Т.7/97

СК РОССИИ

Следственное управление
по Свердловской области
(СУ СК России по Свердловской области)

ул. Карла Маркса, 43-А, г. Екатеринбург,
Россия, 620026

_____ № _____

На № 2012ОЦ79/23

Следователю-криминалисту
следственного отдела по г. Тобольск
следственного управления
Следственного комитета Российской
Федерации по Тюменской области

капитану юстиции

Р.Р. Хабибуллину

«О направлении заключения эксперта»

Направляю, в Ваш адрес, заключение эксперта № 99ктэ от 15.01.2013, выполненное на основании вынесенного Вами постановления о назначении компьютерно-технической экспертизы.

Приложение: заключение эксперта на 18 листах;
приложение к заключению эксперта оптический диск, 1 шт.;
ноутбук, 2 шт.;
системный блок, 1 шт.

И.о. руководителя
экспертно-криминалистического отдела
Следственного управления Н.Б. Стяжкина

СЛЕДСТВЕННЫЙ КОМИТЕТ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Следственное управление
по Тюменской области
СЛЕДСТВЕННЫЙ ОТДЕЛ
по г. Тобольск
Вх. № 01-02 2013

Исп.: Мкртчян Е.Г.
тел.295-18-44

т. 7/98

ПОДПИСКА

Мне, сотруднику Следственного управления Следственного комитета Российской Федерации по Свердловской области Мкртчяну Евгению Георгиевичу, в соответствии с ч.2 ст.199 УПК России разъяснены права и ответственность эксперта, предусмотренные ст. 57 УПК России.

Об ответственности за дачу заведомо ложного заключения по ст.307 УК России предупреждён.

09.10.2012 _____ Мкртчян Е.Г.

ЗАКЛЮЧЕНИЕ ЭКСПЕРТА № 99ктэ

г. Екатеринбург производство экспертизы начато в 09 ч 00 мин 28.11.2012
окончено в 17 ч 30 мин 15.01.2013

Постановлением от 03 октября 2012 г. следователя-криминалиста следственного отдела по г. Тобольск следственного управления Следственного комитета Российской Федерации по Тюменской области капитана юстиции Хабибуллина Р.Р. назначена судебная компьютерно-техническая экспертиза по уголовному делу № 201200079/23.

Производство экспертизы поручено эксперту экспертно-криминалистического отдела Следственного управления Следственного комитета Российской Федерации по Свердловской области Мкртчяну Евгению Георгиевичу, имеющему высшее образование, экспертную специальность судебная компьютерно-техническая экспертиза, стаж экспертной работы 4 года. Экспертиза проведена в лаборатории компьютерно-технической экспертизы экспертно-криминалистического отдела Следственного управления Следственного комитета Российской Федерации по Свердловской области, по адресу: г. Екатеринбург, ул. Фрунзе, д. 40, к. 2.

На разрешение эксперта поставлены следующий вопрос:

1. Имеются ли на жестких дисках системного блока и двух ноутбуках сведения о доступах к сайтам в сети Интернет?
2. Имеются ли на жестких дисках системного блока и двух ноутбуках файлы содержащие слова: алюминиевая пудра, аммиачная селитра, марганцовка, порох, магний, взрыв?
3. Имеются ли на жестких дисках системного блока и двух ноутбуках удаленные файлы? Если да, возможно ли из восстановить?

ЭКСПЕРТНОЕ ОБОРУДОВАНИЕ И МЕТОДИЧЕСКАЯ ЛИТЕРАТУРА, ИСПОЛЬЗОВАННЫЕ ПРИ ПРОВЕДЕНИИ ИССЛЕДОВАНИЯ

Аппаратно-программный комплекс для экспертного исследования компьютерных носителей информации в составе:

– персональная ЭВМ производства фирмы ООО «Целевые технологии» (Россия);

– лазерный принтер «LaserJet P2055d» производства фирмы «Hewlett Packard» (США);

– цифровой фотоаппарат модель «PowerShot A1100IS», производства фирмы «Canon» (Китай);

– криминалистическая линейка;

– сетевое хранилище данных QNAP NAS Server TS-439 Pro;

– адаптер с встроенной опцией блокирования записи модель «T35es», производства фирмы «Tableau» (США);

– операционная система «Microsoft Windows 7 Максимальная» производства фирмы «Microsoft» (США);

– прикладное программное обеспечение «OpenOffice.org» версия 3.3 производства фирмы «Sun Microsystems Inc.»;

– прикладное программное обеспечение для восстановления файлов «R-Studio» версия 6.1 производства фирмы «R-Tools Technology Inc.»;

– антивирусное программное обеспечение «Kaspersky CRYSTAL» производства фирмы ЗАО «Лаборатория Касперского» (Россия);

– программное обеспечение для криминалистического исследования носителей информации «Encase Forensic» производства фирмы «Guidance Software» (США);

– программное обеспечение для экспертного исследования компьютерных носителей информации «Forensic Assistant» (Россия).

Методическая и справочная литература:

Зубаха В.С., Усов А.И., Саенко Г.В. и др. Общие положения по назначению и производству компьютерно-технической экспертизы: Методические рекомендации. – М.: ГУ ЭКЦ МВД России, 2001г;

Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. – М., 2001г;

Усов А.И. Методы и средства решения задач компьютерно-технической экспертизы: Учебное пособие. – М.: ГУ ЭКЦ МВД России, 2002г;

Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения: Учебное пособие / А.И. Усов // Под ред. проф. Е.Р. Россинской. – М., 2003г;

Тушканова О.В. Терминологический справочник судебной компьютерной экспертизы. Справочное пособие. – М., : ГУ ЭКЦ МВД России, 2005г;

Нехорошев А. Б., Шухнин М. Н., Юрин И. Ю., Яковлев А. Н. Практические основы компьютерно-технической экспертизы – Саратов, Национальный центр по борьбе с преступлениями в сфере высоких технологий, 2007г.

Перечень объектов, представленных согласно постановлению:

– системный блок «R-Style» и ноутбук «hp» изъятые по адресу Тюменская область, г. Тобольск, 10 микр., дом 24, кв. 51;

– ноутбук «Lenovo» в корпусе чёрного цвета изъятый по адресу Тюменская область, Тобольский район, дачный кооператив «Механизатор», ул. Плодовая, дом 49.

Осмотр представленных объектов

На исследование поступили объекты:

1. Упаковка № 1, пакет из непрозрачной полимерной плёнки чёрного цвета заклеенный фрагментом бумаги светло-синего цвета (фото. 1, 2). На фрагменте бумаги имеются подписи, нечёткий неразборчивый оттиск круглой печатной формы «Для пакетов» и текст, прочитанный как «Следственный комитет при прокуратуре Российской Федерации Пакет № Уголовное дело № *201200079/23* Описание объекта находящегося в пакете *Ноутбук "Lenovo", изъятый в ходе обыска по адресу Тюменская область, Тобольский р-н дачный кооператив "Механизатор", ул. Плодовая д.49* Дата, место и обстоятельства изъятия:». Используемый способ упаковки не позволяет получить доступ к содержимому пакета без его повреждения. Видимых нарушений целостности упаковки не обнаружено. Из пакета извлечён портативный компьютер типа «ноутбук» (далее **ноутбук № 1**) в корпусе размером 380х250х35 мм чёрного цвета (фото. 3, 4).

На верхней поверхности компьютера имеется надпись «lenovo».

На нижней поверхности компьютера имеются:

– наклейка с надписью, прочитанной как «… lenovo …»;

– наклейка с надписью, прочитанной как «Lenovo G565 Model Name… 20071… S/N: CB05656072…»;

– наклейка сертификата подлинности с текстом, прочитанным как «Windows 7 Home Basic… Product Key: BMWG7-348QQ-CRDJF-T2CKD-M7DR4…».

На боковых поверхностях корпуса компьютера имеются:

– один разъём электрического питания;

– один разъем типа «D-Sub» («VGA»);

– один разъём типа «RJ-45»;

– один разъём для установки карт расширения;

– два разъёма типа «Jack-3.5»;

– три разъёма типа «USB»;

– один разъём для установки карт памяти. В разъём установлена пластина из полимерного материала чёрного цвета.

На рабочей поверхности имеются наклейки с текстом, прочитанным как «lenovo…», «Windows 7», «ULTIMATE VISION AMD».

Для хранения информации в представленном компьютере установлен накопитель на жёстких магнитных дисках (далее **НЖМД № 1**) в корпусе чёрного цвета, крышка корпуса светло-серого цвета (фото. 5). На крышке корпуса имеются наклейки белого цвета с текстом, прочитанным как «Seagate… 320GB… SN: 5VEEKMNK… ST9320325AS», «AM0E5000100 SINO 0A 10C7», «HDD 11S16004183ZZ1MP0CR29F AC».

