Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

РАБОТА ПРОВЕРЕНА
Рецензент, ген. директор АНО
«Центр судебных экспертиз и
научно-технических исследований»
_____ А .В. Волков
_____ 2018 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2018 г.

Разработка методики проведения компьютерно - технических экспертиз вредоносного программного обеспечения на основе реверс - инжиниринга

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.05.2018.351.ПЗ ВКР

Консультанты

Безопасность жизнедеятельности,
к.т.н., доцент
_____ Н.В. Глотова
_____ 2018 г.

Руководитель проекта,
Начальник отдела АНО «Центр
экспертиз и научно-технических
исследований»
_____ В. С. Лужнов
_____ 2018 г.

Автор проекта,
студент группы КЭ-532
_____ Е. А. Валяев
_____ 2018 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2018 г.

Челябинск 2018

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

Специальность 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

УТВЕРЖДАЮ

Заведующий кафедрой
_____ А.Н. Соколов

_____ 2018 г.

З А Д А Н И Е
на выпускную квалификационную работу студента

Валяева Егора Александровича

Группа *КЭ-532*

1 Тема работы

Разработка методики проведения компьютерно-технических экспертиз вредоносного программного обеспечения на основе реверс-инжиниринга

Утверждена приказом ректора ЮУрГУ от _____ № _____
(утверждена, прот. заседания кафедры от _____ № _____)

2 Срок сдачи студентом законченной работы _____

3 Исходные данные к работе

Отчет о преддипломной практике, нормативно-правовые документы в области защиты информации, документация предприятия-базы практики

4 Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов)

1 Анализ нормативно-правовых и научных основ проведения компьютерно-технических экспертиз
1.1 Криминалистика и судебная экспертиза в системе наук
1.2 Специальная методология криминалистики и судебной экспертизы как проблема
1.3 Исследование компьютерно-технических средств
1.4 Уголовно-правовая характеристика и особенности юридической квалификации преступлений, сопряженных с применением компьютерных средств
1.5 Особенности собирания криминалистически значимой компьютерной информации
1.6 Формы использования в уголовном и гражданском судопроизводстве специальных познаний в сфере современных информационных технологий
2 КОМПЬЮТЕРНО-ТЕХНИЧЕСКИЕ ЭКСПЕРТИЗЫ
2.1 Понятие судебной экспертизы
2.2 Понятие компьютерно-технической экспертизы
2.3 Понятие экспертной методики
2.4 Требования законодательства к методике (и методам) производства экспертизы
2.5 Анализ методик производства КТЭ
3 МЕТОДИКА ПРОВЕДЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ
3.1 Подготовительная стадия
3.2 Аналитическая стадия
3.3. Эксперимент
3.4. Синтезирующая стадия
3.5. Результативная стадия
3.6. Формирование выводов
3.7. Заключение эксперта
3.8. Оценка эффективности разработанной методики производства экспертизы
4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ
4.1. Общие требования к организации рабочих мест пользователей
4.2. Требования к помещениям для размещения рабочего места
4.3. Требования к уровням шума на рабочих местах
4.4. Требования к освещению на рабочих местах
4.5. Требования к микроклимату
4.6. Требования к электробезопасности
4.7. Пожарная безопасность
4.8. Сравнение параметров рабочего места с допустимыми нормами.

5 Перечень графического материала (с точным указанием обязательных чертежей, плакатов в листах формата А1)

Всего ___ листов

6 Консультанты по работе (проекту), с указанием относящихся к ним разделов работы (проекта)

Раздел	Консультант	Подпись, дата	
		Задание выдал (консультант)	Задание принял (студент)
БЖД	К.т.н., доцент, Н.В. Глотова		

7 Дата выдачи задания _____

Руководитель,
начальник отдела технических
исследований АНО «ЦНТИ» _____ В.С. Лужнов

Задание принял к исполнению _____Валяев Е.А.

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	**Срок выполнения этапов работы**	**Отметки о выполнении руководителя**
Введение		
1 Анализ нормативно-правовых и научных основ проведения компьютерно-технических экспертиз		
2 Компьютерно-технические экспертизы		
3 Методика проведения компьютерно-технической экспертизы		
4 Безопасность жизнедеятельности		
Заключение		
Библиографический список		
Предзащита ВКР		
Защита ВКР		

Заведующий кафедрой _____ А.Н. Соколов

Руководитель работы _____ В.С. Лужнов

Студент _____ Е.А. Валяев

АННОТАЦИЯ

Валяев Е.А. Разработка методики проведения компьютерно-технических экспертиз вредоносного программного обеспечения на основе реверс-инжиниринга: ЮУрГУ, КЭ-532, 109 с., 1 ил., 2 табл., библиогр. список – 35 наим., 1 прил.

В работе рассмотрена методика проведения компьютерно-технических экспертиз вредоносного программного обеспечения на основе методов реверс-инжиниринга. Проведен обзор существующих на сегодняшний день решений в области проведения компьютерно-технических экспертиз в Российской Федерации и за рубежом, проанализирована нормативно-правовая база и актуальные научные разработки по теме работы. Обоснована актуальность разработки собственной комплексной методики в условиях отсутствия нормативно закрепленных подходов и острой потребности органов внутренних дел и следствия в научно обоснованной, всесторонней методике проведения экспертиз в областях, связанных с вредоносным программным обеспечением. Подробно изучены методические, научные и правовые основы проведения компьютерно-технических экспертиз, технические и программные особенности проведения дизассемблирования программного обеспечения для современных ЭВМ. По результатам проведенного комплексного анализа разработана собственная методика проведения компьютерно-технических экспертиз и проведена ее апробация на реальном объекте в рамках практической деятельности на базе экспертной организации.

					ЮУРГУ-100505.2018.351.ПЗ ВКР		
Изм.	Лист	№ докум.	Подпись	Дата			
Разраб.		Валяев			Разработка методики проведения компьютерно-технических экспертиз вредоносного программного обеспечения на основе реверс - инжиниринга	Лит.	Лист 6 / Листов 109
Пров.		Лужнов					
Рецензент		Волков				ЮУрГУ	
Н. контр.		Мартынов				Кафедра ЗИ	
Утв.		Соколов					

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ 9
ВВЕДЕНИЕ 10
1 АНАЛИЗ НОРМАТИВНО-ПРАВОВЫХ И НАУЧНЫХ ОСНОВ ПРОВЕДЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТИЗ 12
1.1 Криминалистика и судебная экспертиза в системе наук 12
1.2 Специальная методология криминалистики и судебной экспертизы как проблема 14
1.3 Исследование компьютерно-технических средств 19
1.4 Уголовно-правовая характеристика и особенности юридической квалификации преступлений, сопряженных с применением компьютерных средств 26
1.5 Особенности собирания криминалистически значимой компьютерной информации 31
1.6 Формы использования в уголовном и гражданском судопроизводстве специальных познаний в сфере современных информационных технологий 33
Выводы по главе 1 36
2 КОМПЬЮТЕРНО-ТЕХНИЧЕСКИЕ ЭКСПЕРТИЗЫ 38
2.1 Понятие судебной экспертизы 38
2.2 Понятие компьютерно-технической экспертизы 38
2.3 Понятие экспертной методики 40
2.4 Требования законодательства к методике (и методам) производства экспертизы 41
2.5 Анализ методик производства КТЭ 42
Выводы по главе 2 46
3 МЕТОДИКА ПРОВЕДЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ 47
3.1 Подготовительная стадия 48
3.2 Аналитическая стадия 52
3.3. Эксперимент 56
3.4. Синтезирующая стадия 56
3.5. Результативная стадия 62
3.6. Формирование выводов 62
3.7. Заключение эксперта 63

3.8. Оценка эффективности разработанной методики производства экспертизы 64
Выводы по главе 3 65
4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ 67
4.1. Общие требования к организации рабочих мест пользователей 67
4.2. Требования к помещениям для размещения рабочего места 68
4.3. Требования к уровням шума на рабочих местах 69
4.4. Требования к освещению на рабочих местах 69
4.5. Требования к микроклимату 70
4.6. Требования к электробезопасности 71
4.7. Пожарная безопасность 72
4.8. Сравнение параметров рабочего места с допустимыми нормами. 77
Выводы по главе 4 79
БИБЛИОГРАФИЧЕСКИЙ СПИСОК 80
ПРИЛОЖЕНИЕ А. 83

СОКРАЩЕНИЯ

ПО – программное обеспечение.
ОС – операционная система.
ИБ – информационная безопасность.
ЗИ – защита информации.
ЭВМ – электронная вычислительная машина.
ЯП – язык программирования.
Д/А – дизассемблирование.
КТЭ – компьютерно-техническая экспертиза.
СКТЭ – судебная компьютерно-техническая экспертиза.
ПЗУ – постоянное запоминающее устройство.
ОЗУ – оперативное запоминающее устройство.
BIOS – basic input/output system, базовая система ввода-вывода.
НЖМД – накопитель на жестком магнитном диске.

ВВЕДЕНИЕ

Современное состояние мирового сообщества характеризуется всеобъемлющим проникновением современных информационных технологий в различные области человеческой деятельности: экономическую, социальную, управленческую и другие. Рубеж второго и третьего тысячелетия, наступление эры господства информации во всех странах планеты повсеместно характеризуются резким ростом преступлении в сфере компьютерной информации, а также преступлений, где компьютерные средства используются как элементы способа их совершения и сокрытия.

Отдельным видом таких средств является вредоносное программное обеспечение. Ежедневно по данным ведущих компаний-разработчиков антивирусных программных средств появляется более двух миллионов новых вредоносных программ. Преступления, совершенные с их использованием, подпадают в Российской Федерации под действие статьи 273 УК РФ, а установление злоумышленников, способов совершения преступления и расследование таких преступлений в целом затруднено. Зачастую, единственным таким способом является проведение компьютерно-технической экспертизы.

