



АКТ ЭКСПЕРТНОГО ИССЛЕДОВАНИЯ

№10КЭ-17/А

от 17 октября 2017 г.

г. Нижний Новгород

Акт составлен на основании договора №10КЭ-17/А от 11.10.2017 года, заключенного с ИП Загуменнов Д.В.

Исследованием требуется установить:

«1. Исправны или нет представленные на экспертизу (исследование) объекты (накопители информации на жестких магнитных дисках (НЖМД))?»

2. Какие сведения о технических параметрах машинных носителей информации имеются в объектах, представленных на экспертизу?»

3. Экземпляры какого программного обеспечения, согласно зарегистрированных данных, имеются в памяти носителей информации (объектов), представленных на экспертизу?»

4. Имеются ли в памяти машинных носителей, представленных на экспертизу, экземпляры программ, предназначенных для организации и проведения азартных игр, с получением денежного выигрыша или проведения лотерей, в том числе с использованием информации телекоммуникационных сетей, сети интернет, а также средств связи, в том числе подвижной связи?»

5. Содержит ли программное обеспечение на представленных на экспертизу машинных носителях алгоритмы (процедуры, функции), определяющие результаты выигрыша случайным образом?»

6. Имеются ли в памяти машинных носителей, представленных на экспертизу (исследование), файлы, содержащие сведения статистического характера о вводе и выводе денежных средств?»

7. Имеются ли в памяти машинных носителей, представленных на экспертизу (исследование), зарегистрированные сведения о получении доступа к ресурсам в сети интернет и работы с ресурсами интернет-казино (ресурсов, осуществляющих игровой процесс с получением денежного выигрыша)?»

Производство исследования поручено эксперту АНО «Эксперт Союз» Костину Павлу Васильевичу, кандидату юридических наук (специальность 12.00.09 «Криминалистика, судебная экспертиза, оперативно-разыскная деятельность»), доценту, имеющему высшее образование по специальности «Радиосвязь» (квалификация радиоинженер), стаж практической работы с 1988 года, прошедшему переподготовку по программе судебных экспертов по компьютерно-технической экспертизе в Саратовском юридическом институте МВД России (специальность 21.1. «Исследование информационных компьютерных средств», свидетельство №717 от 31 мая 2004 года, свидетельство о праве самостоятельного производства компьютерно-технических экспертиз №00253 ГУ РФЦСЭ при Минюсте РФ), прошедшему обучение по программе повышения квалификации судебных экспертов по специальности 21.1. «Исследование информационных компьютерных средств» (свидетельства от 18 февраля 2010 г., 20 февраля 2013 г.,

Эксперт П.В. Костин



О 17 февраля 2016 г.), имеющему квалификацию судебного эксперта по специальности «Исследование информационных компьютерных средств» (сертификаты соответствия №000677 от 18 февраля 2010 г., №003701 от 20 февраля 2013 г., №007428 от 17 февраля 2016 г.), стаж работы по экспертной специальности с 2004 года.

В соответствии со статьями 41, 8, 16 Федерального закона №73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации», исходя из специальных знаний и компетенции эксперта по специальности 21.1. «Исследование информационных компьютерных средств», объектов, предоставленных для исследования, эксперт понимает поставленные перед ним вопросы следующим образом и рассматривает в следующем порядке:

Вопрос №1 «Исправны или нет представленные на экспертизу (исследование) объекты (накопители на жестких магнитных дисках (НЖМД))?» понимается экспертом следующим образом: «Исправны или не исправны машинные носители информации, представленные на экспертизу?».

Вопрос №2 «Какие сведения о технических параметрах машинных носителей информации имеются на объектах, представленных на экспертизу?» понимается экспертом следующим образом: «Установить марку, модель и основные технические параметры машинных носителей информации, представленных на экспертизу».

Вопрос №3 «Экземпляры какого программного обеспечения, согласно зарегистрированным данным, имеются в памяти носителей информации (объектов), представленных на экспертизу?» понимается экспертом следующим образом: «Экземпляры какого программного обеспечения воспроизведены в памяти машинных носителей информации, представленных на экспертизу?».

Вопрос №4 «Имеются ли в памяти машинных носителей, представленных на экспертизу, экземпляры программ, предназначенных для организации и проведения азартных игр, с получением денежного выигрыша или проведения лотерей, в том числе с использованием информационно-телекоммуникационных сетей, сети интернет, а также средств связи, в том числе подвижной связи?» понимается экспертом следующим образом: «Имеются ли среди программного обеспечения экземпляры программ, предназначенных для осуществления игрового процесса с получением денежного выигрыша (на основе случайного определения выигрыша) или проведения лотерей, в том числе с использованием информационно-телекоммуникационных компьютерных сетей?». Определение понятий «азартная игра» и «организация процесса» выходит за пределы компетенции эксперта.

Вопрос №5 «Содержит ли программное обеспечение на представленных на экспертизу машинных носителях алгоритмы (процедуры, функции), определяющие результаты выигрыша случайным образом?» по смыслу тождественен вопросу №4 в формулировке эксперта. Вопрос №4 и №5 объединяются и рассматриваются совместно как Вопрос №4.

Вопрос №6 «Имеются ли в памяти машинных носителей, представленных на экспертизу (исследование), файлы, содержащие сведения статистического характера о вводе и выводе денежных средств?» понимается экспертом следующим образом: «Имеются ли в памяти машинных носителей информации, представленных на экспертизу, сведения статистического характера о вводе и

Эксперт  П.В. Костин

4

выводе денежных средств (игровых единиц) при осуществлении игрового процесса посредством экземпляров программ, обнаруженных при решении Вопроса №4?»

Вопрос №7 «Имеются ли в памяти машинных носителей, представленных на экспертизу (исследование), зарегистрированные сведения о получении доступа к ресурсам в сети интернет и работы с ресурсами интернет-казино (ресурсов, осуществляющих игровой процесс с получением денежного выигрыша)?» в данной формулировке конкретен (не имеется указание о перечне ресурсов в сети интернет, в отношении которых необходимо проведение анализа) понимается экспертом следующим образом: «Имеются ли в памяти машинных носителей информации, представленных на экспертизу, сведения о получении доступа к ресурсам в сети интернет, в том числе к ресурсам интернет-казино (URL которых имеются в распоряжении эксперта)?»

ИССЛЕДОВАТЕЛЬСКАЯ ЧАСТЬ

Исследование проходило:

1. Экспертный осмотр и получение данных для исследования: по адресу г. Пермь, ул. Героев Хасана, д. 9А:

начало: 11.10.2017 года в 11 ч. 35 мин.

окончание: 11.10.2017 года в 13 ч. 15 мин.

2. Исследование полученных данных: в офисе ООО НПО «Эксперт Союз» д. 58 ул. Студеная, г. Н. Новгород:

начало: 12.10.2017 года в 09 ч. 00 мин.

окончание: 17.10.2017 года в 11 ч. 50 мин.

При производстве исследования использовались нормативно-правовые акты, специальная и методическая литература (список не полный):

1. Федеральный закон № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» от 31 мая 2007 г.
2. Федеральный закон №244-ФЗ от 29 декабря 2006 г. «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты российской федерации».
3. Федеральный закон Российской Федерации от 27 июля 2010 г. №214-ФЗ «О внесении изменений в Федеральный закон «О лотереях».
4. Федеральный закон от 28.12.2013 №416-ФЗ «О внесении изменений в Федеральный закон «О лотереях» и отдельные законодательные акты Российской Федерации».
5. ГОСТ Р 27.403-2009 «Надежность в технике» (термины по ГОСТ Р 27.002-89 «Надежность в технике. Термины и определения», Государственный стандарт Союза ССР, Москва, 1989).
6. 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 РФ, 2001.
7. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. — М., Право и закон, 2001.