В батарейном отсеке установлен аккумулятор, на поверхности которого имеется наклейки с текстом, прочитанным как «lenovo… Model Name… L09S6Y02… », «11S121000938Z1000C94E6 2010.12». Внутри батарейного отсека имеется наклейка с текстом, прочитанным как «2522118300305 PAWE8320840».

Кроме того, в пакете находился адаптер электрического питания. На корпусе адаптера имеется наклейка с текстом «lenovo… MODEL… ADP-90DDB… 11S36001647ZZ1000B87N0».

2. Упаковка № 2, пакет из непрозрачной полимерной плёнки чёрного цвета, горловина пакета перевязана фрагментом нити белого цвета, концы нити заклеены фрагментом бумаги белого цвета (фото. 6, 7). На фрагменте бумаги имеются подписи, нечёткий неразборчивый оттиск круглой печатной формы «Для пакетов» и текст, прочитанный как «*Пакет: ноутбук "HP" изъятый в ходе обыска 28.06.12г по адресу: г. Тобольск* ». Используемый способ упаковки не позволяет получить доступ к содержимому пакета без его повреждения. Видимых нарушений целостности упаковки не обнаружено. Из пакета извлечена сумка из материала чёрного цвета (фото. 8). Из сумки извлечён портативный компьютер типа «ноутбук» (далее **ноутбук № 2**) в корпусе размером 325x270x35 мм чёрного цвета (фото. 9, 10).

На верхней поверхности компьютера имеется надпись «hp».

На нижней поверхности компьютера имеются:
– наклейка с надписью, прочитанной как «hp… HTSNN-I05C…»;
– наклейка с надписью, прочитанной как «… S/N: CNU5521GRG…»;
– наклейка сертификата подлинности с текстом, прочитанным как «Windows XP Professional… Product Key: P4DR9-M7QVK-R9Y44-CFVP9-76XMQ…».

На боковых поверхностях корпуса компьютера имеются:
– один разъём электрического питания;
– один разъем типа «D-Sub» («VGA»);
– один разъём типа «RJ-12»;
– один разъём типа «RJ-45»;

 7.7/102

– один разъём типа «IEEE1394» («FireWire»);
– один разъем типа «PS/2»;
– один разъем типа «COM» (9 pin);
– один разъем типа «LPT»;
– два разъёма типа «Jack-3.5»;
– четыре разъёма типа «USB»;
– два разъёма для установки карт расширения;
– один разъём для установки карт памяти. В разъём установлена пластина из полимерного материала чёрного цвета.

Для хранения информации в представленном компьютере установлен накопитель на жёстких магнитных дисках (далее **НЖМД № 2**) в корпусе чёрного цвета, крышка корпуса светло-серого цвета (фото. 11). На крышке корпуса имеются наклейки белого цвета с текстом, прочитанным как «FUJITSU… MHV2040AH… SER. NO. NT30T5C2BS3L… 40.0GB», «…S/N: 2D9901JCS1VZ3…», «202M1-C8S-Y6HSBFC-5X35…».

В батарейном отсеке установлен аккумулятор, на поверхности которого имеется наклейки с текстом, прочитанным как «Hewlett-Packard… HSTNN-IB05…», «…S/N:6D3F01JCSK3BHK…», «…398854-001», «6027B0006001», «A04D4H510092Y».

Кроме того, в сумке находился адаптер электрического питания. На корпусе адаптера имеется наклейка с текстом «hp… DC359A… CT:592C70AMFSL09A…».

3. Системный блок собранный в корпусе размером 495x415x185 мм чёрного цвета с декоративным элементом серого цвета на лицевой панели. Боковые панели заклеены фрагментами прозрачной неокрашенной полимерной липкой ленты типа «скотч» (фото. 12 – 17). Фрагментами липкой ленты к корпусу приклеен фрагмент бумаги белого цвета. На фрагменте бумаги имеются подписи, оттиск круглой печатной формы «Для пакетов № 6 Следственный комитет Российской Федерации следственное управление по Тюменской области Следственный отдел г. Тобольск», рукописная пояснительная надпись, прочитанная как «*Пакет № 10 Системный блок серийный номер 907 97 12. изъятый в ходе обыска 28-06.2012 года по адресу: г. Тобольск 10 микр., дом 24, кв. 51.*». Используемый способ упаковки не позволяет получить доступ к содержимому системного блока.

На лицевой панели корпуса системного блока имеются:
– четыре отсека для устройств формата 5,25 дюйма. В верхнем отсеке выведена лицевая панель накопителя на оптических дисках. Остальные отсеки закрыты декоративными элементами светло-серого цвета;

– два отсека для устройств формата 3,5 дюйма. В верхнем отсеке выведена лицевая панель накопителя на гибких магнитных дисках формата 3,5 дюйма. Нижний отсек закрыт декоративным элементом чёрного цвета;
– два разъёма типа «Jack-3.5»;
– два разъёма типа «USB»;
– две кнопки;
– два световых индикатора.

На боковой панели системного блока имеется наклейка сертификата подлинности с текстом, прочитанным как «Windows XP Home… Product Key: JRDMC-P2KTG-YRPX3-C6VBH-W9DC6…».

На тыльной стороне корпуса системного блока имеются:
– один разъем электрического питания;
– два разъема типа «PS/2»;
– один разъем типа «COM» (9 pin);
– один разъем типа «LPT»;
– один разъем типа «D-Sub» («VGA»);
– один разъем типа «IEEE 1394» («FireWire»);
– четыре разъема типа «USB»;
– один разъем типа «RJ-45»;
– шесть разъемов типа «Jack-3,5»;
– семь технологических отверстий для установки плат расширения, все отверстия закрыты защитными планками,
– наклейки с текстом, прочитанным как «…R-Style Proxima … Серийный номер 9079712…», «КОНТРОЛЬ КАЧЕСТВА 335383» , «КОНТРОЛЬ КАЧЕСТВА 335384».

При визуальном осмотре системного блока со снятой боковой стенкой (фото. 18) обнаружено, что в данный системный блок установлены блок питания, на корпусе которого имеются наклейки с текстом, прочитанным как «POWER MASTER MODEL… PM (P4) 350W P …», «R 801200…», «2006 12 NO:FL 012356», системная плата на которой имеется маркировка прочитанная как «ASUS», «P5LD2-VM/S». В слоты для установки оперативной памяти установлен один модуль памяти. На модуле памяти имеются наклейки с текстом, прочитанным как «Apacer… 256MB… S/N:230702110028…», «R 1200043 7…».

В монтажной стойке системного блока установлено:
– один накопитель на оптических дисках формата 5,25 дюйма;
– один накопитель на гибких магнитных дисках формата 3,5 дюйма.
Данные устройства из стойки не вынимались и не описывались.

Для хранения информации в представленном системного блоке установлен накопитель на жёстких магнитных дисках (обозначенный как

НЖМД № 3) в корпусе чёрного цвета, крышка корпуса светло-серого цвета (фото. 19). На крышке корпуса имеются наклейки белого цвета с текстом, прочитанным как «HITACHI… MODEL: HDS728080PLA380… 82.3GB… S/N: ELU54D3H…», «R 121376 7…».

Просмотром настроек часов, установленных на системной плате, при помощи программы настройки конфигурации BIOS (BIOS – Basic Input/Output System – базовая система ввода/вывода) установлено соотношение между текущими временем (екатеринбургский часовой пояс) и временем, установленным на часах системной платы (см. таблицу 1).

Таблица 1

Дата и время, установленные на часах системной платы	Текущие дата и время (екатеринбургский часовой пояс)
24.10.2012 14:40	24.10.2012 14:36

Исследование НЖМД

НЖМД № 1 – 3 поочерёдно подключали через блокиратор записи «T35es» к стендовой ПЭВМ. Запись на НЖМД № 1 – 3 была заблокирована.

При этом установлено, что:

– доступ к информации имеющейся на НЖМД № 1 ограничен паролем. Получить доступ к информации имеющейся на НЖМД № 1 при помощи средств имеющихся в распоряжении эксперта не представляется возможным;

– НЖМД № 2, 3 имеют следующую логическую структуру (см. таблицу 2):

Таблица 2

№ НЖМД	№ раздела	Метка тома	Файловая система	Объём (Мб)	Занято (Мб)
2	1		NTFS	38 147,0	7 775,3
3	1		NTFS	78 520,8	7 297,9

При помощи специального программного обеспечения «R-Studio», «Encase Forensic» произведено восстановление удаленной информации в отдельные каталоги на внешнем сетевом хранилище данных QNAP NAS Server TS-439 Pro. После этого, для обеспечения сохранности и неизменности информации в процессе исследования, была сделаны полные посекторные копии (образы) НЖМД № 2, 3 на внешнем сетевом хранилище данных QNAP NAS Server TS-439 Pro с использованием специального программного обеспечения для экспертного исследования компьютерных носителей информации «Encase Forensic». НЖМД № 2, 3 отключены, а исследование информации проводилось на их полных копиях.