На сегодняшний день в Российской Федерации не существует нормативно закрепленных методик проведения компьютерно-технических экспертиз вредоносного программного обеспечения, отдельные научные и методические публикации описывают такие методики формально, оставляя все детали проведения экспертизы на долю компетенции эксперта, обладающего специальными знаниями. В результате это приводит к тому, что большая часть уголовных дел в сфере компьютерных преступлений, связанных с использованием вредоносного программного обеспечения, остаются нераскрытыми, в виду либо недостаточной квалификации эксперта, либо сложности анализа вредоносного программного обеспечения: эксперт не имеет доступа к исходному коду программы, в связи с чем ее анализ либо затруднен, либо в принципе невозможен. Наиболее эффективным в данном случае методом является реверс-инжиниринг, или дизассемблирование, исходного кода вредоносного ПО для установления его принципов работы и потенциального устранения последствий и ущерба.

В связи вышеуказанным актуальной является острая потребность экспертных учреждений и экспертов в методике, которая бы позволяла проводить анализ работы вредоносного программного обеспечения и при этом гарантировала объективность и доказательную базу результатов экспертизы. Целью данной выпускной квалификационной работы является разработка методики проведения КТЭ вредоносного ПО на основе методов реверс-инжиниринга.

Для достижения указанной цели необходимо решить следующие задачи:

- изучить действующую нормативно-правовую, научную и теоретическую базу проведения КТЭ в Российской Федерации;
- изучить методы реверс-инжиниринга и реверсивного анализа исходного кода программного обеспечения с учетом специфики вредоносного ПО;

- разработать методику проведения КТЭ вредоносного ПО на основе методов реверс-инжиниринга и провести ее апробацию на конкретном объекте в рамках практической деятельности.

1 АНАЛИЗ НОРМАТИВНО-ПРАВОВЫХ И НАУЧНЫХ ОСНОВ ПРОВЕДЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТИЗ

1.1 Криминалистика и судебная экспертиза в системе наук

Хотя место криминалистики в системе наук однозначно не определено и в панораме мировой криминалистики она занимает в разных странах различное место, актуальность этой проблематики остается высокой, как с точки зрения развития науки, так и с позиций подготовки и специализации кадров. В настоящее время в связи с криминализацией общества во всех высокоразвитых странах, усложнением и дифференциацией структуры преступности, накоплением колоссального теоретического, эмпирического и практического материала во всех отраслях и уровнях криминалистического знания сама криминалистика превратилась в меганауку с чрезвычайно разветвленной и сложной структурой. Достаточно сказать, что только в области криминалистической экспертизы сейчас насчитываются десятки профессионально специализированных отраслей знания, требующих специальной подготовки, информационно-технологического обеспечения и профессионального опыта. Именно поэтому в ряде стран предпочитают говорить не о криминалистике, а о «судебных науках» (forensic sience), криминологии, «научном расследовании» и т.д., растворяя криминалистику в системе специально-научных знаний.

Именно поэтому в ряде стран криминалистика рассматривается как полицейская наука и в крупнейших университетах мира не преподается.

Более века развития криминалистики показали высокую эффективность научных методов раскрытия и расследования преступлений и значимость ее в этой сфере постоянно возрастает.

Вместе с тем, чрезвычайно возросла роль криминалистики и судебной экспертизы в сфере гражданской юстиции при рассмотрении основной массы гражданских, хозяйственных, семейных, административных, арбитражных и иных дел.

Причина столь широкого расширения сферы приложения криминалистики кроется в потенциале этой науки, накопленном за весь период ее существования.

Поскольку расследование уголовных дел всегда отличались большей сложностью и требовало применения специальных знаний из области естественных и технических наук, криминалистика в системе юридических наук сформировалась как система научно-технического знания, обслуживающая все нуждающиеся в этих знаниях отрасли судебных наук. При этом ее важнейшая функция состоит в «посредничестве» между естественно-техническим и юридическим знанием.

Эта последняя функция в настоящее время приобретает все большее значение в связи с усложнением и специализацией судебно-экспертных знаний и еще низким базовым уровнем подготовки оперативно следственных кадров. Поэтому узкий специалист не понимает своей задачи на месте преступления, а оперативник, не зная возможностей экспертизы, не может сформулировать задачу.

Криминалистика является единственной отраслью научного знания, которая способна преодолеть этот разрыв знаний и навыков и организовать эффективный профессиональный контакт в сфере правоприменительной деятельности. Без этого невозможно говорить о каких-либо современных профессиональных технологиях криминалистической и экспертной деятельности.

В криминалистике и судебной экспертизе созданы и апробированы технологии исследования вещественных доказательств, личных источников доказательств и структуры расследуемых событий.

Эти технологии могут и уже успешно используются в гражданском, арбитражном, административном и любом другом судебном процессе. Принципиальное, методологическое значение при этом имеет положение об инвариантности устанавливаемых посредством указанных технологий фактов. Доказательственное значение таких фактов (тождество, родство, подлинность, причина и др.) не зависит от правовой природы процесса.

Можно утверждать, что информационный и технологический потенциал, накопленный в криминалистике и судебной экспертизе, представляющий информационные технологии процессуального доказывания, является необходимым компонентом любого юридического знания и обязательным элементом профессиональной подготовки любого юриста.

Таким образом, закономерность развития криминалистики в системе юридических наук и ее функциональная востребованность позволяют рассматривать ее на современной стадии как отрасль знания, исследующую средства методологического, информационного и технологического обеспечения правоприменительной деятельности.

При этом:

- к сфере такого обеспечения могут быть отнесены все отрасли правоприменительной деятельности;
- деятельность всех государственных и негосударственных органов, связанных с правоприменительной деятельностью;
- все уровни этой деятельности: технический, тактический и стратегический;
- все субъекты этой деятельности.

Важнейшей функцией криминалистики на современном уровне ее развития является исследование механизма взаимодействия систем юридического и научно-технического знания, а также систем и субъектов различных областей и уровней правоприменительной деятельности.

Анализ наиболее существенных недостатков правоприменительной деятельности в сфере применения современных высоких технологий, показывает, что их причины кроятся в профессиональной, ведомственной и научной разобщенности и изолированности органов и субъектов, осуществляющих единонаправленную правоприменительную деятельность.

Криминалистика в настоящее время является единственной юридической наукой, методологический аппарат которой пригоден для анализа целостной

структуры правоприменительной деятельности с целью ее методологического информационного и технологического обеспечения.

Из сказанного видно, что в настоящее время криминалистика из узко специальной отрасли знания, обслуживающей деятельность по раскрытию и расследованию преступлений, превратилась в науку методологического уровня, исследующую правоприменительную деятельность в ее общем масштабе.

Поэтому она должна рассматриваться и развиваться как дисциплина Методологического уровня в неразрывной связи с общей методологией права, теорией судебных доказательств и судебной экспертизой.

Требуют пересмотра, в связи с этим, место и удельный вес криминалистики в стандартах профессионального юридического образования.

1.2 Специальная методология криминалистики и судебной экспертизы как проблема

Проблема специального метода, точнее методологии, криминалистики возникла не сегодня, но именно сегодня она настоятельно требует своего разрешения, поскольку дальнейшее развитие и криминалистики и судебной экспертизы непосредственно связаны с ее решением.

Актуальность данной проблемы определяется рядом специфических особенностей рассматриваемых отраслей знания в системе наук, обеспечивающих эффективность деятельности государственных оперативно-розыскных, следственных и прокурорских органов, а также всей судебной системы. Эти особенности характеризуются:

Прикладным характером и ролью этих наук, обслуживающих деятельность государственных органов и судебной системы.

Тесной связью методологии и технологий этих наук со способом совершения преступлений и структурой правоотношений.

Особыми свойствами исходной криминалистической информации в следах и последствиях расследуемых событий.

Дефицитом информации, как главной проблемой раскрытия и расследования, и необходимостью специальных технологий его преодоления.

Многосубъектным и многоуровневым характером криминалистической деятельности и необходимостью комплексного использования общенаучных и специальных методов решения криминалистических и судебно-экспертныхзадач.

Актуальность данной проблемы еще более взрастает в связи с тем, что данный уровень методологии криминалистики не был подвергнут специальному научному исследованию.

Решение проблемы специальной методологии криминалистики следует начинать, по нашему мнению, с определения ее места в системе методологии науки и структуре криминалистической деятельности.

В советской криминалистике формула общего метода расследования, не потерявшая своего значения, была предложена Б.М.Шавером: «Идти от метода совершения преступления к методу его раскрытия».

В дальнейшем один из ведущих представителей теоретической криминалистки Р.С.Белкин, пропагандируя идею теоретизации криминалистики,

отождествил методологию науки с ее общей теорией, в связи с чем самостоятельный анализ методологии оказался излишним.

Отождествление теоретической и методологической функции науки имело для развития прикладной науки криминалистики отрицательные последствия: привело к выбору неправильных направлений и приоритетов в оценке значимости теоретических и прикладных исследований, разрыву связи теории и практики, потере актуальности научных разработок и др.

Существенные недостатки в разработке методологии криминалистики, как показывает анализ теоретических разделов учебных и монографических курсов криминалистики, обусловлен недооценкой функционального и системно-деятельностного подходов в исследовании предмета и объектов криминалистики.

Впервые системно-деятельностная концепция криминалистики была предложена в 1986 году и на этой основе обосновано определение криминалистической деятельности как объекта криминалистики.

Современное состояние методологии криминалистики позволяет выделить ряд наиболее актуальных проблем специальной методологии криминалистики.

Анализ методологии криминалистики как функциональной уровневой системы.

Вопросы специальной методологии криминалистики в учебной и монографической литературе рассматриваются, обычно на низшем уровне ее общей методологии и обозначаются как «специальные методы криминалистики», к которым относятся «собственно криминалистические методы, т.е. такие методы, которые возникли в криминалистике, и специальные методы других наук. Последние в криминалистике не утрачивают своей природы и остаются соответственно математическими, физическими, химическими и другими.