Эксперт П.В. Костин



4

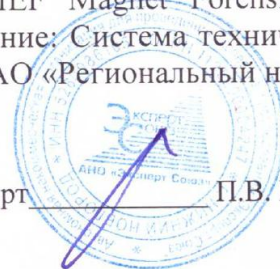
8. Нехорошев А.Б. Практические основы компьютерно-технической экспертизы: учебно-методическое пособие / А.Б. Нехорошев, М.Н. Шухнин, И.Ю. Юрин, А.Н. Яковлев. – Саратов: Научная книга, 2007.
9. Производство судебной компьютерно-технической экспертизы. Часть III. Специализированный словарь компьютерной лексики для экспертов компьютерно-технической экспертизы – М.: ГУ Российский федеральный центр судебной экспертизы. – 2009.
10. Усов А.И. Методы и средства решения компьютерно-технической экспертизы: Учебное пособие. – М.: ГУ ЭКЦ МВД России, 2002.
11. Усов А.И. Судебно-экспертное исследование компьютерных средств и систем: основы методического обеспечения: Учебное пособие. Под ред. проф. Е.Р. Россинской. – М.: Экзамен, Право и закон, 2003.
12. Рекомендация МИ 3017 – 2006 ФГУП «ВНИИМС» «Игровые автоматы с денежным выигрышем. Методы и порядок проведения экспертизы игровых программ с целью обнаружения в них не декларированных возможностей».
13. Рекомендация МИ 2662 – 2005 ФГУП «ВНИИМС» «Игровые автоматы с денежным выигрышем. Типовая методика контроля за соответствием утвержденному типу».

Для проведения исследования и подготовки заключения использовались:

- Мобильный персональный компьютер (ноутбук) ASUSK56CN с процессором Intel Core i5-1700, 8ГБ ОЗУ, оснащенный встроенным машинным носителем SSD TRANSCEND TS512GSSD3 512Гб. На стендовом компьютере установлены экземпляры системного и прикладного программного обеспечения: операционные системы Microsoft Windows 10 (тип лицензии OEM), Linux CAInE (версия 8.0 тип лицензии GPL), пакет офисных программ OpenOffice (версия 4.16, тип лицензии GPL), комплексная антивирусная утилита AVG Internet Security (версия 16.151.8013, тип лицензии «Полная версия», обновление антивирусных баз от 11.10.2017 г.), набор специализированного программного обеспечения (HDDScan, WinAudit, NirSoft, AutoSpy FB (v. 2.24-1)). Использовалось дополнительное оборудование: устройство Agestar AGE-5 V3CP (с аппаратным блокиратором записи), USB-flash накопитель Silicon-Partner 4GB с утилитой DeFacto (v. 1.98).

- Персональный компьютер ASUS на базе системной платы ASUS P9DWS с процессором Intel Core i5 4460 (3200 MHz), 32ГБ ОЗУ, оснащенный встроенным машинным носителем емкостью 2ТБ (Seagate ST2000DM001 SATAIII) и внешним накопителем емкостью 2 ТБ (WD MyBook 1132 USB Device). На стендовом компьютере установлены экземпляры системного и прикладного программного обеспечения: операционные системы Microsoft Windows 10 (тип лицензии OEM), Linux CAInE (версия 8.0 тип лицензии GPL), пакет офисных программ OpenOffice (версия 5.2.0, тип лицензии GPL), комплексная антивирусная утилита AVG Internet Security (версия 16.151.8013, тип лицензии «Полная версия», обновление антивирусных баз от 12.10.2017 г.), AVZ (версия 4.46, базы от 12.10.2017), набор специализированного программного обеспечения (утилита восстановления данных DMDE, комплекс EnCase, AutoSpy FB (v. 2.24-1), IEF` Magnet Forensics (v. 6.8.5.3985)). Использовалось дополнительное оборудование: Система технической экспертизы электронных модулей игровых автоматов (ЗАО «Региональный научно-исследовательский центр», г. Санкт Петербург).

Эксперт _____ П.В. Костин



4

Система технической экспертизы электронных модулей игровых автоматов (аппаратный модуль «Поиск-И» (15240218.465685.006 зав. №0907150062, дата выпуска 15.07.2009 г. и программное обеспечение изделия) входит в комплекс «Автоматизированное рабочее место проведения криминалистических экспертиз в сфере информационных технологий» (патент на изобретение №2297664 от 20 апреля 2007 г., сертификат соответствия №РОСС RU.МЛ03.В268 от 03 января 2007 года выдан ИЦ «Сертификационный испытательный центр» г. СПб, АРМ соответствия №15240218.465685.003).

В распоряжении эксперта имеются экземпляры эталонных программ разработки ООО «Игрософт» (г. Москва), предоставленные в инициативном порядке ООО «Медиа-НН» (официальным представителем ООО «Игрософт») для проведения экспертных исследований. В составе «Системы технической экспертизы электронных модулей игровых автоматов» имеются электронные платы с эталонными программами «Fruit Cocktail» и «Resident» разработки ООО «Игрософт» (г. Москва).

При проведении исследования использовались материалы и образцы, ранее полученные экспертами АНО «Эксперт Союз» при проведении аналогичных экспертиз и исследований.

Накопители на жестких магнитных дисках, установленные на стендовых компьютерах были проверены на наличие вредоносных (вирусных) программ – известных вредоносных программ не имеется.

При внешнем осмотре применялась фотосъемка с помощью цифрового фотоаппарата Canon Digital IXUS 70 с флэш-памяти Kingmax 16 GB (при изготовлении снимков предпринимались специальные меры контроля, и полученное изображение не искажено и точно отражает реальные объекты, для обработки изображений использовались встроенные функции экземпляра операционной системы и офисного пакета).

Эксперт принимает следующий план исследования:

1. Внешний осмотр объектов, представленных на исследование.
2. Получение доступа к машинным носителям информации.
3. Определение исправности и работоспособности машинных носителей.
4. Исследование машинных носителей:
 - определение технических параметров;
 - определение установленного программного обеспечения;
 - анализ ПО и параметров его функционирования;
 - определение сведений о работе в сети интернет.

При проведении исследования использовались следующие определения (см. ГОСТ 27.002-89 «Надежность в технике. Термины и определения»):

Исправное состояние (исправность, Good state) – состояние изделия, при котором оно соответствует всем требованиям нормативной технической и (или) конструкторской документации.

Работоспособное состояние (работоспособность, Up state) – состояние изделия, при котором в данный момент времени его основные параметры находятся в пределах, установленных требованиями нормативно-технической документации.

Эксперт _____ П.В. Костин



4

1. Внешний осмотр объектов

Для исследования предоставлены объекты:

1. 6 (шесть) однотипных системных блоков (далее СБ1-6) нестандартного форм-фактора в корпусах черного цвета со встроенной клавиатурой на 12 клавиш (образец см. Фото №1, 2). На передних стенках корпусов СБ имеются маркировочные обозначения (порядковые номера), на задних стенках - инвентарные номера (см. Таблица №1).