1. Для ответа на поставленный вопрос «Имеются ли на жестких дисках системного блока и двух ноутбуках сведения о доступах к сайтам в сети Интернет?» НЖМД № 2, 3 и каталоги с восстановленными файлами просматривали с целью обнаружения файлов содержащих сведения о доступе к ресурсам сети «Интернет». В результате поиска установлено, что на НЖМД № 2, 3 имеются сведения о доступе к сайтам сети «Интернет». Сведения о дате и времени и посещённых ресурсах сети «Интернет» представлены в приложении к заключению эксперта и сохранены на оптический диск.

2. Для ответа на поставленный вопрос «Имеются ли на жестких дисках системного блока и двух ноутбуках файлы содержащие слова: алюминиевая пудра, аммиачная селитра, марганцовка, порох, магний, взрыв?» НЖМД № 2, 3 и каталоги с восстановленными файлами просматривали с целью обнаружения файлов содержащих указанные сведения. Программами контекстного поиска осуществляли поиск ключевым словам «алюминиевая пудра», «аммиачная селитра», «марганцовка», «порох», «магний», «взрыв». В результате поиска на НЖМД № 2, 3 файлов, в том числе удалённых содержащих ключевые слова: «алюминиевая пудра», «аммиачная селитра», «марганцовка», «порох», «магний», «взрыв», не обнаружено.

3. Для ответа на поставленный вопрос «Имеются ли на жестких дисках системного блока и двух ноутбуках удаленные файлы? Если да, возможно ли из восстановить?» НЖМД № 2, 3 и каталоги с восстановленными файлами просматривали с целью обнаружения удалённых файлов восстановление которых возможно. В результате поиска установлено, на НЖМД № 2, 3 имеются удалённые файлы восстановление которых возможно.

Эксперт отмечает, что дата и время последнего доступа к ресурсам сети «Интернет», фиксируются по часам операционной системы и могут не совпадать с действительными (текущими) датами и временем. Кроме того, дата и время могут быть изменены пользователем или программами.

Таким образом, в результате проведённого исследования накопителей на жёстких магнитных дисках (НЖМД № 1 – 3) установленных в представленных системном блоке и ноутбуках, установлено, что:

– доступ к информации имеющейся на НЖМД № 1 ограничен паролем. Получить доступ к информации имеющейся на НЖМД № 1 при помощи средств имеющихся в распоряжении эксперта не представляется возможным;

– на НЖМД № 2, 3 имеются файлы, содержащие сведения о доступе к ресурсам сети «Интернет». Сведения о дате и времени и посещённых

ресурсах сети «Интернет» представлены в приложении к заключению эксперта и сохранены на оптический диск;

– на НЖМД № 2, 3 файлов, в том числе удалённых, содержащих ключевые слова: «алюминиевая пудра», «аммиачная селитра», «марганцовка», «порох», «магний», «взрыв», не обнаружено;

– на НЖМД № 2, 3 имеются удалённые файлы восстановление которых возможно.

ВЫВОДЫ

1. На накопителях на жёстких магнитных дисках (НЖМД № 2, 3) установленных в представленных ноутбуке № 2 и системном блоке имеются файлы, содержащие сведения о доступе к ресурсам сети «Интернет». Сведения о дате и времени и посещённых ресурсах сети «Интернет» представлены в приложении к заключению эксперта и сохранены на оптический диск.

2. На накопителях на жёстких магнитных дисках (НЖМД № 2, 3) установленных в представленных ноутбуке № 2 и системном блоке файлов, в том числе удалённых, содержащих ключевые слова: «алюминиевая пудра», «аммиачная селитра», «марганцовка», «порох», «магний», «взрыв», не обнаружено.

3. На накопителях на жёстких магнитных дисках (НЖМД № 2, 3) установленных в представленных ноутбуке № 2 и системном блоке имеются удалённые файлы восстановление которых возможно.