Такое понимание специальной методологии криминалистики не отвечает требованиям системно-функционального и уровневого подходов. Отдельные методы не образуют системы, для которой должна быть определена системообразующая функция. Если методы других наук на специальном криминалистическом уровне «не утрачивают своей природы», то в практической экспертизе мы будем иметь дело не с экспертом-криминалистом из ЭКЦ, а физиком из НИЯФ или другого академического института.

Специальная методология криминалистики должна рассматриваться в уровневой структуре общенаучного знания как одна из ее специализированных подсистем.

Такой анализ, в частности, обеспечивает рассмотрение методологии не как простой совокупности методов, а как системы взаимосвязанных, иерархически

соподчиненных, функционально содержательных уровней, на каждом из которых решается совершенно определенный круг исследовательских задач.

Системно-деятельностный анализ позволил выявить ряд методологических ошибок в научных криминалистических исследованиях. К их числу, в частности, относятся:

1. Недостаточность методологической проработки задачи криминалистической деятельности, являющейся системообразующим элементом любой криминалистической деятельности. Отсутствие методологической базы и критериев определения порождает продолжающиеся десятилетиями споры о понятиях идентификации, «диагностики», «распознавания» и др., которых понятия задачи смешивается с понятием метода.

Объясняется это тем, что до последнего времени сама криминалистическая деятельность не рассматривалась как системный объект криминалистической науки.

В связи с этим, методологическая проработка задач криминалистической деятельности должна, в первую очередь, включать:

- выяснение объема и содержания требований к определению понятия криминалистической задачи.
- структуризацию криминалистической деятельности по субъектному, процессуально-правовому и уровневому основанию и классификацию криминалистических задач внутри каждого из этих видов деятельности.

2. Недостаточность анализа уровневой организации самой криминалистической деятельности. Эта организация не получила до настоящего времени своего научного обоснования и практического преломления.

Между тем, на каждом из этих уровней (технический, тактический, стратегический) решаются свои специфические задачи, тесно взаимосвязанные и взаимодействующие с задачами других уровней.

Техника, тактика и методика рассматриваются в учебниках криминалистики как разделы науки, системы знаний, но не уровни криминалистической деятельности.

В связи с этим не возникает и проблемы определения технических, тактических и методических задач.

В этих условиях невозможна и разработка какой-либо специальной криминалистической методологии, а сама наука оказывается системой знаний, лишенной методологической направленности.

3. Неправильное определение методологического уровня специального криминалистического исследования.

Традиционно специальные методы науки криминалистики рассматривались как низший уровень ее общей методологии, нечто вроде необходимого добавления к общенаучным методам.

Применительно к структуре и уровням криминалистической деятельности эта проблема до недавнего времени рассматривалась как «особенности расследования» в методике расследования отдельных видов преступлений. В то же время

сама методика расследования относительно техники и тактики характеризовалась в ряде работ как раздел криминалистики, решающий задачи расследования «стратегического характера».

Такое понимание специальной методологии криминалистики представляется непоследовательным, поскольку низший уровень научной методологии не может обслуживать высший уровень деятельности.

Для разрешения данного противоречия существенно различать систему науки, теорию, искусственно выделяющую в интересах удобства их изучения разделы техники, тактики и методики, с одной стороны, и уровни криминалистической деятельности, в которой технические, тактические и стратегические уровни реализуются в органическом синтезе и единстве целостной единонаправленной деятельности.

Смешение теоретического (анализ структуры объекта) и методологического (оптимизация деятельности) подходов неизбежно будут порождать неразрешимые противоречия.

В соответствии с принципами системно-деятельностного подхода, представляющими аксиомы любой деятельности, формирование структуры любой деятельности должно начинаться с определения ее интегральной задачи, конечной цели. Без определения такой цели невозможны ее алгоритмизация, программирование, информационное и технологическое обеспечение.

В связи с этим, высший, стратегический уровень криминалистической деятельности может быть определен только как уровень, обеспечивающий решение конечных задач такой деятельности в форме соответствующих методик и технологий.

Такие методики и технологии должны рассматриваться как конечный продукт криминалистической науки, рассматриваемой в качестве прикладной области знания, обеспечивающей задачи раскрытия, расследования преступлений и нужды судопроизводства.

Отдельные приемы, методы и рекомендации, заимствованные из других наук или разработанные в самой криминалистике на техническом или тактическом уровне, могут рассматриваться в системе специальной криминалистической методологии только в составе специальной методики или технологии, обеспечивающей решение конечной криминалистической или экспертной задачи.

В связи со сказанным, вряд ли методологически обосновано рассматривать в качестве задач криминалистики не методики и технологии решения конечных задач деятельности, а отдельные приемы, средства и методы.

Принципиальный характер такого утверждения со всей очевидностью выявляется при ознакомлении с общей панорамой криминалистических и судебно экспертных исследований.

При этом нетрудно убедиться, что подавляющее большинство из них связано с рассмотрением узко специальных методов или методик, фундаментальная разработка которых осуществлена в других отраслях общенаучного или специального знания. Популяризация общенаучных или специальных знаний на опреде-

ленных этапах развития науки оправдана и необходима, но она не может подменить разработку и решение собственных криминалистических и экспертных задач.

Между тем, существенные недостатки в их решении видны уже при первом ознакомлении.

Приведем некоторые примеры.

- весьма распространенной, но методологически ошибочной является тенденция рассмотрения на уровне специальной методологии криминалистики методов частных естественных технических и гуманитарных наук (ср., например, «судебная физика», «криминалистическая кибернетика», «криминалистическая систематика» и т.д.). При этом творческое использование общенаучного знания для решения собственно криминалистических и судебноэкспертных задач (распознавание, отождествление, установление причины и др.) подменяется переложением общенаучных сведений с примерами из практики их использования.

- игнорирование законов, принципов и методов вышележащих уровней методологии. В игнорировании элементарных законов логики и общенаучной методологии легко убедиться на примере формирования понятия «криминалистической характеристики преступлений», в котором прямо игнорируются требования однозначности, существенности, функционального и системного подходов.

- отсутствие фундаментальной научной проработки общей системы криминалистических и судебно-экспертных задач. Большинство традиционных криминалистических и экспертных методик были сформированы на эмпирической основе по мере возникновения в следственной и судебной практике задач по исследованию ситуаций и источников доказательств. Методики, как правило, представляли эмпирическое обобщение следственной и экспертной практики, не обеспечивающее требуемых в настоящее время показателей эффективности.

Принципиальный методологический смысл этой проблемы прямо связан с задачей прикладной науки по созданию современных технологий криминалистической и судебно-экспертной деятельности.

В отличие от эмпирических обобщений практики цикл создания таких технологий предусматривает следующие обязательные этапы работ:

Определение задачи - Создание алгоритма - Определение технологических параметров - Эксперимент - Внедрение.

Из сказанного видно, что системная проработка задач является предпосылкой научного подхода к созданию современных методик и технологий криминалистической и судебно-экспертной деятельности.

На основе изложенного, предлагается следующее определение:

Специальная методология криминалистики и судебной экспертизы представляет методологический уровень ее общей системы, синтезирующий методологический потенциал философского, общенаучного, частно-научного уровней с методами и средствами, выработанными в самой криминалистике, с целью созда-

ния методики технологий решения типовых криминалистических и судебно-экспертных задач.

Существенное отличие этого определения от других заключается в том, что:

- специальная методология рассматривается как функциональная подсистема общей методологии, решающая специальные задачи своего методологического уровня;

- в качестве основания криминалистических и судебно-экспертных исследований рассматривается классификация типовых задач, обуславливающих структуру и конечный результат исследований;

- в качестве цели и конечного результата научных исследований рассматриваются не закономерности в исследуемых объектах и отдельные методы и рекомендации, могущие быть промежуточными результатами, а методики и технологии, обеспечивающие решение конечных типовых задач целостной системы деятельности.

Понимание специальной методологии криминалистики и судебной экспертизы как ее высшего методологического уровня позволяет решить ряд важных методологических проблем.

- организация криминалистической деятельности в соответствии с требованиями высших методологических уровней (недопустимость нарушения законов гносеологии, логики, общенаучных принципов, аксиом и т.п.);

- использование общих и частных закономерностей и методов вышележащих уровней для познания объектов собственного изучения и использования их в целях формирования криминалистических методик и технологий;

- использование уровня специальной методологии криминалистики как методологической базы, специальной лаборатории разработки и формирования специальных криминалистических методик и технологий, обеспечивающих решение криминалистических задач.

В свете данного понимания специальной методологии науки можно говорить и пересмотре самих концепций теории и методологии криминалистики.

На смену науковедческой концепции криминалистики, отождествляющей ее теорию и методологию внутри разрабатываемых ею закономерностей и систем знаний, должна прийти системно-деятельностная концепция.

Она видит себя как методологию деятельности, подчиняющую закономерности объекта разработке систем целенаправленной криминалистической и судебно-экспертной деятельности.

1.3 Исследование компьютерно-технических средств

Исследование компьютерно-технических следов в процессе расследования преступлений, сопряженных с использованием средств компьютерной техники, осуществляется с использованием специальных знаний в различных процессуальных формах. Уголовно процессуальный закон не содержит определение спе-

циальных знаний. Вместе с тем, данный термин употребляется законодателем в тексте УПК РФ как минимум, 4 раза: (ст.57, ст.58, ст. 195, ст. 199).

Федеральный закон от 31.05.2001г. №73-ФЗ «О государственной судебно-экспертной деятельности в РФ» устанавливает, что в результате деятельности экспертов разрешаются вопросы, требующие специальных знаний «в области науки, техники, искусства или ремесла».