Таблица №1

№ п/п	Условный номер	Имеющиеся обозначения	
		Порядковый номер	Инвентарный номер
1	2	3	4
1.	СБ1	5 (Г.5)	0049/4
2.	СБ2	Г8	-
3.	СБ3	Г.10	0051/4
4.	СБ4	Г.11	0053/4
5.	СБ5	Г.12	0057/4
6.	СБ6	Г.13	0052/4

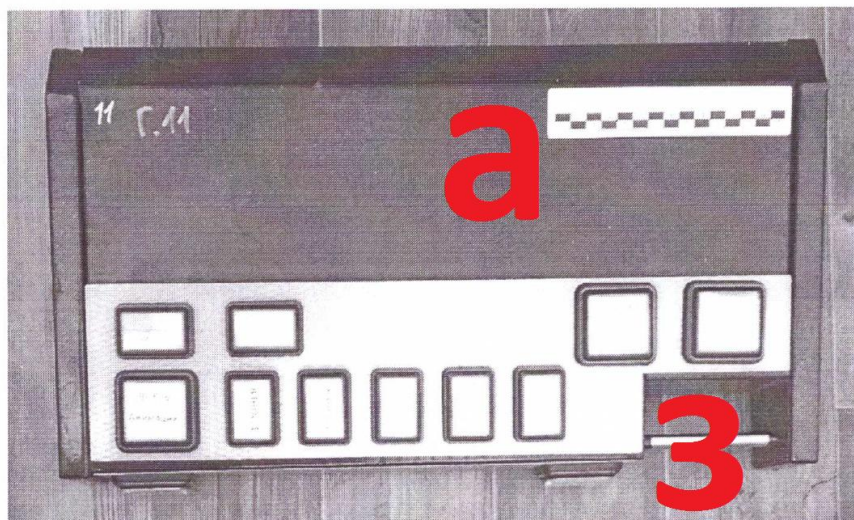


Фото №1

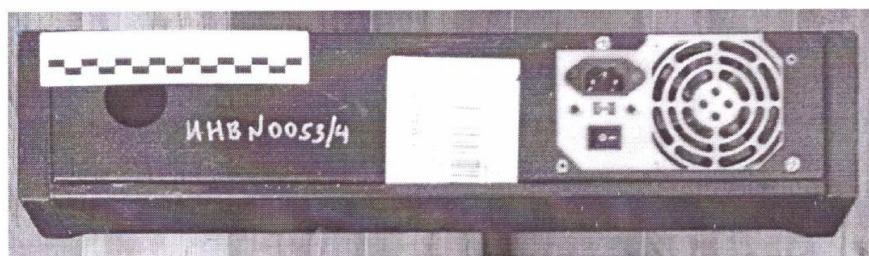


Фото №2

Внутри СБ1-6 обнаружены машинные носители информации (см. Фото №3), из них:

- в СБ1, 3, 4, 5, 6 - накопители на жестких магнитных дисках (далее НЖМД1, 3, 4, 5, 6, см. Фото №4, 6-9);
- в СБ2 - твердотельный накопитель (далее ТД2, см. Фото №5).

Эксперт _____ П.В. Костин



4

О

Для упрощения идентификации исследуемые машинные носители были пронумерованы экспертом с нанесением условного номера (5, 8, 10, 11, 12, 13 в соответствии с порядковыми номерами СБ, из которых НЖМД были изъяты) маркером черного цвета на лицевые поверхности НЖМД (имеющиеся идентификационные обозначения не затронуты). Сведения об исследуемых машинных носителях (получены анализом имеющихся идентификационных обозначений и использованием специализированного программного обеспечения) приведены в Таблице №2.