ЭКСПЕРТ Е.Г. Мкртчян

Приложение
к заключению эксперта
№ 99ктэ от 15.01.2013

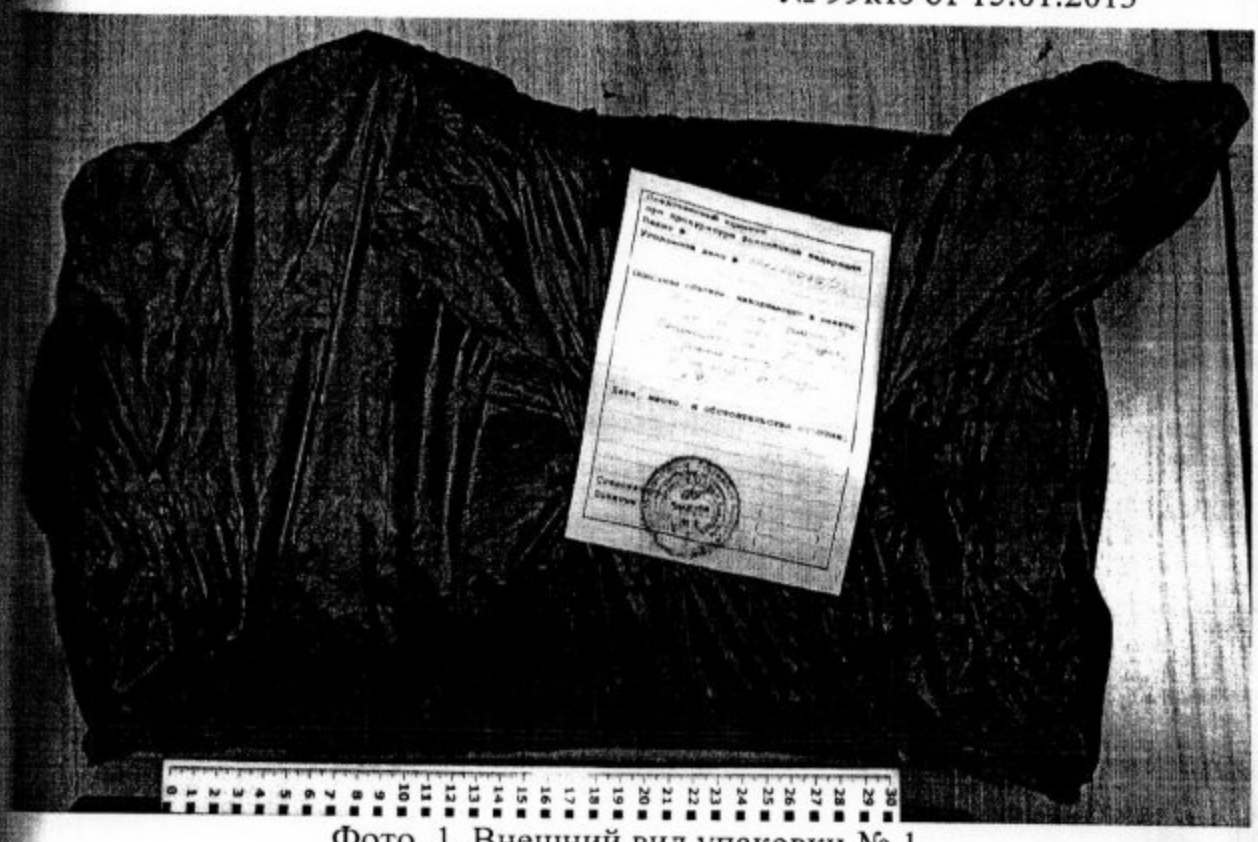

Фото. 1. Внешний вид упаковки № 1

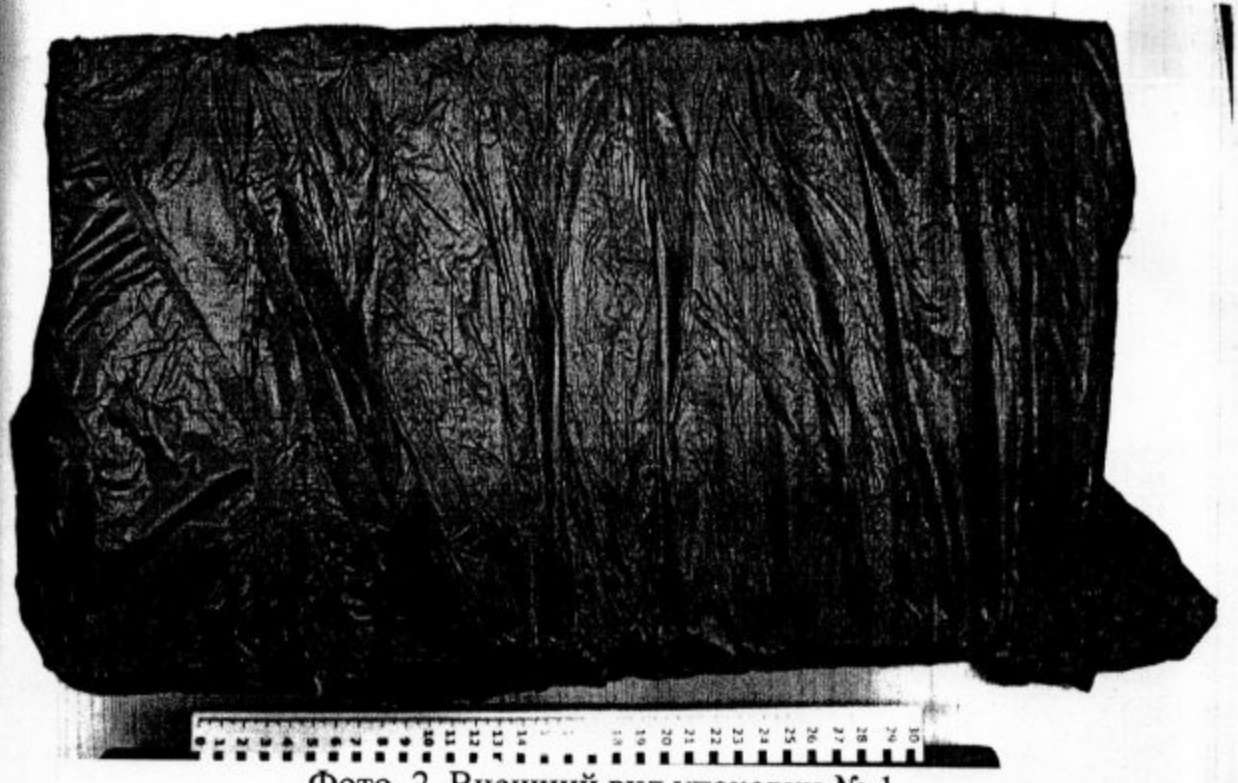

Фото. 2. Внешний вид упаковки № 1

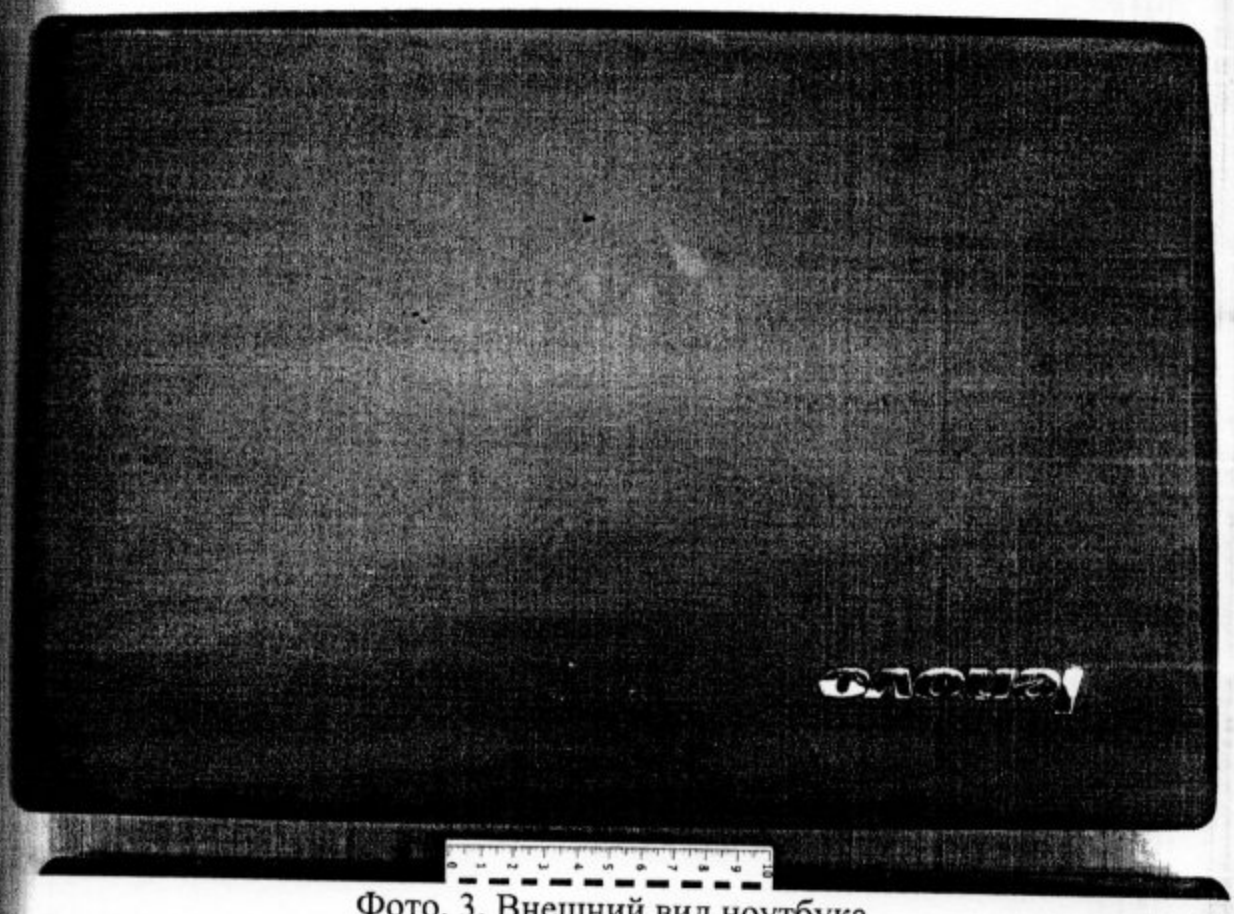