Использование судебной экспертизы в доказательственной деятельности возможно, а в установленных законом случаях необходимо, поскольку регламентируется процессуальным законом и в первую очередь законодателем регулируется основание назначения экспертизы по уголовному делу, где фактическим основанием является возникшая при производстве по нему необходимость в специальных познаниях в науке, технике, искусстве или ремесле. Как способ собирания доказательств по уголовному делу экспертиза обладает рядом особенностей, а познавательная деятельность здесь, хотя она и управляется и контролируется следователем, все же в основе своей лежит вне сферы уголовно-процессуальных правоотношений и осуществляется не тем лицом, в чьем производстве находится уголовное дело, а экспертом.

Для разъяснения этих и других вопросов представляется необходимым выделить ряд дополнительных критериев, помогающих отграничить специальные знания от иных. Так, проф. В.Я. Колдин указывает, что специальные знания приобретаются «посредством специального (профессионального) образования и опыта», иными словами, автор связывает формирование специальных знаний получением как высшего профессионального образования, так и практического опыта. Представляется, что отмеченное свойство специальных знаний является весьма важным, но не единственным. Ю.В. Гаврилин дополнительно выделяет следующие признаки специальных знаний: возможность их неоднократного применения; представление специальных знаний не в прямой, а в опосредованной форме; исключительная компетенция эксперта (специалиста) в вопросе, требующем специального исследования; ограниченный круг субъектов применения.

Формы использования специальных знаний в процессе расследования подразделяются на процессуальную и непроцессуальную. К процессуальной форме относятся: приглашение специалистов в ходе производства отдельных следственных действий, производство экспертизы, заключение специалиста (представленные в письменном виде суждения по вопросам, поставленным перед специалистом сторонами), допрос эксперта (специалиста). К непроцессуальной форме относятся: производство предварительного исследования объектов, консультации, выполнение поручений технического характера, использование средств криминалистической регистрации, участие специалистов в оперативно-розыскных мероприятиях, в производстве ревизии и документальных проверок.

Изучение следственной практики убедительно свидетельствует о том, что при исследовании компьютерно-технических следов преступления в процессе расследования, производство экспертизы представляет собой наиболее распространенную форму использования специальных знаний.

Вопросам назначения и производства судебной экспертизы посвящена глава 27 УПК РФ. Производство (назначение) судебной экспертизы – следственное (судебно-следственное) действие, сущность которого заключается в даче заключения лицом, обладающим специальными знаниями в науке, технике, искусстве или ремесле (экспертом) после проведения специальных исследований по вопросам, поставленным перед ним должностным лицом, осуществляющим производство по делу, в постановлении о назначении экспертизы.

Компьютерно-техническая экспертиза – самостоятельный род судебных экспертиз, относящийся к классу инженерно-технических экспертиз, проводимый в целях: определения статуса объекта как компьютерного средства, выявления и изучения его роли в расследуемом преступлении, а также получения доступа к информации на электронных носителях с последующим всесторонним ее исследованием. Указанные цели представляются родовыми задачами компьютерно-технической экспертизы.

Рассматривая компьютерно-техническую экспертизу как самостоятельный род судебных экспертиз, относящийся к классу инженерно-технических, Е.Р.Россинская и А.И. Усов выделяет следующие ее виды: аппаратно-компьютерная экспертиза; программно-компьютерная экспертиза; компьютерно-сетевая экспертиза.

Система объектов компьютерно-технической экспертизы по классификационному основанию видового деления выглядит следующим образом:

- класс аппаратные объекты, включающий в себя виды: персональные компьютеры (стационарные, портативные), периферийные устройства, сетевые аппаратные средства (серверы, рабочие станции, активное оборудование, сетевые кабели и т.д.), интегрированные системы (органайзеры, пейджеры, мобильные телефоны и т.п.), встроенные системы на основе микропроцессорных контроллеров (иммобилайзеры, транспондеры, круиз-контроллеры и т.п.), любые комплектующие всех указанных компонент (аппаратные блоки, платы расширения, микросхемы и т.п.). Указанные виды могут охватывать различные сочетания подвидов. В криминалистическом аспекте наиболее важен подвид запоминающих устройств и носителей данных (все известные на момент проведения экспертизы электронные носители): микросхемы памяти, магнитные и лазерные диски, магнитооптические диски, магнитные ленты, карты и т.п.;

- класс программные объекты, включающий в себя виды: системное программное обеспечение (подвиды: операционная система, вспомогательные программы-утилиты, средства разработки и отладки программ, служебная системная информация); прикладное программное обеспечение [подвид приложения общего назначения (текстовые и графические редакторы, системы управления базами данных, электронные таблицы, редакторы презентаций и т.д.) и подвид приложения специального назначения (для решения задач в определенной области науки, техники, экономики и т.д.)];

- класс информационные объекты (данные), включающий в себя виды: текстовых и графических документов (как в бумажной, так и электронной форме),

изготовленных с использованием компьютерных средств; данных в форматах мультимедиа; информации в форматах баз данных и других приложений, имеющей прикладной характер.

Сущность судебной аппаратно-компьютерной экспертизы заключается в проведении исследования технических (аппаратных) средств компьютерной системы. Предметом данного вида судебной компьютерно-технической экспертизы являются факты и обстоятельства, устанавливаемые на основе исследования закономерностей эксплуатации аппаратных средств компьютерной системы – материальных носителей информации о факте или событии уголовного, или гражданского дела.

Для проведения экспертного исследования программного обеспечения предназначен такой вид компьютерно-технической экспертизы, как программно-компьютерная экспертиза. Ее видовым предметом являются закономерности разработки (создания) и применения (использования) программного обеспечения компьютерной системы, представленной на исследование в целях установления истины по гражданскому или уголовному делу. Целью программно-компьютерной экспертизы является изучение функционального предназначения, характеристик и реализуемых требований, алгоритма и структурных особенностей, текущего состояния, представленного на исследование программного обеспечения компьютерной системы.

Судебная информационно-компьютерная экспертиза (данных) является ключевым видом судебной компьютерно-технической экспертизы, так как позволяет завершить целостное построение доказательственной базы путем окончательного разрешения большинства диагностических и идентификационных вопросов, связанных с компьютерной информацией. Целью этого вида является поиск, обнаружение, анализ и оценка информации, подготовленной пользователем или порожденной (созданной) программами для организации информационных процессов в компьютерной системе.

Отдельный вид компьютерно-технической экспертизы – судебная компьютерно-сетевая экспертиза, в отличие от предыдущих основывается, прежде всего, на функциональном предназначении компьютерных средств, реализующих какую-либо сетевую информационную технологию. Поэтому исследование фактов и обстоятельств, связанных с использованием сетевых и телекоммуникационных технологий, по заданию следственных и судебных органов в целях установления истины по уголовному или гражданскому делу составляют видовой предмет компьютерно-сетевой экспертизы. Она выделена в отдельный вид в связи с тем, что лишь использование специальных познаний в области сетевых технологий позволяет соединить воедино полученные объекты, сведения о них и эффективно решить поставленные экспертные задачи. Особое место в компьютерно-сетевой экспертизе занимают экспертные исследования по уголовным и гражданским делам, связанным с Интернет-технологиями.

Объект применения специальных знаний этой экспертизы может быть разным – от компьютеров пользователей, подключенных к Internet, до различных ресур-

сов поставщика сетевых услуг (провайдера Internet) и предоставляемых им информационных услуг (электронная почта, служба электронных объявлений, телеконференции, WWW-сервис и пр.). В связи со стремительным развитием современных телекоммуникаций и связи, в судебной компьютерно-сетевой экспертизе можно выделить судебную телематическую экспертизу, предметом которой являются фактические данные, устанавливаемые на основе применения специальных познаний при исследовании средств телекоммуникаций и подвижной связи как материальных носителей информации о факте или событии какого-либо уголовного либо гражданского дела.

Можно выделить следующие виды компьютерно-технических экспертиз, необходимость назначения которых возникает при расследовании преступлений в сфере компьютерной информации компьютерной информации:

1. Техническая экспертиза компьютеров и периферийных устройств. Она назначается и проводится в целях изучения технических особенностей компьютера, его периферийных устройств, технических параметров компьютерных сетей, а также причин возникновения сбоев в работе компьютерного оборудования.

2. Техническая экспертиза оборудования защиты компьютерной информации. Проводится в целях изучения технических устройств защиты информации, используемых на данном предприятии, организации, учреждении или фирме.

3. Экспертиза машинных данных и программного обеспечения ЭВМ. Осуществляется в целях изучения информации, хранящейся в компьютере и на магнитных носителях, в том числе изучение программных методов защиты компьютерной информации.

4. Экспертиза программного обеспечения и данных, используемых в компьютерной сети. Проводится в целях изучения информации, которая обрабатывается с помощью компьютерных сетей, эксплуатируемых на данном предприятии, организации, учреждении, фирме или компании.

С. А. Катков выделяет в качестве самостоятельного вида экспертизы по восстановлению содержания документов на магнитных носителях. Нам представляется, что, исходя из решаемых данным видом экспертного исследования вопросов, оно целиком относится к экспертизе машинных данных и программного обеспечения.

Как показывает практика, возможно так же назначение комплексной экспертизы, сочетающей в себе дактилоскопическую, компьютеро-техническую экспертизу, экспертизу веществ и материалов, технико-криминалистическую экспертизу документов, а также иные виды экспертного исследования.

На разрешение технической экспертизы компьютеров ставятся следующие диагностические вопросы:

- какая модель компьютера представлена на исследование, каковы его технические характеристики, параметры периферийных устройств;

- находится ли представленная компьютерная техника в исправном состоянии? Возможна ли ее эксплуатация? Если нет, то по каким причинам;

- соответствует ли представленная документация данным техническим устройствам и периферийному оборудованию;

- каковы условия сборки компьютера и его комплектующих: фирменная сборка, сборка из комплектующих в другой фирме или кустарная сборка? Имеются ли в наличии дополнительные устройства, не входящие в базовый комплект поставки (базовый комплект определяется из документации);

- имеет ли место наличие неисправностей отдельных устройств, магнитных носителей информации (выявляются различными тестовыми программами);

- не проводилась ли адаптация компьютера для работы с ним специфических пользователей (левша, слабовидящий и пр.).