Б

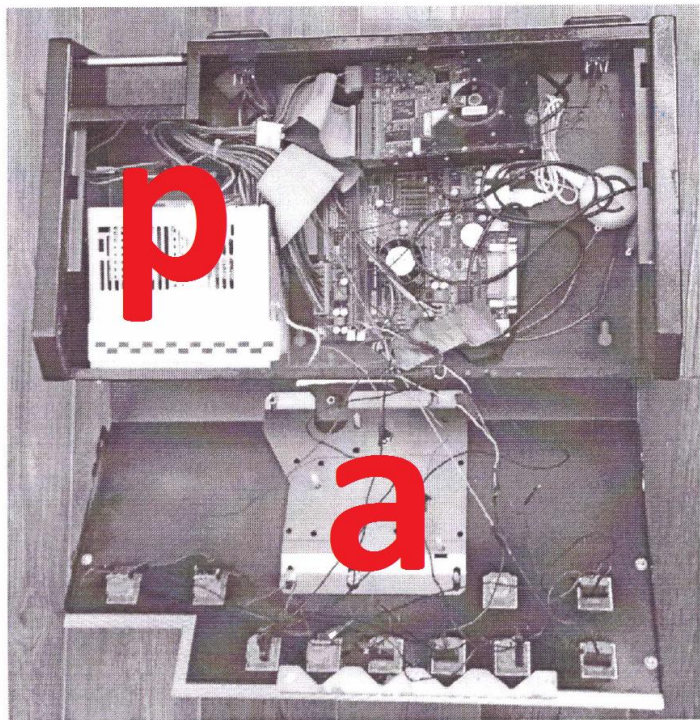


Фото №3

З

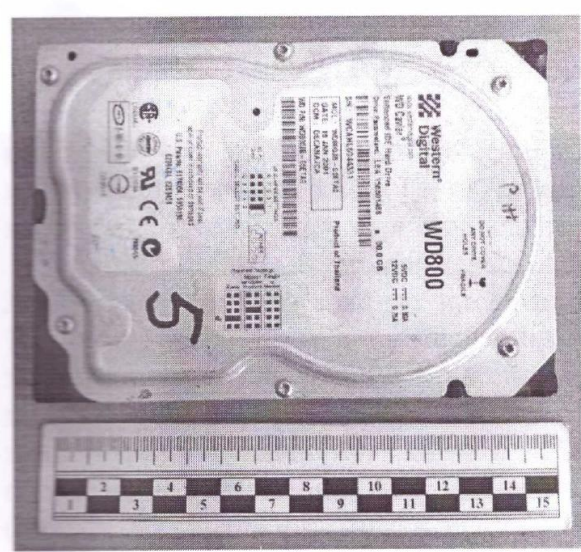


Фото №4

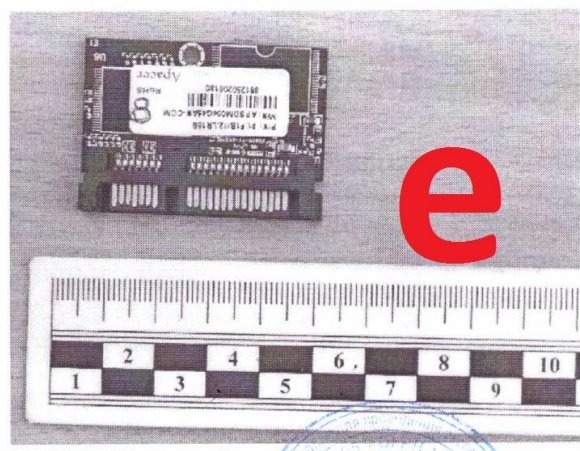


Фото №5

Ч

Эксперт _____ П.В. Костин



О



Фото №6

Б

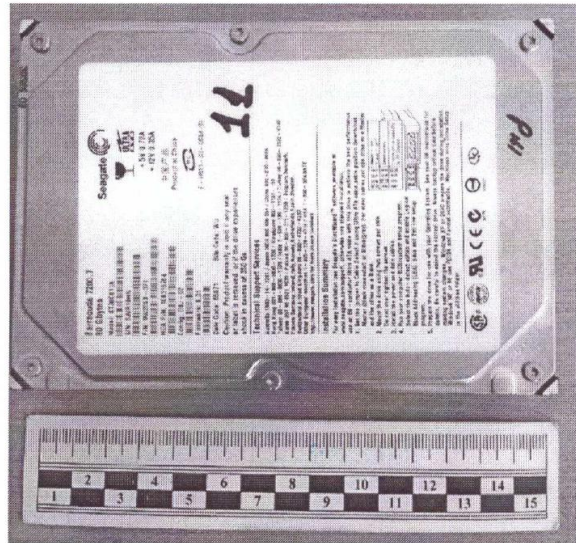


Фото №7

Р



Фото №8

А

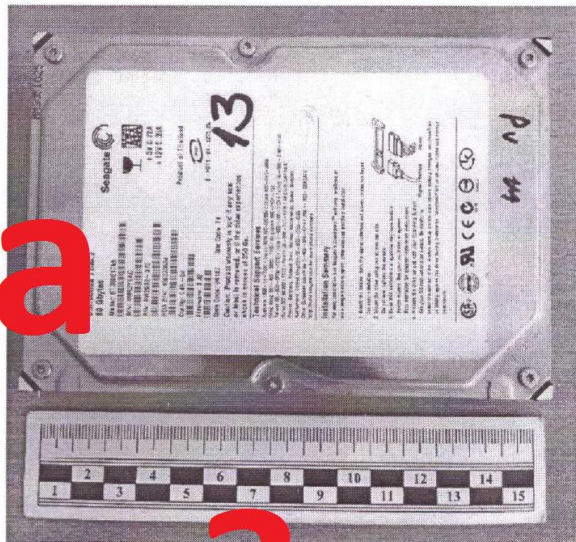


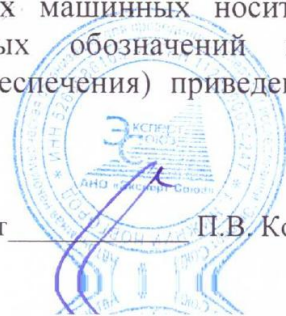
Фото №9

З

2. 2 (два) однотипных системных блока (далее СБ7, 8) нестандартного форм-фактора в корпусах оранжевого/зеленого цвета со встроенной клавиатурой на 12 клавиш (см. Фото №10, 11, 12). На задних стенках корпусов СБ имеются маркировочные обозначения (порядковые номера 16, 17).

Внутри СБ7, 8 обнаружены машинные носители информации (см. Фото №13)- накопители на жестких магнитных дисках (далее НЖМД7, 8, см. Фото №14, 15). Для упрощения идентификации исследуемые машинные носители были пронумерованы экспертом с нанесением условного номера (16, 17 в соответствии с порядковыми номерами СБ, из которых НЖМД были изъяты) маркером черного цвета на лицевые поверхности НЖМД (имеющиеся идентификационные обозначения не затронуты). Сведения об исследуемых машинных носителях (получены анализом имеющихся идентификационных обозначений и с использованием специализированного программного обеспечения) приведены в Таблице №2.