Фото. 3. Внешний вид ноутбука

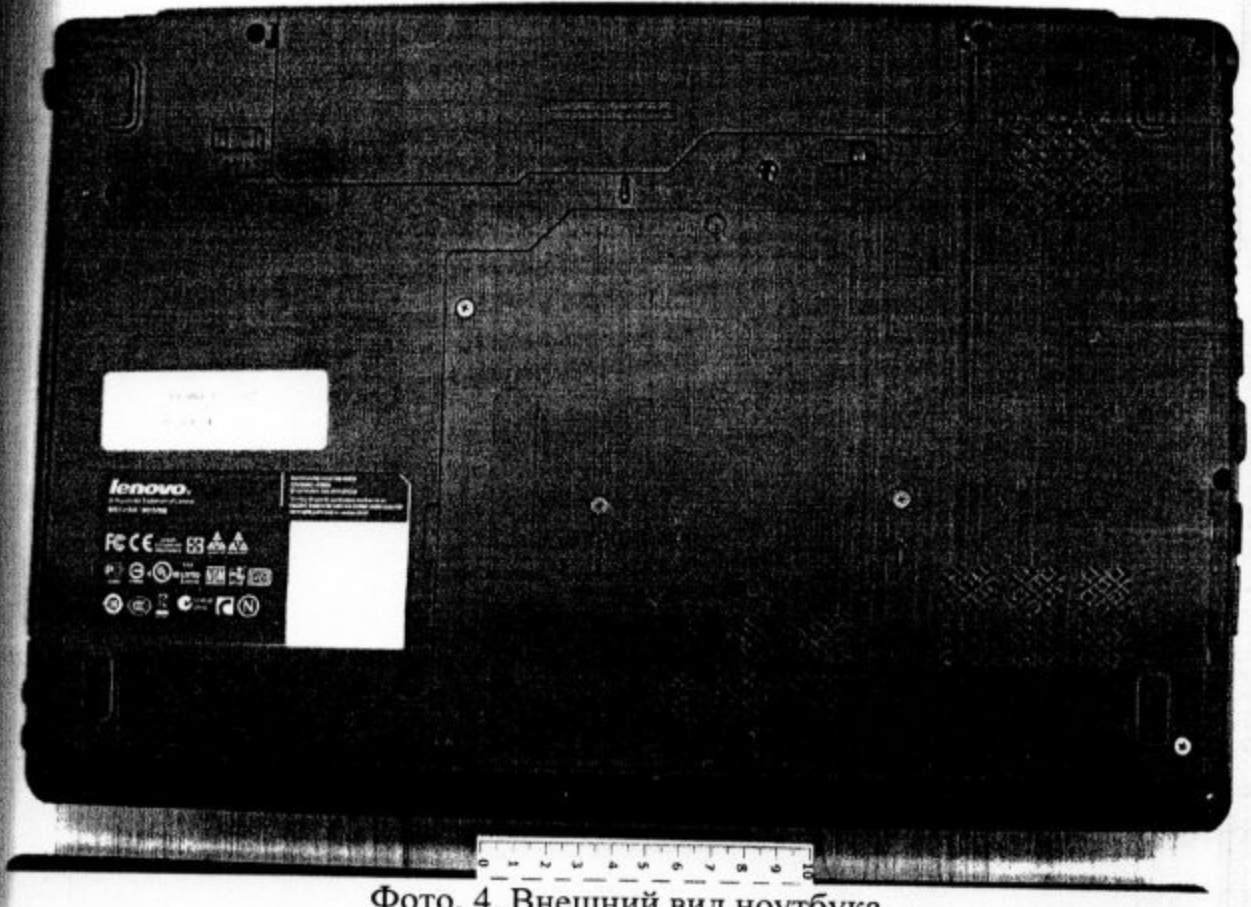

Фото. 4. Внешний вид ноутбука

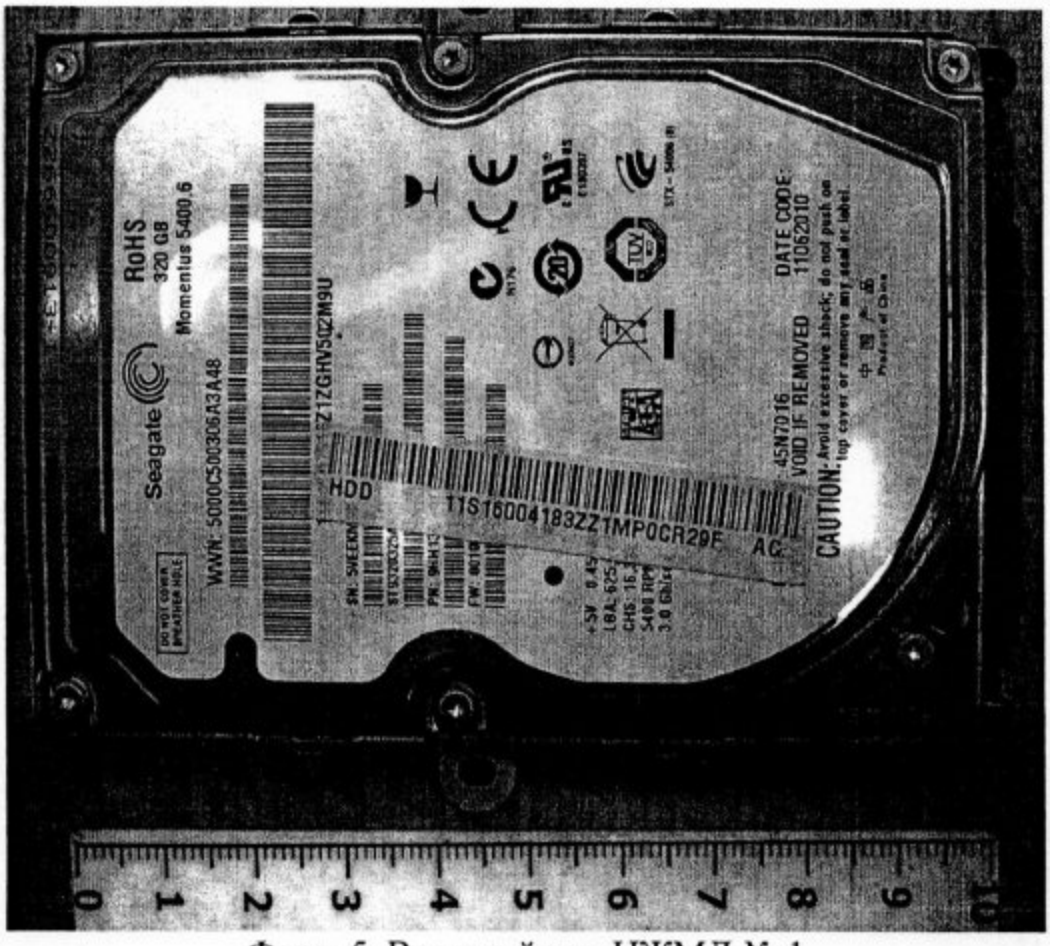

Фото. 5. Внешний вид НЖМД № 1

Фото. 6. Внешний вид упаковки № 2

Фото. 7. Внешний вид упаковки № 2

Фото. 8. Внешний вид сумки