К идентификационным можно отнести вопрос о наличии у комплектующих компьютера (например, печатных плат, магнитных носителей, дисководов и пр.) единого источника происхождения.

При технической экспертизе оборудования защиты ставятся следующие вопросы:

- какие технические устройства используются для защиты компьютерной информации? Каковы их технические характеристики;

- есть ли в наличии техническая документация на эти изделия? Соответствуют параметры устройств, изложенным в документации;

- подвергались или нет средства защиты программной модификации или физическому воздействию? Используются или нет кустарные средства защиты информации.

При экспертизе данных и программного обеспечения могут решаться как диагностические, так и идентификационные задачи. В зависимости от конкретных обстоятельств вопросы могут быть следующими. При решении диагностических задач:

1. Каков тип операционной системы, используемой в компьютере? Какова ее версия;

2. Какие программные продукты эксплуатируются на данном компьютере? Являются ли они лицензионными, или «пиратскими» копиями, или собственными оригинальными разработками? Когда производилась инсталляция (установка) данных программ;

3. Каково назначение программных продуктов? Для решения каких прикладных задач они предназначены? Какие способы ввода и вывода информации используются? Соответствуют ли результаты выполнения программ требуемым действиям;

4. Какие программные методы защиты информации используются (пароли, идентификационные коды, программы защиты и т.д.)? Не предпринимались ли попытки подбора паролей или иные попытки неправомерного доступа к компьютерной информации;

5. Какая информация содержится в скрытых файлах;

6. Имеются ли на представленном магнитном носителе стертые (удаленные) файлы? Если да, то каковы их имена, размеры и даты создания, давность удаления;

7. Возможно ли восстановление ранее удаленных файлов и каково их содержание;

8. Изменялось ли содержание файлов (указать, каких именно), если да, то в чем оно выразилось;

9. В каком виде хранится информация о результатах работы антивирусных программ, программ проверки контрольных сумм файлов? Каково содержание данной информации;

10. Имеет ли место наличие сбоев в работе отдельных программ? Каковы причины этих сбоев;

11. В каком состоянии находятся и что содержат файлы на магнитных носителях? Когда производилась последняя корректировка этих файлов;

12. К каким именно файлам делала обращение программа (указать, какая именно), представленная на машинном носителе и какие информационные файлы она создавала.

При решении идентификационных задач могут быть поставлены следующие вопросы:

1. Выполнена ли отдельная программа (или ее часть) определенным лицом (как справедливо отмечают авторы учебника «Криминалистика», данный вопрос решается комплексно при производстве компьютеро-технической и автороведческой экспертизы);

2. Соответствуют ли используемые в программах пароли и идентификационные коды вводимым пользователем.

При экспертизе сетевого программного обеспечения и данных ставятся следующие вопросы:

3. Какое программное обеспечение используется для функционирования компьютерной сети? Является ли оно лицензионным;

4. Каким образом осуществляется соединение компьютеров сети? Имеется ли выход на глобальные компьютерные сети;

5. Какие компьютеры являются серверами (главными компьютерами) сети? Каким образом осуществляется передача информации на данном предприятии, учреждении, организации, фирме или компании по узлам компьютерной сети;

6. Используются ли для ограничения доступа к информации компьютерной сети пароли, идентификационные коды? В каком виде они используются;

7. Имеются ли сбои в работе отдельных программ, отдельных компьютеров при функционировании их в составе сети? Каковы причины этих сбоев;

8. Какая информация передается, обрабатывается и модифицируется с использованием компьютерной сети.

Необходимо отметить, что объектами компьютерно-технических экспертиз кроме компьютеров в привычном понимании, их отдельных блоков, периферий-

ных устройств, технической документации к ним, а также носителей компьютерной информации могут выступать и компьютеры в непривычном понимании: электронные записные книжки, пейджеры, сотовые телефоны, электронные кассовые аппараты, иные электронные носители текстовой или цифровой информации, документация к ним. При этом на разрешения эксперта ставятся аналогичные вопросы.

Представляет интерес позиция В.В. Агафонова и А.Г. Филиппова, считающих, что в определенных случаях производство экспертизы можно заменить другим следственным действием, в частности, следственным осмотром или следственным экспериментом. Не вдаваясь в дискуссию по данному вопросу, отметим, что в тех случаях, когда собственных познаний следователя достаточно, и ему не требуются привлечения специальных познаний (например, при установлении факта нахождения определенной информации на машинном носителе), экспертизу действительно можно не назначать, а зафиксировать факт нахождения данной информации путем следственного осмотра с участием специалиста.

Следует отметить, что в настоящее время, класс компьютерно-технических экспертиз находится еще в стадии разработки. Проведенное исследование показало, что следователи испытывают значительные сложности с назначением подобных экспертиз, поскольку не во всех экспертных учреждениях имеются соответствующие специалисты, большинство следователей не знают о возможностях компьютерно-технических экспертиз, какие вопросы ставятся на их разрешение и какие материалы предоставляются в распоряжение экспертов.

1.4 Уголовно-правовая характеристика и особенности юридической квалификации преступлений, сопряженных с применением компьютерных средств

Стремительное развитие микропроцессорной техники и телекоммуникаций, а также обусловленное ими повсеместное внедрение современных информационных технологий во все жизненные сферы человека, в частности, породило новую форму криминальной деятельности. Как справедливо заметила Б.Х. Толеубекова «... признание компьютеризации как социально значимого явления неизбежно привело к признанию его криминального проявления как социально значимого. А это, в свою очередь, ставит перед исследователем задачу выявления индикаторов, указывающих на социальную обусловленность компьютерной преступности» [1].

В настоящее время проблема «компьютерной» преступности во всех странах мира, независимо от их географического положения, вызывает необходимость привлечения все большего внимания и сил правоохранительных органов для организации борьбы с данным видом преступлений.

До недавнего времени в России вообще отсутствовали какие-либо серьезные разработки, касающиеся юридической оценки исследуемой проблемы. Хотя первая информация о совершении хищения денежных средств с применением средств электронно-вычислительной техники относится еще к 1979 году, когда в

Вильнюсе было похищено 78584 рубля путем манипуляции на входе ЭВМ [2]. Новый скачек в развитии информационных технологий еще с большей степенью активизировал действия преступников в рассматриваемой сфере. Своеобразный «отсчет» компьютерных преступлений в России был начат с преступления, совершенного с использованием компьютерной технике в 1991 г., когда было похищено 125,5 тысяч долларов США во Внешэкономбанке СССР. Приведенный эпизод стал в юридической литературе уже классическим примером того, как можно проникнуть в систему электронных платежей и организовать хищение денежных средств путем перечисления их с одного счета на другой.

По оценкам отечественных и зарубежных исследователей уровень латентности компьютерных преступлений составляет около 90%. Из оставшихся 10% выявленных компьютерных преступлений, раскрывается только 1%. Анализ практики расследования других видов преступлений показывает, что компьютерная информация позволила в 52% случаев предъявить обвинение, в 35% — оказала существенную помощь в розыске преступников и позволила установить механизм совершение преступления.

Большинство рассматриваемых преступлений совершается в кредитно-финансовой сфере. Эта уголовно-правовая категория далеко не охватывает всего спектра применения компьютерных средств в преступных целях. Более того, есть все основания предполагать, что только в 10 % случаев пострадавшие организации обращаются в правоохранительные органы.

Анализ собственной практики, а также информационных материалов показал, что негативно на принятие решения потерпевшей стороной об обращении в правоохранительные органы по факту совершения преступления в рассматриваем случае влияют следующие факторы:

1. Неверие в компетентность сотрудников правоохранительных органов в вопросе установления самого факта совершения преступления, не говоря уже о процессе его раскрытия и расследования. Это утверждение в равной мере относится к сотрудникам как российских, так и зарубежных правоохранительных органов;

2. Боязнь подрыва собственного авторитета в деловых кругах и как результат этого - потеря значительного числа клиентов. Это обстоятельство особенно характерно для банков и крупных финансово-промышленных организаций, занимающихся широкой автоматизацией своих производственных процессов;

3. Неминуемое раскрытие в ходе судебного разбирательства системы безопасности организации, создание этой системы вновь сопряжено часто с большими затратами, чем ущерб, нанесенный преступлением;

4. Боязнь возможности выявления в ходе расследования преступления собственного незаконного механизма осуществления отдельных видов деятельности и проведения финансово-экономических операций (например, сокрытия части прибыли и т. п.);

5. Выявление в ходе расследования компьютерного преступления причин, способствующих его совершению, может поставить под сомнение профессиональную пригодность (компетентность) отдельных должностных лиц, что в конечном итоге приведет к негативным для них последствиям;

6. Правовая неграмотность подавляющего большинства должностных лиц в рассматриваемых вопросах нами, часто весьма далекое представление о реальной ценности информации, содержащейся в их компьютерных системах.

Современное состояние компьютерной преступности и следственной практики требует акцентировать внимание не только на преступлениях в сфере компьютерной информации, но и на расследовании таких «традиционных» преступлений, как: присвоение, мошенничество (наблюдается резкий скачек в сфере электронной торговли и развлечений), фальшивомонетничество, лжепредпринимательство и др. Здесь компьютерные средства задействуются для фальсификации платежных документов; хищения наличных и безналичных денежных средств (путем перечисления на фиктивные счета); «отмывания» денег; вторичного получения уже произведенных выплат; совершения покупок с использованием фальсифицированных или похищенных электронных платежных средств (кредитных карт) и пр.

В уголовно-правовом аспекте многие исследователи вышеозначенных вопросов до сих пор видят основную проблему понятия, классификации и криминалистической характеристики «компьютерных» преступлений в сложности и неоднозначность объектов посягательства. Сегодня Уголовный кодекс Российской Федерации определяет эти преступления как:

1.Неправомерный доступ к компьютерной информации, повлекший за собой уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети (ст. 272);

2. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами (ст. 273);

3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред (ст. 274).