Е



Эксперт П.В. Костин

Ц

О



Фото №10

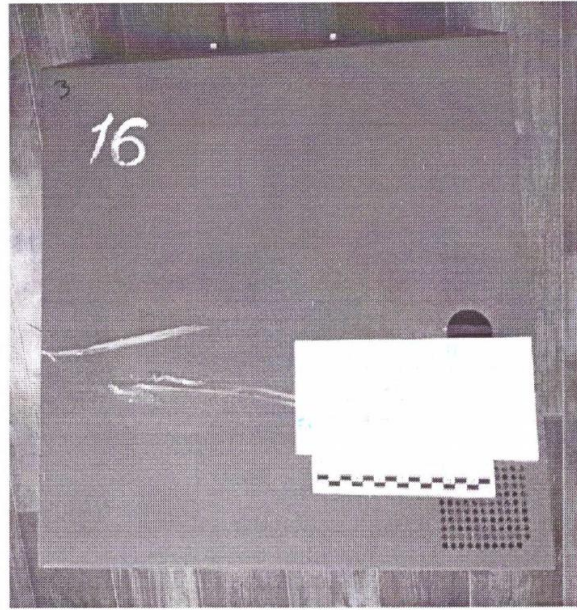


Фото №11

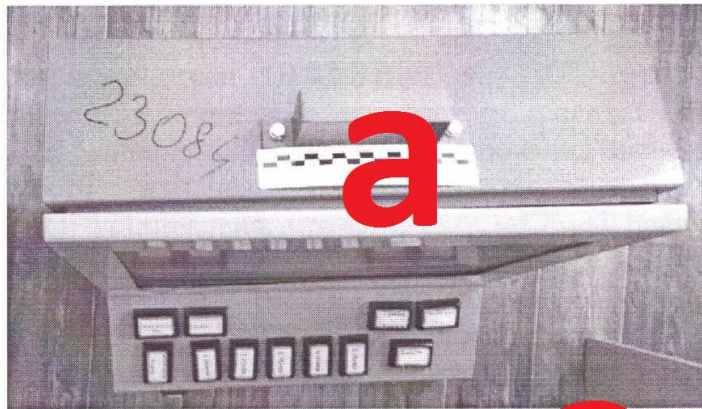


Фото №12

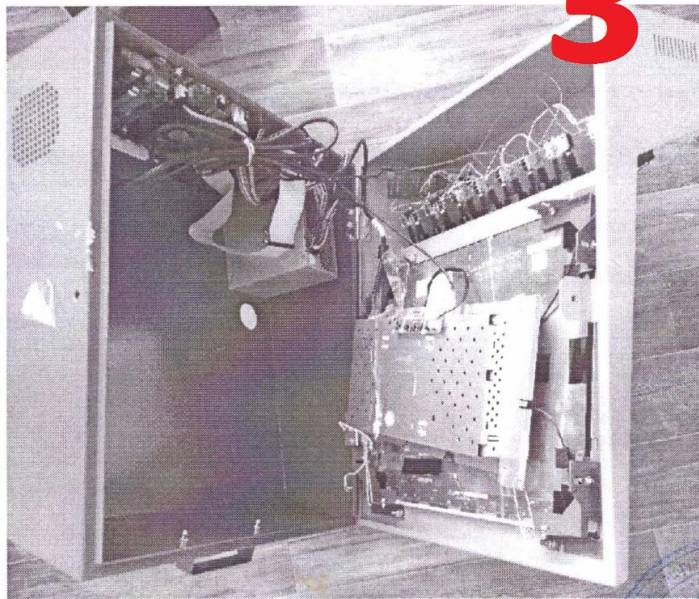


Фото №13

е

ц

Эксперт П.В. Костин



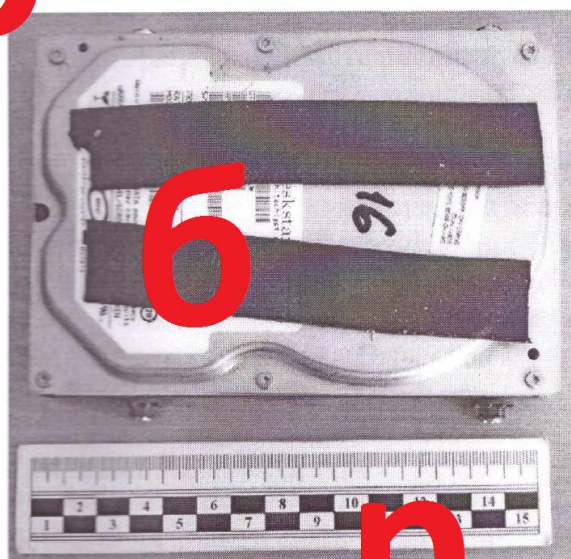


Фото №14

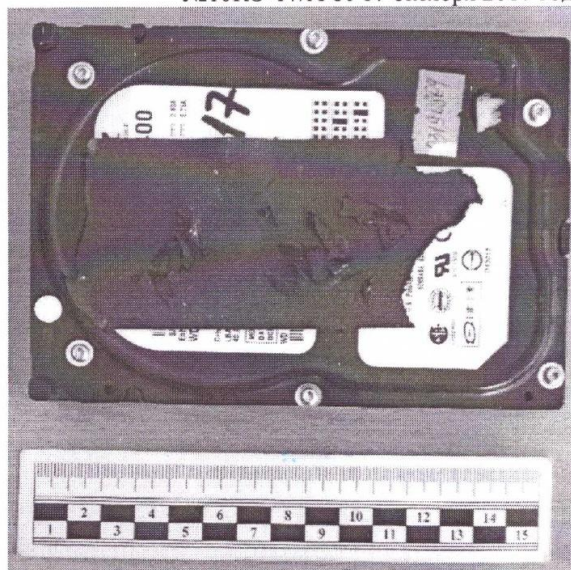


Фото №15

2. Определение исправности

Исследуемые накопители (НЖМД1, 3-8, ТД2) были последовательно поочередно подключены к стендовому компьютеру с использованием устройства Agestar AGE 3FBCP (аппаратное средство фиксации записи для исключения несанкционированного изменения содержания исследуемых машинных носителей). При этом установлено, что НЖМД1, 3-8, ТД2 правильно опознаются экземпляром операционной системы, воспроизведенной на НЖМД стендового компьютера, доступ к файловым системам исследуемых накопителей возможен в полном объеме. НЖМД1, 3-8, ТД2 исправны. С использованием специализированного программного обеспечения HDDScan получены сведения об основных технических параметрах исследуемых машинных носителей (см. Таблица №2).

Таблица №2

№ п/п	Условный номер	Порядковый номер	Параметры				
			Производитель	Модель	Серийный номер	Емкость (ГБ)	Интерфейс
1	2	3	4	5	6	7	8
1.	НЖМД1	5	WDC	WD800	WCAML6044331	80	SATA
2.	ТД2	8	Apacer	SFDDA01C	C011201111090000373	4	SATA
3.	НЖМД3	10	WDC	WD800JD	WMAM9DPM8832	80	SATA
4.	НЖМД4	11	Seagate	ST380011A	5JR19HN	80	SATA
5.	НЖМД5	12	WDC	WD800JD	WMAM9AEL9968	80	SATA
6.	НЖМД6	13	Seagate	ST380817AS	4MR3YEAD	80	SATA
7.	НЖМД7	16	Hitachi	HDS721680PLA380	PVFB04ZLRB98WE	80	SATA
8.	НЖМД8	17	WDC	WD400BB	WMAJC1260514	40	IDE

3. Исследование машинных носителей

Исследование проводилось методом анализа файловых систем, воспроизведенных на исследуемых машинных носителях, анализа файлов экземпляров операционной системы (ОС) и протоколов работы программного обеспечения с использованием специализированного программного обеспечения и встроенных средств экземпляров операционных систем Microsoft Windows 10 (с

Эксперт _____ П.В. Костин

драйвером Ext2FS) и Linux CAInE 8.0, воспроизведенных на НЖМД стенового компьютера. В результате анализа установлено:

На исследуемых машинных носителях воспроизведены экземпляры программного обеспечения:

- НЖМД1, НЖМД3, НЖМД4, НЖМД5, НЖМД6 - содержат тождественные наборы экземпляров программного обеспечения: экземпляр операционной системы *Microsoft Windows XP Professional Russian* (дата установки: 11.01.2016 г. со следующими учетными данными: владелец: «888», ключ продукта: VNHWK-69Y6M-WM8YD-MB8TR-K86FB); экземпляры прикладного программного обеспечения: *HashTab, DriverPack Solution, Intel Processor Graphics, Microsoft Windows Internet Explorer*.

- ТД2, НЖМД7, НЖМД8 - содержат тождественные наборы экземпляров программного обеспечения: экземпляр операционной системы *Microsoft Windows XP Professional Russian* (дата установки: ТД2 - 29.10.2015 г., НЖМД7 - 11.01.2016 г., НЖМД8 - 11.01.2016 г. со следующими учетными данными: владелец: «888», ключ продукта: VNHWK-69Y6M-WM8YD-MB8TR-K86FB); экземпляры прикладного программного обеспечения: *HashTab, Intel Processor Graphics, Microsoft Windows Internet Explorer*.

На исследуемых НЖМД1, 3-8, ТД2 сведений о воспроизведении экземпляров программного обеспечения игрового назначения, в том числе тождественного эталонным игровым программам правообладателей «Игрософт», «Novomatic AG» и иных, имеющих в распоряжении эксперта, не обнаружено. На исследуемых машинных носителях сведений о воспроизведении экземпляров программного обеспечения, позиционируемых как «лотерея» не имеется.

На исследуемых НЖМД1, 3-8, ТД2 зарегистрировано воспроизведение экземпляров программного обеспечения, сведения о которых не зафиксированы в реестре экземпляров ОС (см. Таблица №3).

Таблица №3

№ п/п	Машинный носитель		Наименование	Размещение	Исполнимый файл	Версия	Дата воспроизведения
1	Условный номер	Порядковый номер	4	5	6	7	8
1.	НЖМД1	5	Dominator	C:\games_full\	game.exe	3.75.0.105	27.06.2016
2.	ТД2	8	Dominator	C:\games_full\	game.exe	3.75.0.105	27.06.2016
3.	НЖМД3	10	Dominator	C:\games_full\	game.exe	3.75.0.105	27.06.2016
4.	НЖМД4	11	Dominator	C:\games_full\	game.exe	3.75.0.105	27.06.2016
5.	НЖМД5	12	Dominator	C:\games_full\	game.exe	3.75.0.105	27.06.2016
6.	НЖМД6	13	Dominator	C:\games_full\	game.exe	3.75.0.105	27.06.2016
7.	НЖМД7	16	Dominator	C:\games_full\	game.exe	3.75.0.105	11.06.2016
8.	НЖМД8	17	Dominator	C:\games_full\	game.exe	3.75.0.105	06.02.2016

Временные метки указаны в соответствии с зарегистрированными значениями (по системной дате/времени устройства, на котором осуществлялась обработка).

4. Определение работы в сети интернет

При анализе настроек сетевых соединений установлено, что в реестрах экземпляров ОС, воспроизведенных на исследуемых НЖМД, зарегистрированы сведения о подключениях по локальной сети (см Таблица №4).

