbook of Digital Forensics and Investigation, Various, 2009. – С. 86.
4. Результаты конференции Usenix FAST 11 http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf, 2011. – С. 4.
5. *Graeme B. Bell and Richard Boddington.* Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Discovery // Journal of Digital Forensics, Security and Law. – 2010. – № 3. – P. 11.
6. Результаты конференции Usenix FAST 11 http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf, 2011. – С. 11.

Статью рекомендовал к опубликованию д.т.н., доцент И.В. Щербань.

Тищенко Евгений Николаевич
Ростовский государственный экономический университет.
E-mail: brann@mail.ru.
344007, г. Ростов-на-Дону, ул. Б. Садовая, 69.
Тел.: 88632402123.
Д.э.н.; доцент.

Максимов Алексей Михайлович
E-mail: ironmanpc@rambler.ru.
Тел.: 88632402123.
Аспирант.

Tishchenko Yevgeny Nikolayevich
Rostov State Economic University.
E-mail: brann@mail.ru.
69, B. Sadovaya Street, Rostov-on-Don, 344007, Russia.
Phone: +78632402123.
Dr of Ec. Sc., Associate Professor.

Maksimov Alexsej Mikhajlovich
E-mail: ironmanpc@rambler.ru.
Phone: +78632402123.
Postgraduate Student.