Современная практика раскрытия и расследования преступлений характеризуется ростом преступлений в сфере компьютерной информации (ст.ст. 272, 273, 274 УК РФ), т.е. преступлений, сопряженных с использованием ЭВМ, систем ЭВМ или их сети, а также преступлений, где компьютерные средства используются как элементы способа их совершения и сокрытия. Необходимо отметить, что помимо предусмотренных уголовным законом самостоятельных составов преступлений гл.28 «Преступления в сфере компьютерной информации», еще целый ряд уголовно наказуемых деяний по своему составу вплотную сопрягают-

ся с указанной сферой. С позиций дифференциации обстоятельств, подлежащих установлению и доказыванию, здесь могут быть выделены следующие группы:

1. Первая группа, объединяет преступления, предметом которых являются компьютерные средства;

2. Вторая группа - компьютерные средства выступают одновременно как предмет и средство совершения преступления;

3. Третья группа охватывает преступления, где компьютерные средства выступают как средства совершения и (или) сокрытия преступления;

4. Четвертая группа - преступления, в которых компьютерные средства выступают как источник криминалистически значимой информации.

Для всех указанных групп преступлений характерны следующие особенности: использование современных информационных технологий и средств их реализации, высокий уровень латентности; сложность своевременного выявления преступления и установление виновного, трудности собирания доказательств и пр.

Практика расследования преступлений, сопряженных с использованием компьютерных средств, свидетельствует о значительном преобладании количества уголовных дел по другим статьям УК РФ над делами, относящихся по своему составу к главе 28 УК РФ. К ним относятся преступления, предусмотренные:

- ст. 146 - нарушение авторских и смежных прав (в части защиты авторских прав на программы для ЭВМ и баз данных); ст. 159 - мошенничество;

- ст. 165 - причинение имущественного ущерба путем обмана или злоупотребления доверием;

- ст. 187 - изготовление и сбыт поддельных кредитных либо расчетных карт и иных платежных документов; ст.292 - служебный подлог;

- ст. 174 - легализация (отмывание) денежных средств или иного имущества, приобретенного незаконным путем (в случае, если преступник перевел деньги со счета зарубежного банка на свой счет в российском банке и получает по этому вкладу начисляемые проценты);

- ст. 183 - незаконное получение или разглашение сведений, составляющих коммерческую или банковскую тайну (здесь под категорию коммерческой тайны подпадает список пользователей компьютерной системы с их паролями);

- ст. 129 - клевета (в случае размещения в сети Интернет заведомо ложных сведений, порочащих честь и достоинство определенного лица);

- ст. 137 - нарушение неприкосновенности частной жизни (при размещение информации, которая относиться к категории личной или семейной тайны);

- ст. 138 - нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (здесь речь идет об уголовной ответственности за чтение чужих электронных писем).

Проведение следственных действий по ряду статей УК РФ сопряжено с защитой безопасности интересов государства. Это, в первую очередь, ст. 207 - заведомо ложное сообщение об акте терроризма (например, в случае ложного сообщения о заминированных объектах посредством сети Интернет), затем ст. 276 -

шпионаж. Примером может являться проникновение в одну из компьютерных сетей Министерства обороны РФ . Ст. 283 - разглашение государственной тайны, устанавливает ответственность за предание огласке или распространение с нарушением установленного порядка (правил) сведений, составляющих государственную тайну, вследствие чего они становятся известны другим лицам (например, неограниченному числу пользователей Интернет).

Общим объектом преступлений, указанных в главе 28 УК РФ, являются общественные отношения, возникающие в процессе компьютерной обработки информации. К непосредственным предметам преступного посягательства относят: конкретную компьютерную информацию, базы данных определенных компьютерных систем и сетей, их отдельные файлы, а также специальные технологии и программные средства их обеспечения, включая средства защиты компьютерной информации . Денежные средства, другие материальные (например, контрафактная информационно-программная продукция и пр.) и нематериальные (например, разглашение государственной тайны и т.п.) ценности являются предметами преступного посягательства иных преступлений, предусмотренных в УК РФ помимо гл.28. Так, если в результате неправомерного доступа к компьютерной информации было совершено преступление, связанное с незаконным получением и разглашением сведений, составляющих коммерческую или банковскую тайну, виновные в их совершении должны нести уголовную ответственность по совокупности преступлений, предусмотренным другими статьями УК (в примере - статьи 272 и 183 УК РФ).

В криминалистике под механизмом следообразования понимается «специфическая конкретная форма протекания процесса, конечная фаза которого представляет собой образование следа-отображения. Элементами этого механизма являются объекты следообразования - следообразующий, следовоспринимающий и вещество следа, следовой контакт как результат взаимодействия между ними вследствие приложения энергии к объектам следообразования» .

Для преступлений, сопряженных с использованием компьютерных средств, одной из первых, представляющих практический интерес, была предложена следующая следовая картина1:

- следы на компьютерных средствах (в т.ч. носителях компьютерной информации), посредством которых действовал преступник на своем рабочем месте (в файловой системе, в ОЗУ, аппаратно-программная конфигурация и пр.) и вне носителей информации (рукописные записи и распечатки с принтера - коды доступа, тексты программ, телефонные счета и пр.);

- следы на «транзитных» (коммуникационных) носителях информации, посредством которых преступник осуществлял связь с информационными ресурсами, подвергавшимися неправомерному доступу (следы в линиях электросвязи: документированная информация о трафике через оператора телематических услуг, результаты наблюдения в ходе проведения ОРМ и следствия);

- следы в компьютерной системе (в т.ч. на носителях информации компьютерной) системы, в которую осуществлен неправомерный доступ, либо иные

противоправные действия (изменения в файловой системе, ОЗУ, аппаратно-программной конфигурации и пр.);

- следы на компьютерных средствах, которые сопряжены с иными (не только в сфере компьютерной информации) преступлениями - криминалистически значимая информация в компьютерах, органайзерах, мобильных телефонах, смарт-картах и пр.

Следует отметить, что сложность и многогранность рассматриваемого «нетрадиционного» типа следов в условиях отсутствия достаточно разработанного методологического аппарата накладывают особые требования к использованию специальных познаний при раскрытии и расследовании компьютерных преступлений.

Современная практика судопроизводства доказала, что раскрытие и расследование преступлений, в которых современные информационные технологии используются как средство совершения и сокрытия преступлений, невозможно без использования познаний, как в области современных информационных технологий, так и в сфере уголовного права, уголовного процесса и криминалистики. Поэтому успешно решать задачи борьбы с этими проявлениями преступности могут только всесторонне подготовленные специалисты. Существует сложившееся мнение: специалисты в области высоких технологий (инженеры-электронщики, программисты, математики и пр.), якобы, могут разрешить все специальные задачи по собиранию и исследованию криминалистически значимой информации, как в аппаратных, так и программных объектах исследования. Однако общая теория криминалистики и судебной экспертизы, а также практическая работа давно доказали, что это далеко не так.

1.5 Особенности собирания криминалистически значимой компьютерной информации

Преступления, сопряженные с использованием компьютерных средств, носят зачастую латентный характер, не оставляют видимых следов и сложны с точки зрения раскрытия и собирания доказательственной информации в связи со сложностью объектов - носителей этой информации, широким применением средств удаленного доступа и рядом других причин. При расследовании по делам указанной категории участие специалиста в сфере разработки и использования современных информационных технологий необходимо, поскольку, даже малейшие неквалифицированные действия с компьютерной системой зачастую заканчиваются безвозвратной утратой ценной розыскной и доказательственной информации.

Отмеченные уже ранее новые положения УПК РФ (ст.70), не препятствующие производства судебной экспертизы специалистом, участвующем в проведении следственного действия, имеют большое значение для собирания доказательств по делам, сопряженным с использованием компьютерных средств.

Практика показывает, что наиболее полезно участие специалиста в следственном осмотре, обыске и выемке. Собирание доказательств из автономных компьютерных систем, компьютеров, входящих в вычислительную сеть, а также других компьютерных средств в процессе следственного осмотра состоит в следующем.

Объектами осмотра по делам, связанным с компьютерными преступлениями, являются место происшествия и его обстановки, отдельные компьютерные средства и комплектующие, иные предметы, документы. При расследовании компьютерных преступлений производятся, как правило, следующие виды следственного осмотра:

- осмотр места происшествия или помещений, не являющихся местом преступления (офис или производственное помещение организации любой из форм собственности, квартира, частный дом, компьютерный класс учебного заведения, Интернет-кафе и пр.);
- осмотр предметов (компьютеров, органайзеров, мобильных телефонов, их комплектующих, носителей компьютерной информации и пр.);
- осмотр документов (описаний к компьютерным системам, производственно-эксплуатационной документации, документов финансовой отчетности, телефонных счетов и др.)

Осмотр места происшествия по делам, сопряженным с использованием компьютерных технологий - неотложное следственное действие, направленное на установление, фиксацию и исследование обстановки места происшествия, следов преступления и преступника, отобразившихся в компьютерном устройстве или вычислительной сети и иных фактических данных, позволяющих в совокупности с другими доказательствами сделать вывод о механизме компьютерного преступления и иных обстоятельствах расследуемого события.

Известно, что место происшествия (в пределах которого обнаружены следы совершенного преступления) может не совпадать с местом преступления. Это особенно характерно для преступлений в сфере компьютерной информации, например, когда вредоносная программа заносится в компьютерную сеть в одном городе, а преступный результат наступает в другом или даже в другой стране.