Эксперт  П.В. Костин

№ п/п	Машинный носитель	Наименование подключения	Адаптер	IP-адрес	Сервер	Шлюз	Маска подсети
1		2	3	4	5	6	7
1.	НЖМД1	Подключение по локальной сети 4	Realtek PCIe GBE Family Controller	192.168.1.108	192.168.1.1	192.168.1.1	255.255.255.0
2.	ТД2	Подключение по локальной сети 2	Realtek PCIe GBE Family Controller	192.168.1.10	192.168.1.1	192.168.1.1	255.255.255.0
3.	НЖМД3	Подключение по локальной сети 4	Realtek PCIe GBE Family Controller	192.168.1.105	192.168.1.1	192.168.1.1	255.255.255.0
4.	НЖМД4	Подключение по локальной сети 4	Realtek PCIe GBE Family Controller	192.168.1.109	192.168.1.1	192.168.1.1	255.255.255.0
5.	НЖМД5	Подключение по локальной сети 4	Realtek PCIe GBE Family Controller	192.168.1.104	192.168.1.1	192.168.1.1	255.255.255.0
6.	НЖМД6	Подключение по локальной сети 4	Realtek PCIe GBE Family Controller	192.168.1.103	192.168.1.1	192.168.1.1	255.255.255.0
7.	НЖМД7	Подключение по локальной сети 4	Realtek PCIe GBE Family Controller	192.168.1.107	192.168.1.1	192.168.1.1	255.255.255.0
8.	НЖМД8	Подключение по локальной сети 4	Realtek PCIe GBE Family Controller	192.168.1.106	192.168.1.1	192.168.1.1	255.255.255.0

Для определения целей работы в сети интернет и перечня посещенных интернет-ресурсов на исследуемых НЖМД1, 3-8, ТД2 были проанализированы протоколы работы (история) и КЭШи установленных интернет-браузеров. В результате анализа установлено, что в памяти исследуемых НЖМД1, 3-8, ТД2 сведений об осуществлении доступа к ресурсам в сети интернет (в том числе к ресурсам известных игровых ресурсов (интернет-казино *Lucky Golden Dragon Casino, Novotech, NUMBER 1 Casino, Yoo Ya Casino, Atlantida, Казино Chicago, Platinum Games, Superomatic, GlobalSlot, SunLight Casino* и иных, а также аффилированных платежных систем, предоставляющих возможность осуществления игрового процесса с получением денежного выигрыша) с использованием экземпляров веб-браузеров не имеется.

5. Анализ программного обеспечения *Dominator*

Исследование программного обеспечения производилось на стендовом компьютере эксперта в виртуальной среде *Hyper-V* с эмуляцией работы операционной системы *MS Windows XP* с подключением к сети интернет. В результате проведенного исследования установлено:

Согласно настроек, зарегистрированных в файле «*.\game.ini*», при запуске ПО осуществляет обращение к ресурсу в сети интернет с URL «*http://relay.dyndns.org/relay/*». При старте программное обеспечение осуществляет процедуру обновления (IP-адрес сервера обновлений *52.31.111.206*) в процессе работы обращается к ресурсу с IP-адресом *148.251.166.211* (URL *http://relay.dyndns.org/*) используя в качестве параметров идентификации логин «*dominator*». С использованием сервиса *Whois* установлены сведения о принадлежности IP-адресов:

- *148.251.166.211* (URL *http://relay.dyndns.org/*): принадлежит пулу сети адресов сети HETZNER-RZ-BLK-ERX2 (Hetzner Online GmbH, Industriestrasse 25, D-91710 Gunzenhausen, Germany);

- *52.31.111.206* (URL *ec2-52-31-111-206.eu-west-1.compute.amazonaws.com*): принадлежит пулу сети адресов сети AT-88-Z (Amazon Technologies Inc, 410 Terry Ave N., Seattle, USA - Washington).

Эксперт  П.В. Костин

Ресурс в сети интернет с URL «*dyndns.org*» представляет собой сервис, который позволяет пользователям получить личный адрес, который будет привязан к пользовательскому компьютеру, не имеющему постоянного IP-адреса. Ресурс в сети интернет с URL «*amazonaws.com*» предоставляет услуги файлового хостинга.

Таким образом, экземпляр программного обеспечения «*Dominator*», является терминальным клиентом, работающим под управлением программного обеспечения сервера (ресурс в сети интернет с URL «*http://relay.dyndns.org/*») с получением обновлений с сервера файлового хостинга (52.31.111.206).

Программное обеспечение «*Dominator*» не функционирует без связи с внешним сервером (см. Иллюстрация №1). Основная управляющая программа размещена на внешнем сервере. Конфигурационные файлы экземпляров программного обеспечения (*game.ini*) содержат сведения об аутентификационных данных (см. Таблица №5).

Таблица №5

№ п/п	Условный номер	Порядковый номер	Условный MAC-адрес (ForceMac)
1	2	3	3
1.	НЖМД1	5	din05
2.	ТД2	8	dr08
3.	НЖМД3	10	din10
4.	НЖМД4	11	din11
5.	НЖМД5	12	din12
6.	НЖМД6	13	din13
7.	НЖМД7	16	lar03
8.	НЖМД8	17	lar02

На момент проведения исследования экземпляры программного обеспечения «*Dominator*» с имеющимися идентификационными данными авторизацию на внешнем сервере не осуществляют (см. Иллюстрация №2). Проведение полного анализа функционирования программного обеспечения «*Dominator*» не представляется возможным по причине не возможности авторизации на внешнем сервере исследуемых экземпляров программы.



Иллюстрация №1



Иллюстрация №2

Согласно данным, предоставляемых ресурсом в сети интернет URL «*http://dminator.ru/*», «автоматизированный программный комплекс для приёма и выдачи благотворительных пожертвований для залов и терминалов "DOMINATOR"» (Иллюстрация №3). Примеры графического интерфейса программы см. Иллюстрация №4-8 (по материалам «*http://dminator.ru/*»).



Эксперт П.В. Костин

о



Иллюстрация №3

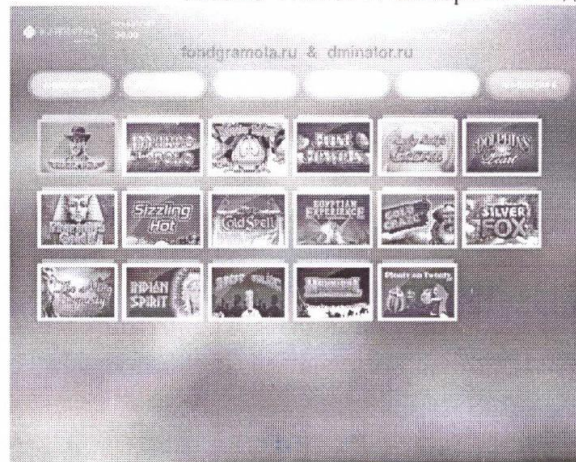


Иллюстрация №4



Иллюстрация №5



Иллюстрация №6

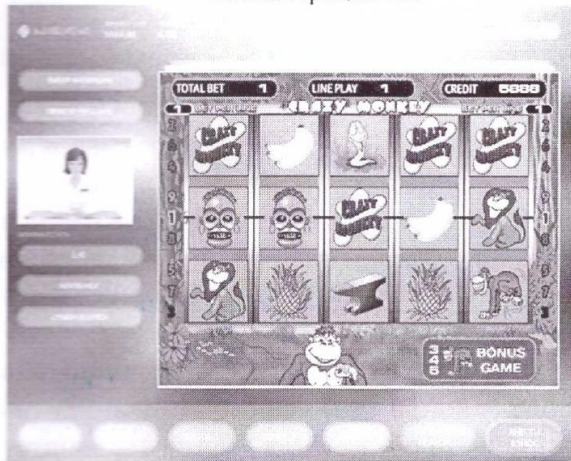


Иллюстрация №7



Иллюстрация №8

Интерфейс программы предполагает отображение данных в двух режимах: *Режим 1* - представлен в виде анимированного изображения, пример см. Иллюстрация №8) и *Режим 2* - режим мультипликационной визуализации («анимации», пример см. Иллюстрация №7). Мультипликации «Режима 2», частично тождественны по генерируемым изображениям с эталонными игровыми программами, имеющимися в распоряжении эксперта.