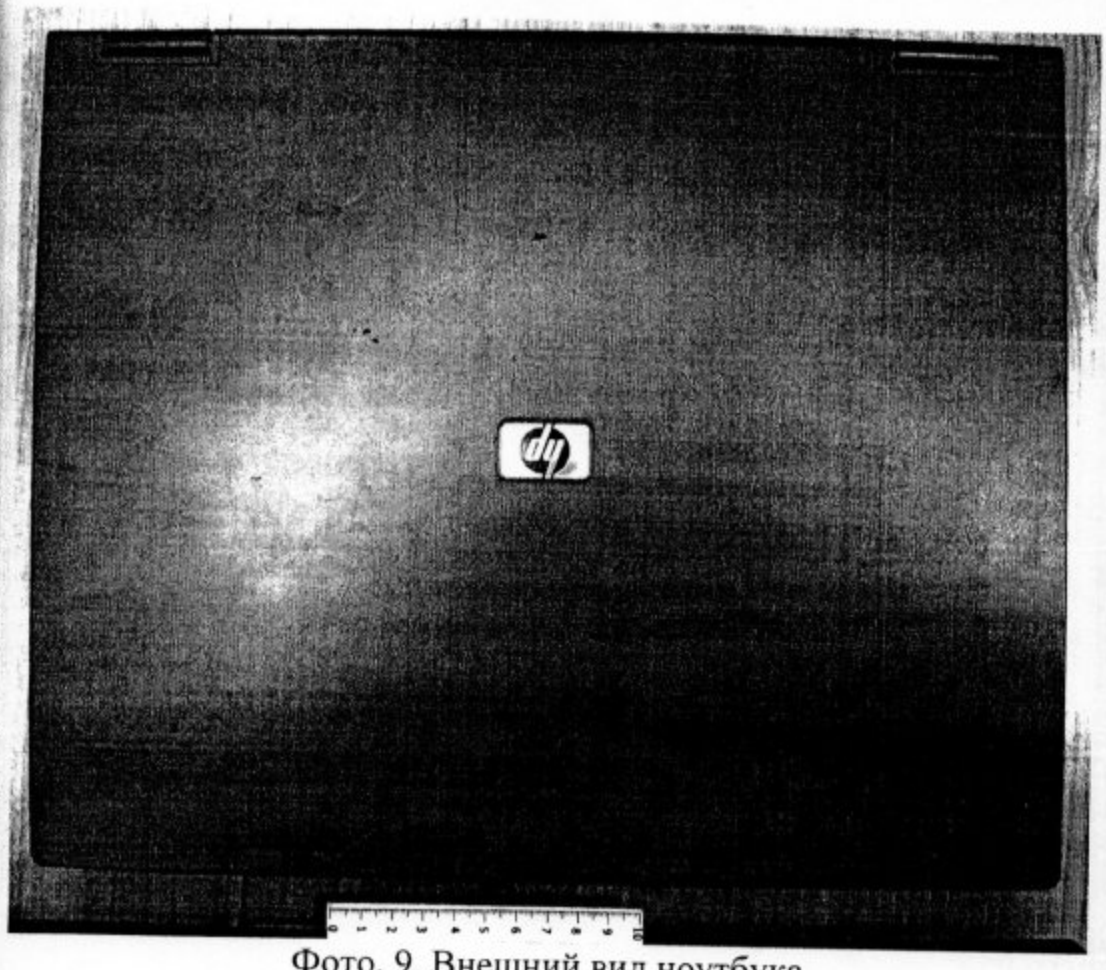

Фото. 9. Внешний вид ноутбука

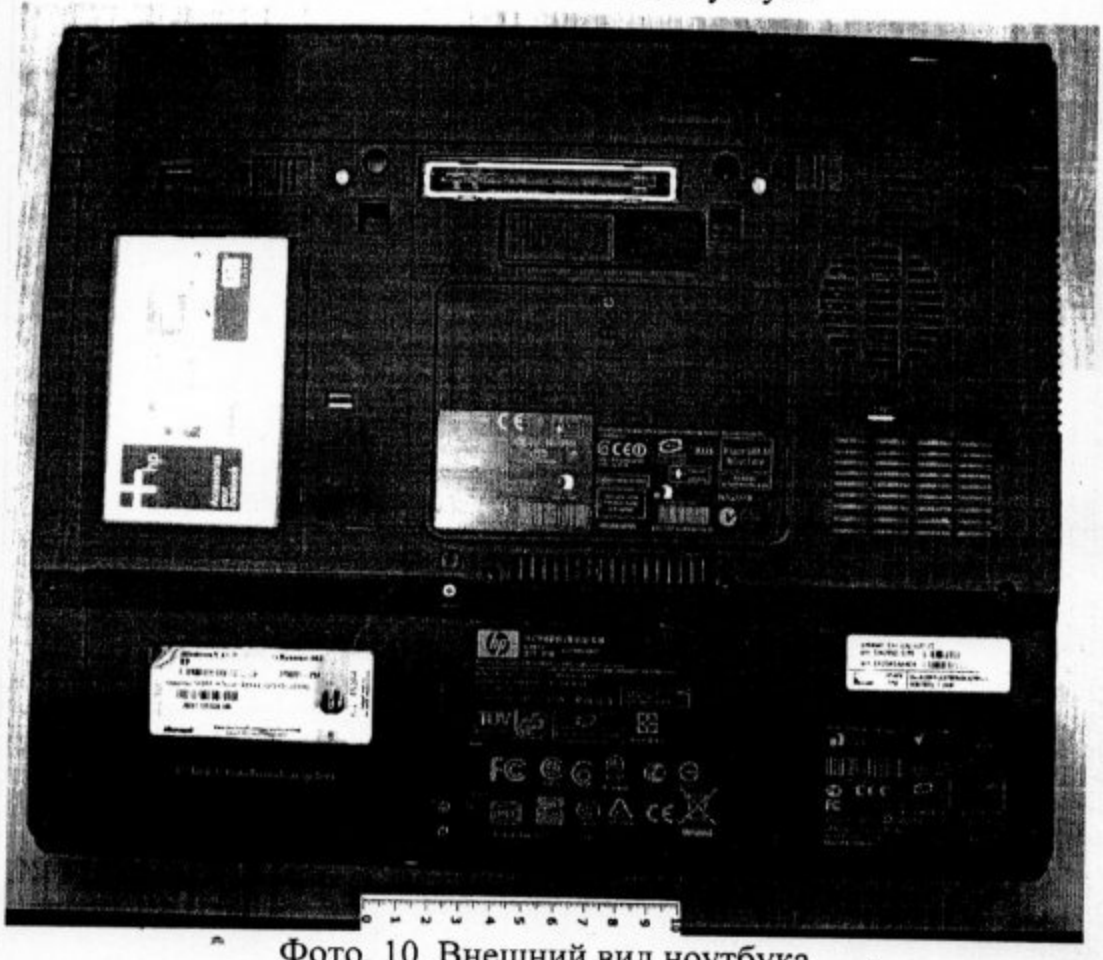

Фото. 10. Внешний вид ноутбука

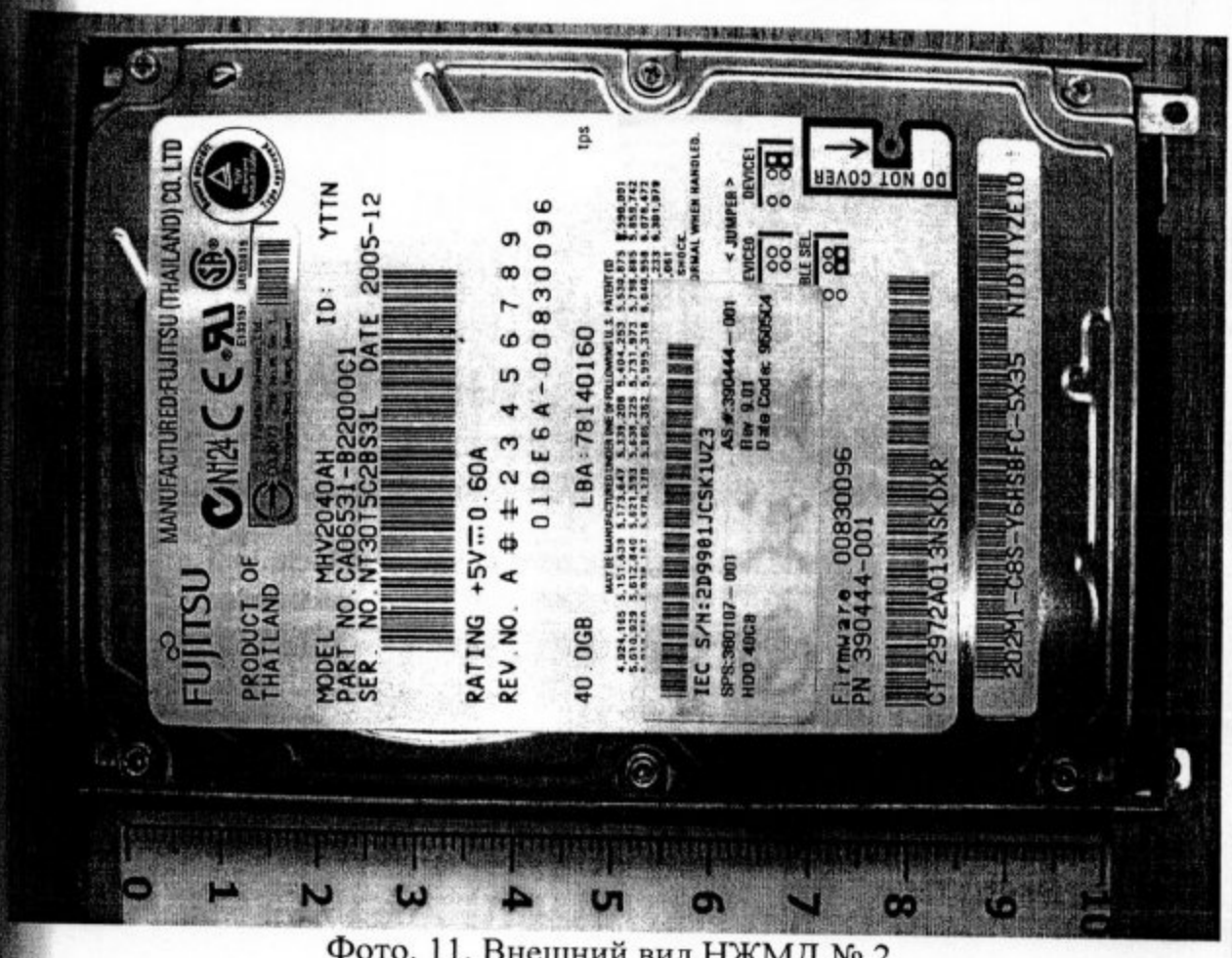

Фото. 11. Внешний вид НЖМД № 2

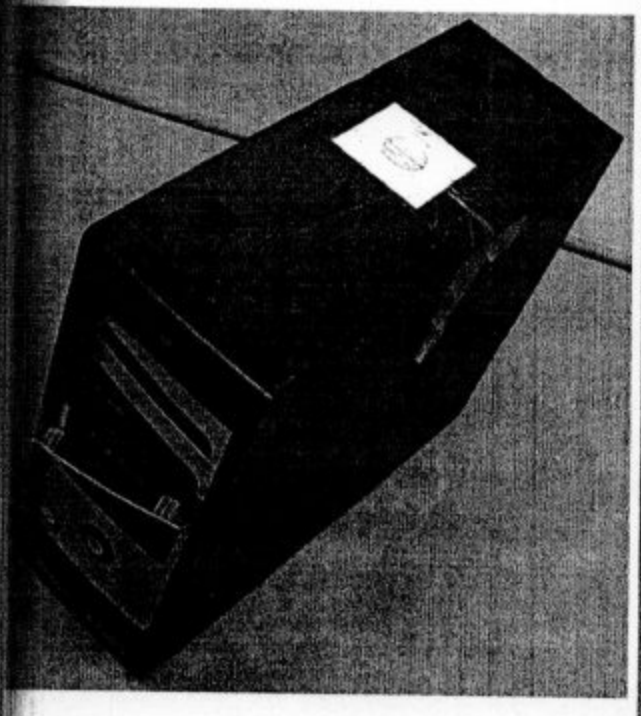

Фото. 12. Внешний вид системного блока