Осмотр предметов - компьютерных средств - позволяет устанавливать состояние предмета, наименование и назначение, выявить индивидуальные признаки компьютера, дискеты или носителя данных, его дефекты и особенно признаки, свидетельствующие о том, по какому назначению он использовался и как интенсивно, а также признаки, указывающие на связь предмета, с расследуемым событием. В процессе осмотра компьютерных средств необходимо сосредоточить свои усилия на выявлении тех следов и признаков, которые впоследствии станут объектами экспертного исследования, и строго соблюдать правила обращения с этими объектами, чтобы обеспечить их сохранность и доказательственную силу. Все это возможно только при участии специалиста.

Осмотр документов - источников и носителей криминалистически значимой компьютерной информации - имеет своей целью выявление и фиксацию таких их

признаков, которые придают документам значение вещественных доказательств, а также установление удостоверенных документами или изложенных в них обстоятельств и фактов, имеющих значение для дела. Тщательный осмотр документации, распечаток с принтеров, листингов программ, различных записей, даже на клочках бумаги, может иметь значение для успешного достижения цели. Сделать это необходимо и потому, что программисты часто не надеются на свою память и оставляют записи о паролях, изменениях конфигурации системы, особенностях построения информационной базы, комментариях к используемым идентификаторам и пр.

1.6 Формы использования в уголовном и гражданском судопроизводстве специальных познаний в сфере современных информационных технологий

Производство по уголовным и гражданским делам, сопряженным с использованием компьютерных средств и информационных технологий, представляет значительные трудности . Сам специфический способ совершения подобных деяний еще недостаточно изучен, а значит, имеются сложности не только в обнаружении криминалистически значимой информации, но и в ее фиксации, изъятии и последующем исследовании. Кроме того, по нашему мнению, следователи, прокуроры и судьи ни психологически, ни технически, ни профессионально не готовы к целенаправленному и эффективному противодействию рассматриваемым преступлениям, объективному и обоснованному разрешению дел, сопряженных с использование компьютерных технологий.

Залогом успешного раскрытия и расследования таких преступлений, судебного рассмотрения уголовных и гражданских дел является, в первую очередь, всестороннее выявление и исследование компьютерной информации, что невозможно без использования специальных познаний.

Закон не дает определения понятия «специальные познания». Традиционно в юридической литературе под этим термином понимают систему теоретических знаний и практических навыков в области конкретной науки, либо техники, искусства или ремесла, приобретаемых путем специальной подготовки или профессионального опыта и необходимых для решения вопросов, возникающих в процессе уголовного или гражданского судопроизводства . Применительно к теме настоящего исследования специальные познания в сфере современных информационных технологий составляют следующие научные направления: электроника, электротехника, информационные системы и процессы, радиотехника и связь, вычислительная техника (в том числе программирование) и автоматизация.

Основной формой использования научно-технических достижений в уголовном, гражданском и арбитражном процессе, производстве по делам об административных правонарушениях является судебная экспертиза. Сущность судебной экспертизы состоит в анализе по заданию следователя, суда, органа, рассматривающего административное правонарушение, сведущим лицом - экспертом -

предоставляемых в его распоряжение материальных объектов экспертизы (вещественных доказательств), а также различных документов (в том числе протоколов следственных действий), с целью установления фактических данных, имеющих значение для правильного разрешения дела. Судебную экспертизу от экспертиз, осуществляемых в иных сферах человеческой деятельности, в т.ч. сфере информационных технологий, отличают следующие признаки:

- подготовка материалов на экспертизу, назначение и проведение ее с соблюдением специального правового регламента, определяющего (наряду с соответствующей процедурой) права и обязанности эксперта, субъекта, назначившего экспертизу, участников уголовного, гражданского и арбитражного процесса;
- проведение исследования, основанного на использовании специальных знаний в различных областях науки, техники, искусства или ремесла;
- дача заключения, имеющего статус доказательства.

В соответствии со ст. 74 УПК РФ, заключение и показания эксперта допускаются в качестве доказательств. Основания и порядок назначения судебных экспертиз по уголовным и гражданским делам определяются соответствующими кодексами России (УПК, ГПК, АПК, КоАП) и Федеральным законом «О государственной судебно-экспертной деятельности в Российской Федерации»1. В этих нормативных актах устанавливаются права и обязанности лиц, принимающих участие в производстве судебной экспертизы, их правоотношения, содержание составляемых при этом основных процессуальных документов, регламентируются и другие вопросы, связанные с порядком назначения и производства экспертизы.

В соответствии с нормами процессуального законодательства Российской Федерации судебная компьютерно-техническая экспертиза может производиться как государственными судебными экспертами, так и иными экспертами из числа лиц, обладающих специальными знаниями (ст. 195 УПК). Правовая основа, принципы организации и основные направления государственной судебно-экспертной деятельности в РФ регламентированы соответствующим Федеральным законом.

Учитывая возрастающее вовлечение компьютерных систем в преступную деятельность, сотрудники судебно-экспертных учреждений все чаще в последнее время сталкиваются с таким объектом экспертных исследований, как компьютерные средства. Результаты проведенного исследования выявили динамику потребности в проведении судебно-экспертных исследований компьютерных средств и систем ЭКП ОВД.

Основным носителем специальных познаний (ст. 57 УПК, ст. 74 ГПК, ст. 66 АПК, ст. 252 КоАП) является эксперт. В качестве эксперта может быть вызвано любое лицо, обладающее необходимыми для дачи заключения познаниями.

Вопросы, поставленные на разрешение эксперта, не должны выходить за пределы его специальных познаний. Однако в процессуальном законодательстве не конкретизируется, каким образом определяются пределы компетенции судебного эксперта, кому конкретно может быть поручено производство судебных экспер-

тиз. Квалификацию эксперта обычно исследует субъект, назначивший экспертизу, при оценке заключения.

Статус судебного эксперта определяется кодифицированными законами (ст. 57 УПК; ст. 76 ГПК, ст.45 АПК; ст. 252 КоАП), которые предъявляют к эксперту серьезные требования. Эксперт обязан явиться по вызову суда (прокурора, следователя, лица, производящего дознание, органа, рассматривающего дело об административном правонарушении) и от своего имени дать объективное беспристрастное заключение по поставленным ему вопросам на основании исследования представленных материалов в соответствии со своими специальными знаниями.

Объективность заключения означает, что его дает лицо, не заинтересованное в исходе дела. Заключение эксперта должно основываться на положениях, дающих возможность проверить обоснованность и достоверность сделанных выводов на базе общепринятых научных и практических данных (ст.8 ФЗ).

Согласно ст. 12 Федерального закона РФ «О государственной судебно-экспертной деятельности в Российской Федерации» государственным судебным экспертом является аттестованный работник государственного судебно-экспертного учреждения, производящий судебную экспертизу в порядке исполнения своих должностных обязанностей. В указанном Федеральном законе указаны обязанности государственного эксперта, а также оговорены действия, которые он не вправе предпринимать (ст. 16).

Вместе с тем, эксперт обладает широкими полномочиями. Он может отказаться от дачи заключения, если представленные материалы недостаточны или поставленный вопрос выходит за рамки его компетенции. О невозможности дать заключение эксперт сообщает назначившему экспертизу в письменной форме.

Поскольку это необходимо для дачи заключения, эксперт имеет право знакомиться с материалами дела, заявлять ходатайства о предоставлении ему дополнительных материалов, участвовать в следственных действиях и судебном разбирательстве.

Участвуя в судебном заседании, эксперт может задавать вопросы участникам процесса (подсудимому, потерпевшему, свидетелям, представителям сторон и другим) об обстоятельствах, имеющих значение для дачи заключения. Эксперт может указать в заключении на имеющие значение для дела обстоятельства, в отношении которых ему не были заданы вопросы (ст. 204 УПК, ст. 77 ГПК, ст. 68 АПК).

В соответствии со ст. 41 действия ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» на судебно-экспертную деятельность лиц, не являющихся государственными судебными экспертами, распространяется большинство прав и обязанностей государственных экспертов:

Специальные познания, которыми обладают судебные эксперты, хотя во многом близки к тем, которыми оперируют представители базовых наук, но в то же время, весьма специфичны. Для решения задач судебной экспертизы, большинство из которых составляют обратные задачи (например, от следствий - следов

преступления - к причине - способу совершения и сокрытия), судебные эксперты пользуются специально разрабатываемыми методиками, незнакомыми специалистам из «большой науки». Поэтому судебно-экспертные исследования компьютерных средств и систем позволяют придать изъятым аппаратным средствам, программному обеспечению и компьютерной информации доказательственное значение.

Выводы по главе 1

Фактическое наступление эры господства информации во всех странах планеты, в т.ч. в России, повсеместно характеризуются резким ростом преступлений в сфере компьютерной информации, а также преступлений, где компьютерные средства используются как элементы способа их совершения и сокрытия. Законодательная регламентации правовых отношений и установления уголовной ответственности за совершение преступлений в сфере компьютерной информации нашло своё прямое отражение в ряде Федеральных Законов РФ, а также УК РФ.

Проведенный анализ норм уголовного права позволяет уточнить современные подходы к квалификации преступлений, сопряженных с использованием компьютерных средств, и рассматривать дефиницию «компьютерные преступления» в криминалистическом аспекте, как связанную со способом совершения и сокрытия преступления и, соответственно, с методикой его раскрытия и расследования. Развитие норм законодательного регулирования информационных правоотношений неизбежно повлекло за собой необходимость всесторонней проработки всех процессуальных механизмов их реализации.

В системе типичных признаков компьютерных преступлений, отражаемых их родовой криминалистической характеристикой, среди прочих, не менее важных, элементов, особое внимания уделяется данным о следах преступления. Современные исследования отдельных положений криминалистического учения о механизме следообразования применительно к сфере компьютерной информации привели к выделению особой группы следов, так называемых «виртуальных» следов. В развитие этого предложено толкование дефиниции «виртуальный след», не связанное с физическими (или иными) принципами отображения данных, но объективно обусловленное существованием компьютерной информации в компьютерных средствах и системах.