Эксперт _____ П.В. Костин

ц

Проведение полнофункционального сравнения изображений выходит за пределы формальной компетенции эксперта.

Вместе с тем, эксперт отмечает, что игровые программы правообладателей «Novomatic AG» и «Игрософт» разработаны для функционирования на специализированных платформах (электронных модулях игровых автоматов «CoolFire II» компании «Novomatic AG»); «Игрософт. Тип 1» и «IGP II» (компания «Игрософт»). Программное обеспечение «Dominator» функционирует на универсальной платформе с архитектурой x86 и работает под управлением операционной системы Windows. Таким образом, ПО «Dominator» и ПО правообладателей «Novomatic AG» и «Игрософт» являются различными программами для ЭВМ.

Для проверки наличия внутренних функций (в том числе функций, определяющих результат игры и процент выигрыша пользователя, а также порядок формирования анимированных визуализаций) осуществлено декомпилирование основного исполнимого файла пакета («game.exe») с использованием интерактивного дисассемблера IDA (версия 6.0, <https://www.hex-rays.com/>) с последующим анализом.

При проведении процедуры декомпиляции основного исполнимого файла пакета установлено:

- декомпиляция файла производится успешно;
- язык разработки ПО – Visual C++ v6;
- программное обеспечение не содержит узлов, функций и алгоритмов, не доступных для исследования;
- в декомпилированном коде исполнимого файла пакета («game.exe») процедур, формирующих результат игры и процент выигрыша пользователя, не обнаружено;
- код программы содержит функции случайных чисел (*rand()*, *srand()*), которые используются при формировании интерфейсной части.

Анализируя полученные данные, эксперт приходит к промежуточным выводам:

1. Программное обеспечение «Dominator», является терминальным клиентом, работающим под управлением программного обеспечения сервера (ресурс в сети интернет с URL «<http://relay.dyndns.org/>», IP адрес «148.251.166.211»).

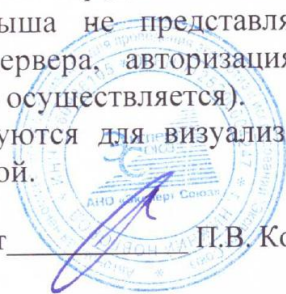
2. Исполнимый файл (*game.exe*) экземпляра программного обеспечения «Dominator», функций (алгоритмов), определяющих результаты выигрыша случайным образом (на основе работы генератора случайных чисел) либо устанавливающих какой-либо процент выигрыша, не содержит.

3. Сведений о возможном использовании программного обеспечения «Dominator» для проведения игрового процесса с материальным (денежным) выигрышем, который определяется случайным образом, не выявлено.

4. Анализ основной управляющей программы в целях определения наличия (отсутствия) функции случайного определения выигрыша не представляется возможным (воспроизведена на ресурсах внешнего сервера, авторизация на внешнем сервере исследуемых экземпляров программы не осуществляется).

5. Графические изображения (анимации) используются для визуализации процесса, реализуемого основной управляющей программой.

Эксперт _____ П.В. Костин



4

6. ПО «*Dominator*» и игровые программы правообладателей «Novomatic AG» и «Игрософт» являются различными программами для ЭВМ.

Анализ вероятных статистических данных

Программное обеспечение «*Dominator*» ведет протокол работы методом генерации лог-файлов (формат файла - «*txt*», название - (пример) «*20160221*» (дата, за которую ведется протокол работы)). Протоколы сохраняются в каталоге «*..logs*».

При анализе файлов, содержащих протоколы работы экземпляров программного обеспечения «*Dominator*», воспроизведенных на исследуемых НЖМД1, 3-8, ТД2, установлено:

- экземпляры программного обеспечения функционировали в период:

НЖМД1 - 05.06.2016 - 11.11.2016;

ТД2 - 27.06.2016 - 11.11.2016;

НЖМД3 - 27.06.2016 - 12.11.2016;

НЖМД4 - 27.06.2016 - 02.11.2016;

НЖМД5 - 27.06.2016 - 27.11.2016;

НЖМД6 - 27.06.2016 - 27.11.2016;

НЖМД7 - 11.06.2016 - 19.07.2016;

НЖМД8 - 06.02.2016 - 19.07.2016;

- клиенты системы «*Dominator*» работали не в режиме терминала (купюроприемник не задействован);

- сведения о количестве внесенных в данные средства не фиксировались.

Совокупность полученных результатов позволяет эксперту говорить о следующем:

ВЫВОДЫ

1. (ответ на Вопрос №1). Машинные носители информации, представленные на экспертизу, исправны.

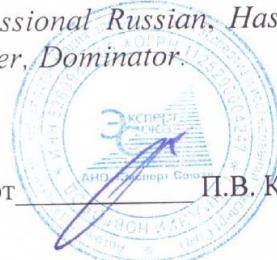
2. (ответ на Вопрос №2). Сведения о технических параметрах машинных носителей, представленных на экспертизу, приведены в Таблице №2 исследовательской части заключения.

3. (ответ на Вопрос №3). В памяти машинных носителей, представленных на экспертизу, согласно зарегистрированных данных воспроизведены экземпляры программного обеспечения:

- НЖМД1, НЖМД3, НЖМД4, НЖМД5, НЖМД6 - содержат тождественные наборы экземпляров программного обеспечения: *Microsoft Windows XP Professional Russian, HashTab, DriverPack Solution, Intel Processor Graphics, Microsoft Windows Internet Explorer, Dominator*.

- ТД2, НЖМД7, НЖМД8 - содержат тождественные наборы экземпляров программного обеспечения: *Microsoft Windows XP Professional Russian, HashTab, Intel Processor Graphics, Microsoft Windows Internet Explorer, Dominator*.

Эксперт _____ П.В. Костин



4, 5. (ответ на Вопрос №4, №5). В памяти машинных носителей информации, представленных на экспертизу, экземпляров программ, предназначенных для осуществления игрового процесса с получением денежного выигрыша (на основе случайного определения выигрыша), в том числе с использованием информационно-телекоммуникационных компьютерных сетей не имеется. В исследуемых машинных носителях сведений о воспроизведении экземпляров программного обеспечения, позиционируемых как «лотерейное» не имеется.

6. (ответ на Вопрос №6). В памяти машинных носителей информации, представленных на экспертизу, сведений статистического характера о вводе и выводе денежных средств (игровых единиц) не имеется.

7. (ответ на Вопрос №7). В памяти машинных носителей, представленных на экспертизу, сведений о получении доступа к ресурсам в сети интернет (в том числе к ресурсам известных интернет-казино (*Lucky Golden Dragon Casino, Novotech, NUMBER 1 Casino, Ya888Ya Casino, Atlantida, Казино Chicago, Platinum Games, Superomatic, Globalslots, SunLight Casino* и иных), а также аффилированных платежных систем, предоставляющих возможность осуществления игрового процесса с получением денежного выигрыша), не имеется.