Фото. 13. Внешний вид системного блока

 77/113

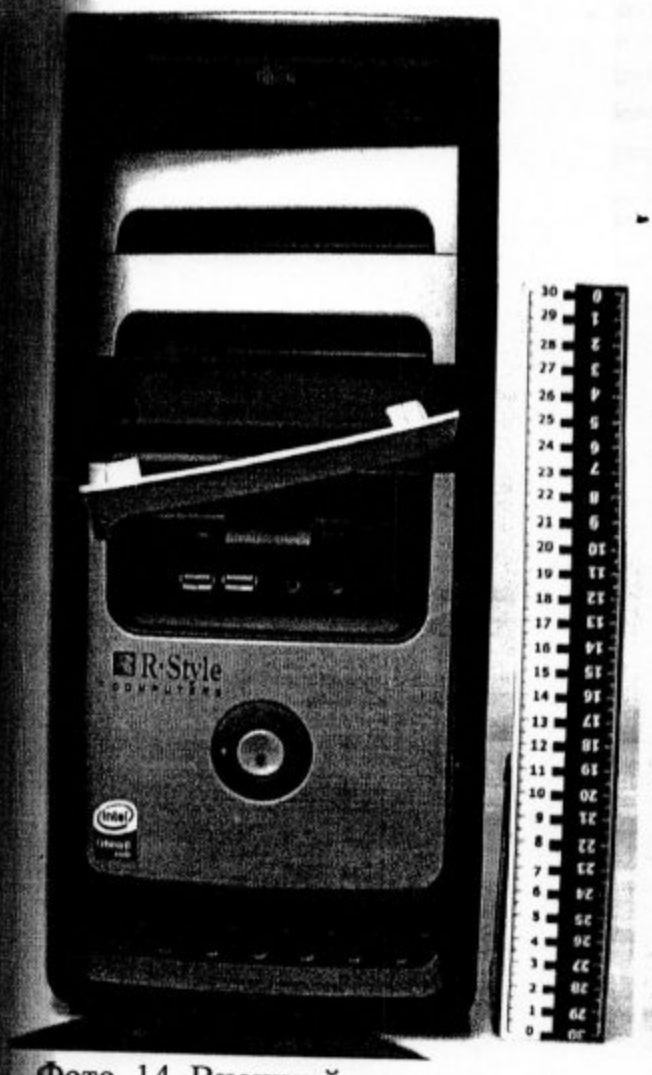

Фото. 14. Внешний вид системного блока

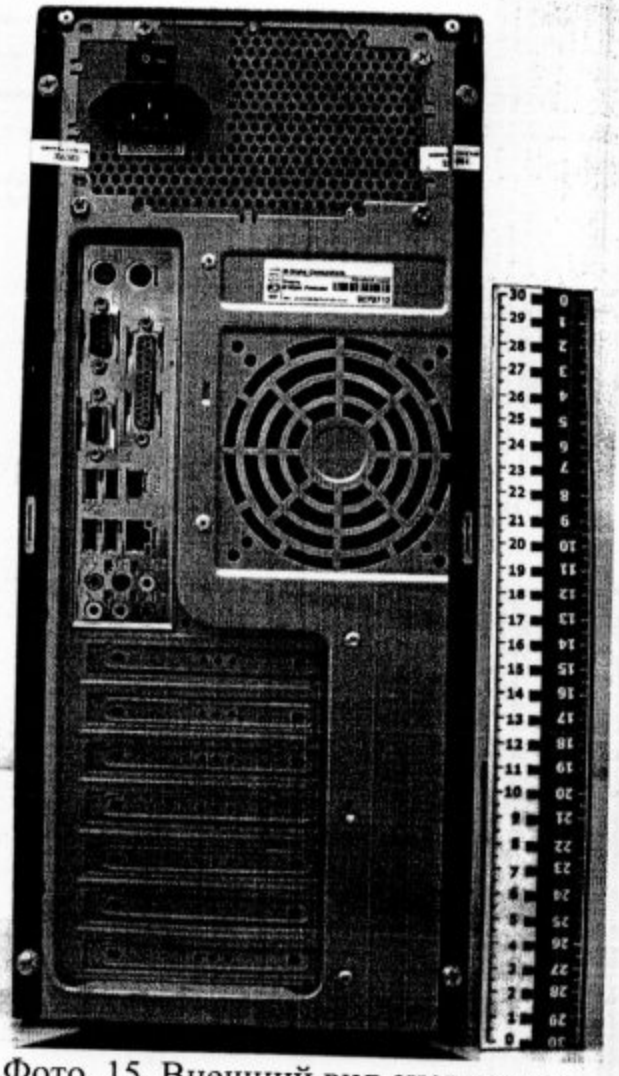

Фото. 15. Внешний вид системного блока

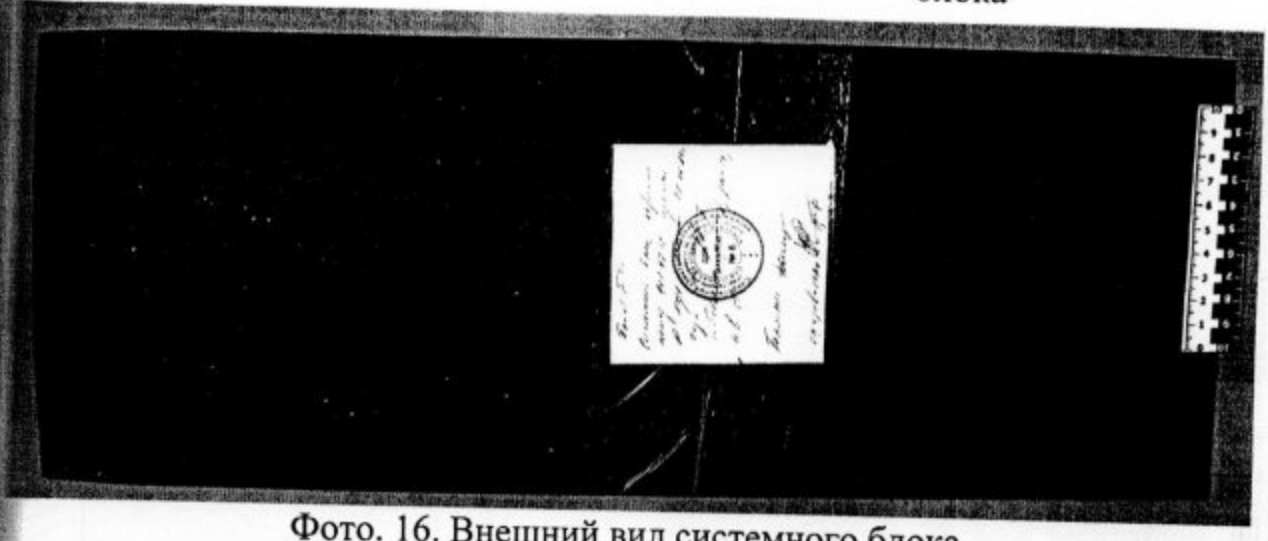

Фото. 16. Внешний вид системного блока

