АНАЛИЗ МЕТОДОВ ПРЕДОТВРАЩЕНИЯ УТЕЧКИ ИНФОРМАЦИИ, ХРАНЯЩЕЙСЯ В НАКОПИТЕЛЯХ НА ЖЕСТКИХ МАГНИТНЫХ ДИСКАХ

Гуров В.О., Губенко Н.Е.
Донецкий национальный технический университет

Размещение конфиденциальной информации в устройствах долговременной энергонезависимой памяти компьютеров создает возможность формирования специфических каналов ее утечки. Наиболее распространенными устройствами такого назначения на данный момент являются накопители на жестких магнитных дисках (НЖМД). Широкому применению НЖМД способствует ряд положительных эксплуатационных качеств: надежность, быстрота доступа и относительная дешевизна в расчете на единицу хранимой информации.

Пути или каналы утечки информации, позволяющие несанкционированно и безнаказанно снимать копии с информации, непосредственно связаны с технологиями обработки, передачи и утилизации информации, хранящейся на НЖМД:

1) Утечка информации при замене исправного НЖМД:

a) Перенос ПК на другое место
b) Продажа ПК как "second hand"
c) Дарение ПК

2) Утечка информации при замене неисправного НЖМД.

Основные положения защиты информации, хранимой на НЖМД Обеспечение надежного уничтожения корпоративной информации в конце
жизненного цикла НЖМД требует тщательной проработки вопросов безопасности информации.

Удаление данных с НЖМД само по себе не обеспечивает защиты информации. Процесс ЗИ должен основываться на ряде согласованных методик, обеспечивающих в конечном итоге высокую вероятность уничтожения информации.

Хотя ни одна из методик не может гарантировать 100% надежность уничтожения информации, существуют основные положения и условия защиты информации:

1. Необходимость физической защиты НЖМД. Кража ПК или отдельных накопителей приводит к утечке информации, поэтому необходимо обеспечить их физическую сохранность с момента окончания срока эксплуатации до получения документированного подтверждения об уничтожении данных.

2. Систематический контроль и ведение отчетности. Систематический контроль подразумевает отслеживание выбывающих из эксплуатации накопителей, контроль процесса уничтожения информации и составление отчета об отклонениях в этом процессе и допущенных ошибках.

Таким образом, процедура обеспечения защиты информации, хранимой на НЖМД, должна включать следующие действия:

1. Физическая защита информации, включающая в себя инвентаризацию и ограничения доступа к НЖМД.

2. Систематический контроль над процессом замены, передачи и уничтожения информации на НЖМД.

3. Использование стандартизованных приложений и методик по уничтожению

информации на НЖМД.

4. Систематическая проверка процессов уничтожения информации на НЖМД.

5. Периодический контроль надежности уничтожения информации с произвольно выбранных НЖМД.

6. Выбор методик и способов для уничтожения информации на неисправных НЖМД, путем анализа категорийности хранимой на них информации.

7. Обеспечение процедуры сбора и уничтожения НЖМД.

8. Ведение отчетности по каждому уничтоженному НЖМД.

Способы уничтожения информации на НЖМД делятся на три большие группы:

1. Программные, в основу которых положено уничтожение информации, записанной на магнитном носителе, посредством штатных средств записи информации на магнитных носителях. В случае уничтожения информации на НЖМД программным методом, он может быть повторно использован в других ПК, после инсталляции новой ОС и приложений. Уничтожение производится наиболее простым и естественным способом - перезаписью информации. Следует отметить очень важную деталь - при перезаписи информации работоспособность НЖМД полностью сохраняется, в случае, если он был полностью исправным. На изношенном или неисправном НЖМД провести надежное уничтожение информации невозможно.

2. Механические, связанные с механическим повреждением основы, на которую нанесен магнитный слой - физический носитель информации.

3. Физические, связанные с физическими принципами цифровой записи на магнитный носитель, и основанные на перестройке структуры магнитного материала рабочих поверхностей носителя.

По способу воздействия на накопитель:

a. без разрушения гермокамеры и рабочих поверхностей НЖМД;

b. с разрушением НЖМД.

Наиболее выгодными экономически являются программные методы. Программные методы уничтожения информации на НЖМД имеют следующие недостатки:

1. Низкая надежность уничтожения информации. После применения программных методов стирания информации перезаписью имеется возможность восстановления информации квалифицированным экспертом с помощью или без специальных средств.

2. Длительное время перезаписи информации носителя (десятки минут, часы). При многопроходной перезаписи время уничтожения информации для одного носителя умножается на количество проходов.

3. Перезапись информации возможна только на исправном НЖМД. Достоинства:

1. Имеется возможность повторного использования НЖМД;

2. Низкая цена и стоимость эксплуатации ПО или специальных средств.

Література

[1] www.epos.kiev.ua «Безопасность хранения информации на жестких дисках»

[2] «Бизнес и безопасность» №2/2005 «Анализ возможностей предотвращения утечки информации, хранящейся в накопителях на жестких магнитных дисках»