Эксперт



П.В. Костин

З

е

Ц

аттестат является документом
государственного образца

серия ДЦ № 018661

Москва

Федеральной службы по надзору
в сфере образования и науки

от 16 июля 2008 г. № 1637/2008-г

Космину Тавлу Васильевну

ПРИСВОЕНО УЧЕНОЕ ЗВАНИЕ

ДОЦЕНТА

управления и цифровых технологий



Л.Н.Глебова

Руководитель

Российская Федерация



ДИПЛОМ ЯВЛЯЕТСЯ ДОКУМЕНТОМ
ГОСУДАРСТВЕННОГО ОБРАЗЦА

Решение
Высшей аттестационной комиссии
Министерства образования и науки
Российской Федерации
о выдаче диплома

от 15 апреля 2007 г. № 266/43

Серия ДКН № 030530 *

г. МОСКВА

Решением
диссертационного совета

Нижегородской государственной академии МВД России

от 5 апреля 2007 г. № 17

Костину Павлу Васильевичу

ПРИСУЖДЕНА УЧЕНАЯ СТЕПЕНЬ

КАНДИДАТА

юридических наук

Председатель
диссертационного совета



е

д

з

а

р

б

о

ДИПЛОМ

№В М 747780

Настоящий диплом выдан *Сосиски*

в том, что он *Сосиски* поступил
в *Лавку* в *Алтай* *Республике*
в *Великом* *Усть-Каменогорске*
Жандарма *Восточной*
и в *1988* *г.*
по *Службе*



Решением Государственной экзаменационной
комиссии от *21* *июня* *1988* г.

Розина Г.В.
Филиция *Розинская*



Московская типография Голака, 1985.

МАТРИЧНЫЙ
ЗНАК ВЫДАН



о

б

р

а

з

е

ц

О

Б



СЕРТИФИКАТ.RU
СИСТЕМА ДОБРОВОЛЬНОЙ
СЕРТИФИКАЦИИ

Зарегистрирована в Едином реестре
зарегистрированных систем добровольной сертификации
Федеральным агентством по техническому регулированию и метрологии
Российской Федерации

РЕГИСТРАЦИОННЫЙ НОМЕР РОСС RU. И864.04ФВНО

Орган по сертификации АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ЦЕНТР СЕРТИФИКАЦИИ, ТЕХНИЧЕСКИХ ИСПЫТАНИЙ И ИССЛЕДОВАНИЙ
"СЕРТИФИКАТ.РУ" (АНО "СЕРТИФИКАТ.РУ")

Р

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ 396-19 действия
с 29 апреля 2016 г.
по 29 апреля 2019 г.

Настоящий сертификат удостоверяет, что
КОСТИН ПАВЕЛ ВАСИЛЬЕВИЧ

(ФИО, название организации)

соответствует требованиям системы и сертифицирован(а) в качестве
судебного эксперта (судебной экспертной организации) в области
Исследование промышленных (непродовольственных)
товаров, в том числе с целью проведения их оценки

(область специализации)

Основание для выдачи сертификата
Решение Аттестационной комиссии № 205 от 29 апреля 2016г.



Руководитель органа
по сертификации


(подпись)

И.В. Вашуркин
(инициалы, фамилия)

Е



Ц

некоммерческое партнерство
"ПАЛАТА СУДЕБНЫХ ЭКСПЕРТОВ"

Москва

20 февраля 2013 г.

СВИДЕТЕЛЬСТВО

*Косин Павел
Васильевич*

прошел (прошла) обучение по программе
повышения квалификации судебных экспертов
в объеме 104 учебных часов:

21.1 « Исследование информационных компьютерных средств »

утвержденной Приказом Минюста России от 13 октября 2004 г., № 169.



Генеральный директор
НП "СУДЭКС"

С.Е. (с.е.)

Федеральный закон
«О государственной судебно-экспертной деятельности в Российской Федерации»
(№73-ФЗ от 31.05.2001).

Статья 41. Распространение действия настоящего Федерального закона на судебно-экспертную деятельность лиц,
не являющихся государственными судебными экспертами

В соответствии с нормами процессуального законодательства Российской Федерации судебная экспертиза может
производиться вне государственных судебно-экспертных учреждений лицами, обладающими специальными знания-
ми в области науки, техники, искусства или ремесла, но не являющимися государственными судебными экспертами.





Ассоциация
образовательных учреждений
«Судебная экспертиза»



Некоммерческое партнерство
саморегулируемая организация
«Национальное Объединение
Судебных Экспертов»



«СУДЭКС»

Удостоверение является документом
о повышении квалификации

Регистрационный номер
1886/16



з

т

о

«СУДЭКС»

Некоммерческое партнерство
«ПАЛАТА СУДЕБНЫХ ЭКСПЕРТОВ»

**УДОСТОВЕРЕНИЕ
О ПОВЫШЕНИИ КВАЛИФИКАЦИИ**

Костин

Павел Васильевич

(фамилия, имя, отчество)

прошел(а) обучение по программе 21.1 Исследование
информационных компьютерных средств

(наименование программы)

«СУДЭКС»
дополнительного профессионального образования)

В период с 03 февраля 2016 по 17 февраля 2016

Объем программы 104 академических часа



Киселев С.Е.

Ректор (директор)

Швецова А.В.

Секретарь

Город Москва

а

**СИСТЕМА ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ
НЕГОСУДАРСТВЕННЫХ СУДЕБНЫХ ЭКСПЕРТОВ**

Зарегистрирована в Едином реестре
зарегистрированных систем добровольной сертификации
Федеральным агентством по техническому регулированию и метрологии
Российской Федерации

Регистрационный № РОСС RU.И597.04НЯ00 от 16 октября 2009 г.

№ 007428

Некоммерческое партнерство
«ПАЛАТА СУДЕБНЫХ ЭКСПЕРТОВ»
Исполнительное отделение по сертификации
Адрес: 127018, г. Москва, ул. Складочная, д. 1, стр. 15

СЕРТИФИКАТ СООТВЕТСТВИЯ

Дата внесения в Реестр «18» февраля 2010 г.
Действителен с «17» февраля 2016 г. по «16» февраля 2019 г.

НАСТОЯЩИЙ СЕРТИФИКАТ УДОСТОВЕРЯЕТ, ЧТО

КОСТИН ПАВЕЛ ВАСИЛЬЕВИЧ

является компетентным и соответствует требованиям системы
добровольной сертификации негосударственных судебных
экспертов по специальности:

«ИССЛЕДОВАНИЕ ИНФОРМАЦИОННЫХ КОМПЬЮТЕРНЫХ СРЕДСТВ»

ОСНОВАНИЕ ДЛЯ ВЫДАЧИ ИЛИ ПРОДЛЕНИЯ СРОКА ДЕЙСТВИЯ СЕРТИФИКАТА:

Решение Совета Системы от 18.02.2010 (Протокол № 12)

Срок действия сертификата продлен решением Совета Системы от 17.02.2016 г. (Протокол № 16)



Руководитель органа
по сертификации

Н.М. Гречуха



Ц

о

б

р

а

з

е

Пронумеровано, прошнуровано и

скреплено

И. Ибрагимов

директор

подпись

«14» октября 2017г.