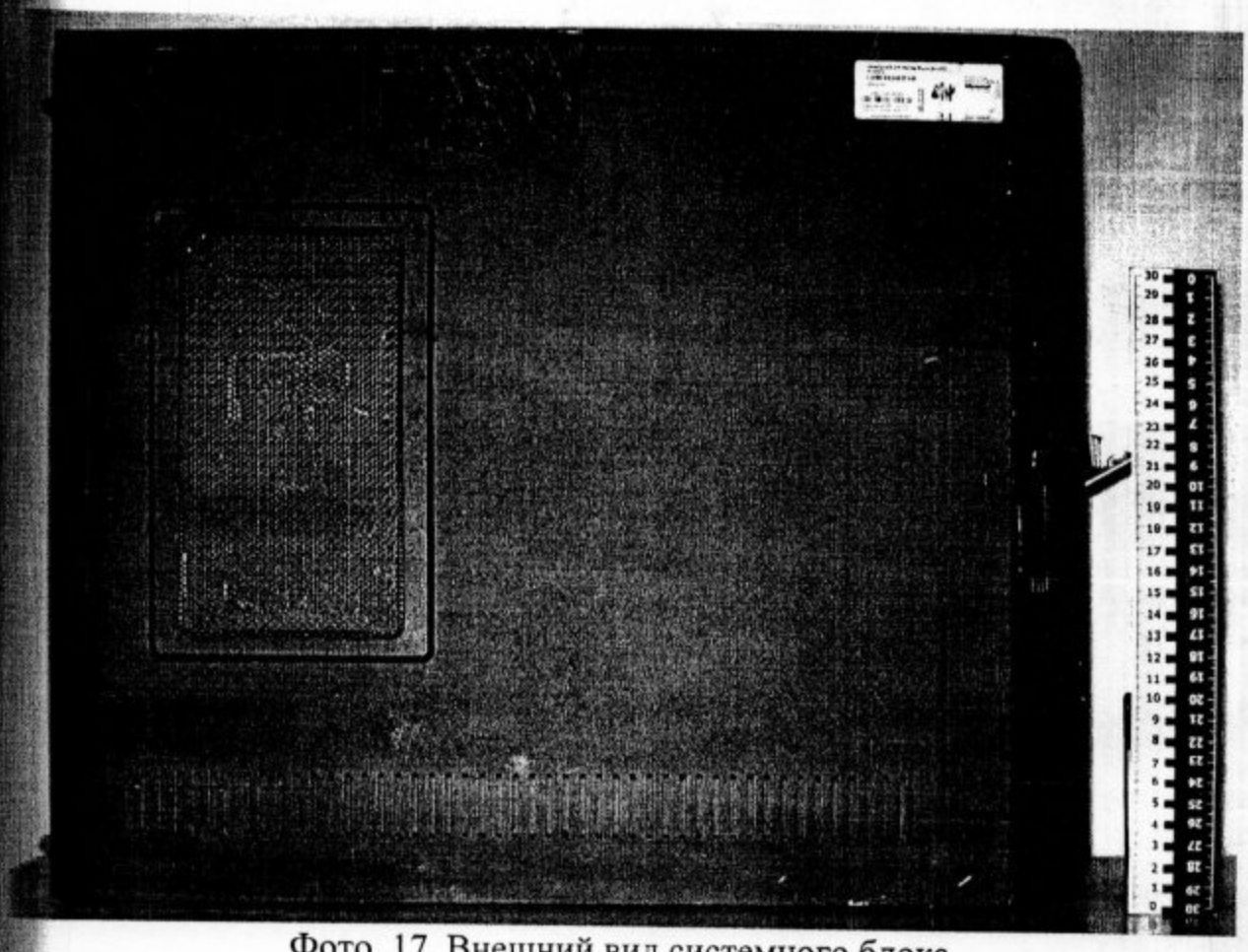

Фото. 17. Внешний вид системного блока

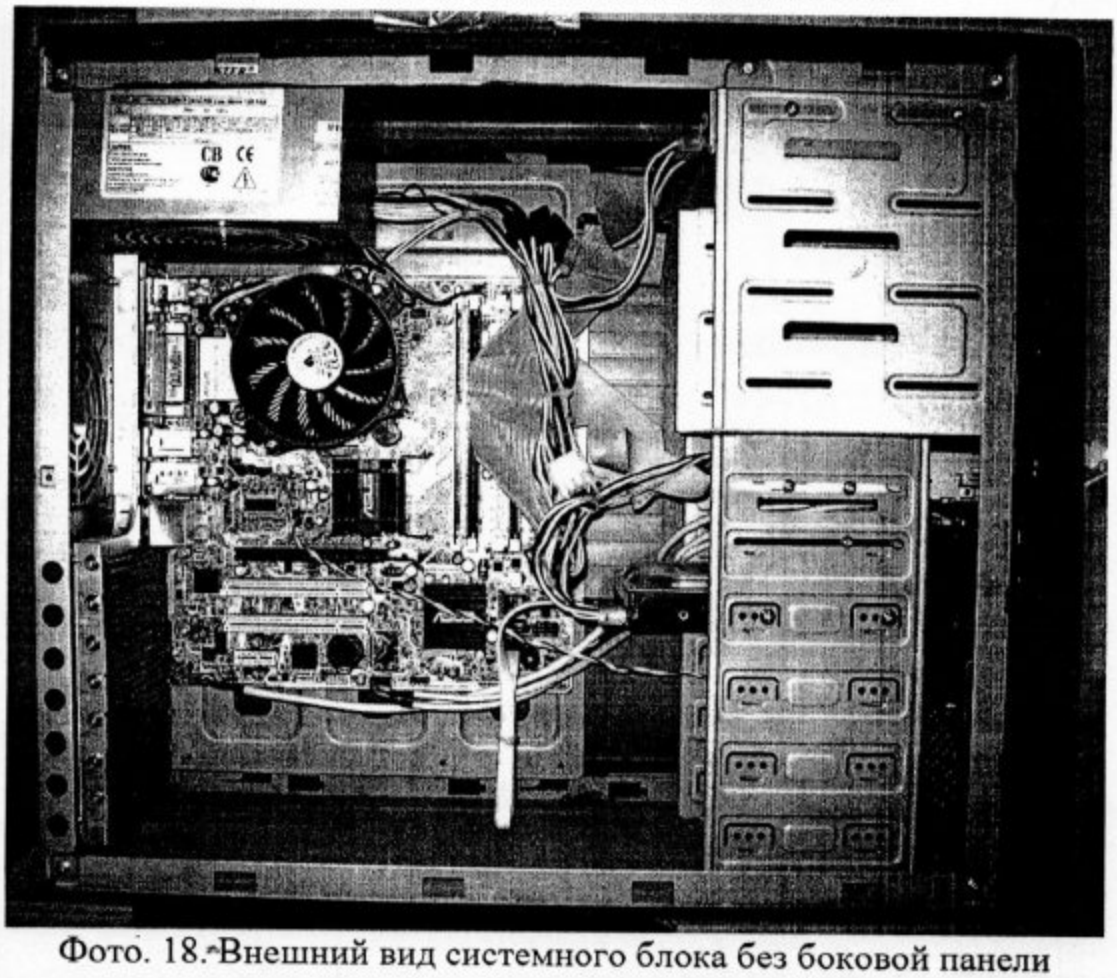

Фото. 18. Внешний вид системного блока без боковой панели

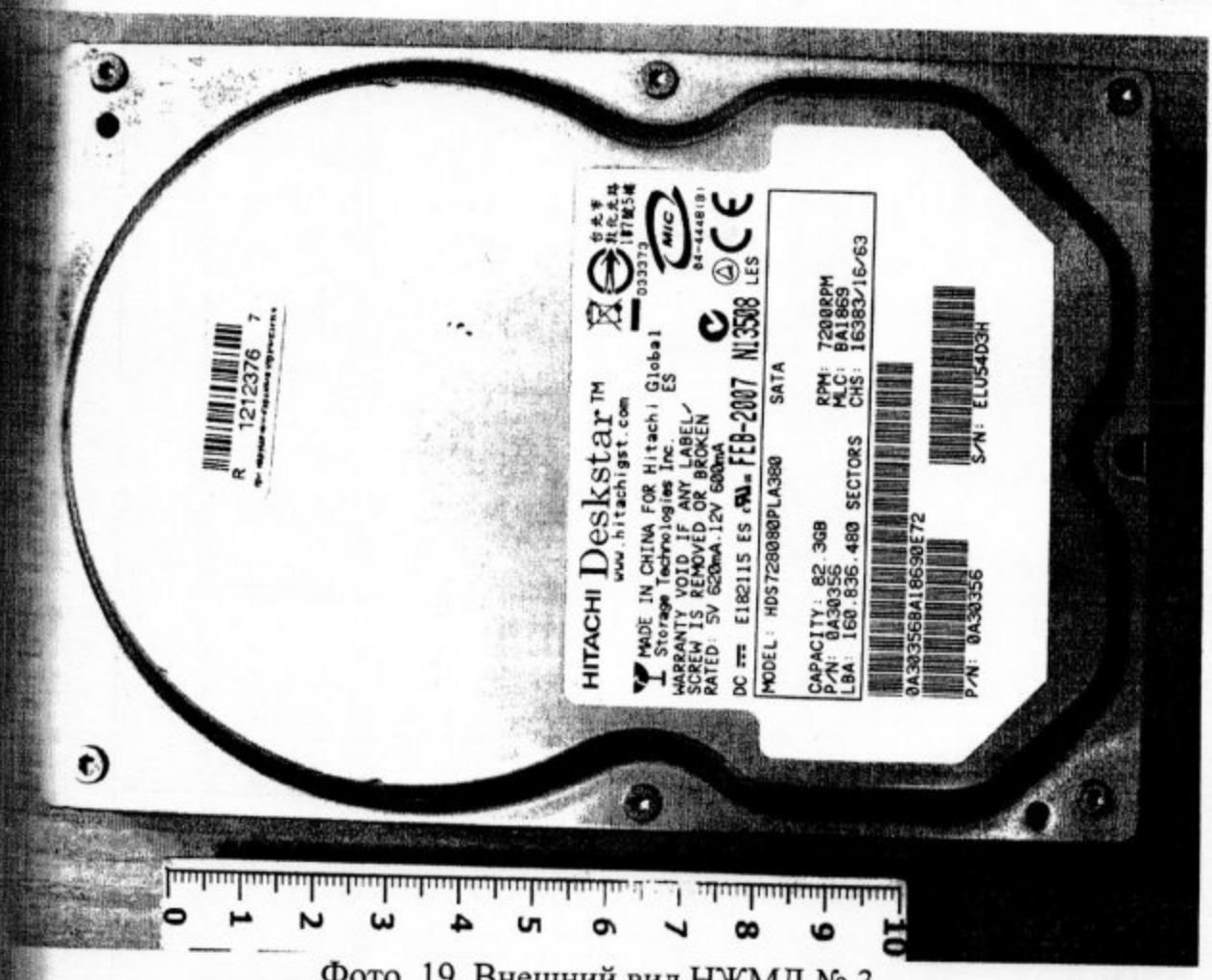

Фото. 19. Внешний вид НЖМД № 3

ЭКСПЕРТ Е.Г. Мкртчян