Преступления, сопряженные с использованием компьютерных средств, носят зачастую латентный характер, не оставляют видимых следов и сложны с точки зрения раскрытия и собирания доказательственной информации в связи со сложностью объектов - носителей этой информации, широким применением средств удаленного доступа и рядом других причин. Разработанные теоретические и методические основы собирания криминалистически значимой компьютерной информации позволяют учитывать особенности обнаружения, фиксации и изъятия компьютерных средств при производстве следственных действий. Введение в уголовное судопроизводство дополнительных следственных действий (арест

электронно-почтовой корреспонденции и локальной вычислительной сети) позволят значительно повысить эффективность собирания доказательств по рассматриваемым уголовным делам.

Залогом успешного раскрытия и расследования компьютерных преступлений, судебного рассмотрения уголовных и гражданских дел является, в первую очередь, всестороннее выявление и исследование криминалистически значимой компьютерной информации, что невозможно без использования специальных познаний. Специальные познания в сфере современных информационных технологий составляют следующие научные направления: электроника, электротехника, информационные системы и процессы, радиотехника и связь, вычислительная техника (в том числе программирование) и автоматизация.

При расследовании по делам указанной категории участие специалиста в сфере разработки и использования современных информационных технологий необходимо, поскольку, даже малейшие неквалифицированные действия с компьютерными средствами и системами неизбежно заканчиваются безвозвратной утратой ценной розыскной и доказательственной информации.

Среди ряда рассмотренных процессуальных и непроцессуальных форм использования специальных познаний в сфере современных информационных технологий выделяется основная процессуальная форма - судебная экспертиза, позволяющая придать изъятым аппаратным средствам, программному обеспечению и компьютерной информации доказательственное значение. Анализ статистических данных экспертной практики свидетельствуют уже о фактически начавшейся работе в направлении становления нового рода судебных экспертиз - судебной экспертизы компьютерных средств и систем, что обуславливает потребность всестороннего развития ее концептуальных основ.

2 КОМПЬЮТЕРНО-ТЕХНИЧЕСКИЕ ЭКСПЕРТИЗЫ

2.1 Понятие судебной экспертизы

Согласно ст. 9 ФЗ № 73 «О государственной судебно-экспертной деятельности в Российской Федерации» [4]:

1. «Судебная экспертиза – это процессуальное действие, состоящее из проведения исследований и дачи заключения экспертом по вопросам, разрешение которых требует специальных знаний в области науки, техники, искусства или ремесла и которые поставлены перед экспертом судом, судьей, органом дознания, лицом, производящим дознание, следователем, в целях установления обстоятельств, подлежащих доказыванию по конкретному делу»;

2. «Заключение эксперта – это письменный документ, отражающий ход и результаты исследований, проведенных экспертом».

Таким образом, судебная экспертиза – это особое процессуальное действие, проводимое в случае возникновения в деле вопросов, требующих специальных познаний в области науки, техники, искусства или ремесла. Понятие судебной экспертизы, как средства доказывания, присутствует во всех процессах. Судебная экспертиза – это отдельный и самостоятельный вид доказательства, имеющий перед законом одинаковую доказательную силу наравне с прочими доказательствами.

Предметом рода экспертизы является информация об экспертных задачах, экспертных методиках, методов решения вопросов, а также информация об объектах и их свойствах.

Предметом исследования в рамках экспертизы является предмет познания. Под предметом познания понимаются сведения об объектах, целях и условиях исследования, полученные в опыте и используемые на практике.

Экспертная задача – это цель исследования. Экспертные задачи делятся на общие, типовые, частные и конкретные. Общие задачи – задачи, решаемые во всех классах экспертиз (диагностические, идентификационные и 17 классификационные задачи). Типовые задачи - задачи, представляющие общую формулировку задач для рода экспертизы. Частные задачи – специфичные задачи для каждой экспертизы. Конкретные задачи – это конкретные вопросы, поставленные перед экспертом.

2.2 Понятие компьютерно-технической экспертизы

Компьютерно-техническая экспертиза (КТЭ) является самостоятельным родом судебных экспертиз. Она относится к классу инженерно-технических экспертиз. КТЭ проводится в «целях определения статуса объекта как компьютерного средства, выявления и изучения его следовой картины в расследуемом преступлении, получения доступа к информации на носителях данных с последующим всесторонним еѐ исследованием».

Основной задачей компьютерно-технической экспертизы является ответ на вопросы, требующие специальных познаний в области форензики (компьютерной криминалистики) – знаний о методах поиска, закрепления и исследования цифровых доказательств по преступлениям, связанным с компьютерной информацией (киберпреступлениям).

Согласно Приказу Министерства юстиции Российской Федерации (Минюст России) от 27 декабря 2012 г. N 237 г. Москва «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России», в рамках компьютерно- технической экспертизы происходит исследование информационных компьютерных средств. Такое определение существенно ограничивает круг вопросов, решаемых КТЭ.

В современной научной среде круг вопросов, относящихся к КТЭ значительно шире, так в составе КТЭ выделяют четыре вида экспертиз - аппаратно-компьютерную, программно-компьютерную, информационно- 18 компьютерную (она же экспертиза данных) и компьютерно-сетевую. Выделение такого количества и именно таких видов обусловлено свойствами объектов, предоставляемых на экспертизу, и вопросами решаемыми в рамках каждой конкретной экспертизы.

Аппаратно-компьютерная экспертиза направлена на решение вопросов, связанных с исследованием технической (аппаратной) части компьютерных средств, как правило, эти вопросы носят диагностический характер.

Программно-компьютерная экспертиза направлена на решение вопросов, связанных с исследованием программного обеспечения. В рамках программно- компьютерной экспертизы исследуются процедуры, алгоритмы, принципы разработки программного обеспечения, а также его использование, текущее состояние, структурные особенности, особенности эксплуатации.

Выделение компьютерно-сетевой экспертизы связано с бурным развитием науки и техники, и появлением широкого круга специфичных задач, сопряженных с сетевыми информационными технологиями. Компьютерно- сетевая экспертиза занимается исследованием обстоятельств и фактов, связанных с применением телекоммуникационных и сетевых технологий.

Ключевым видом КТЭ, позволяющим сформировать целостное построение доказательной базы путем решения большей части диагностических и идентификационных вопросов данного рода экспертизы, является информационно-компьютерная экспертиза. Информационно-компьютерная экспертиза решает задачи, связанные с поиском, обнаружением, оценкой и анализом информации, содержащейся в компьютерной системе.

В результате КТЭ, проводимой при расследовании преступлений, связанных с нарушением информационной безопасности в открытых компьютерных сетях, хищением (разрушением, модификацией) информации и нарушением информа-

ционной безопасности, формируется информация об уязвимости процессов переработки информации в информационных системах. В соответствии с правилами производства экспертизы эксперты КТЭ в своем заключении отвечают на вопросы экспертизы и не дают рекомендаций по 19 совершенствованию существующих средств защиты информации и обеспечения информационной безопасности (если это не является вопросом экспертизы). При этом результаты КТЭ могут быть использованы специалистами по информационной безопасности для совершенствования существующих средств защиты информации и обеспечения информационной безопасности.

Учитывая современный уровень развития науки и техники, и практический опыт производства КТЭ, подтверждающий тот факт, что рассмотренные выше виды КТЭ при производстве большей части экспертных исследований применяются комплексно (как правило, изучение начинается с технической части, далее – программной, после – исследование данных), предлагается введение нового определение КТЭ и внесение в связи с этим поправок в соответствующие законодательные акты.

Под компьютерно- технической экспертизой предлагается понимать самостоятельный род судебных экспертиз, относящийся к классу инженерно-технических экспертиз, проводимой в целях выявления и изучения следовой картины в расследуемом преступлении, путем комплексного исследования компьютерных средств: технической (аппаратной) части компьютерных средств; программного обеспечения; объектов сетевых информационных технологий; информации, содержащейся в компьютерной системе.

В дальнейшем в тексте термин КТЭ используется именно в этой трактовке.

2.3 Понятие экспертной методики

Существует несколько определений понятия «экспертная методика». В общем смысле, под экспертной методикой (методикой экспертного исследования) понимается последовательность изучения свойств объекта экспертизы с целью решения экспертной задачи, путем упорядоченного применения научно разработанной системы методов экспертного познания.

Экспертная методика может содержать как последовательность категорических, так и альтернативных методов и средств решения задач.

Экспертные методики разделяются на общие, частные и конкретные.

Общая методика описывает технологию экспертного исследования и является общей для всех видов экспертиз.

Частная методика - создается под частную ситуацию определенного рода, вида экспертиз.

Конкретная методика – методика, используемая для производства конкретной экспертизы. Как правило, конкретная методика – это частная методика, адаптированная под определенные задачи отдельной экспертизы.

Предлагаемая в настоящей работе методика относится к виду частных методик – она содержит практические рекомендации, и при этом является применимой для решения широкого круга частных задач КТЭ.

2.4 Требования законодательства к методике (и методам) производства экспертизы

Требования законодательства к методике и методам производства экспертизы в целом и КТЭ в частности, определяются основными процессуальными нормами, определенными УПК РФ в отношении судебной экспертизы, а также Федеральным законом №73 «О государственной судебно- экспертной деятельности в Российской Федерации».

Российское судопроизводство выдвигает следующий перечень требования к экспертному заключению:

1. Полнота – указание всех признаков; исследование в отношении всех поставленных вопросов; ответ на все поставленные вопросы; исследование всех объектов, предоставленных на исследование; исследование всех материалов, относящихся к предмету экспертизы; использование необходимых методик, обеспечивающих полноту исследования;
2. Объективность – применение объективно существующих специальных знаний; объективный подход к исследованию; использование научно обоснованных методик;
3. Всесторонность – изучение объекта со всех сторон, в т.ч. экспертная инициатива;
4. Достоверность – возможность проверки экспертного заключения на относимость (относимость установленного факта к предмету доказывания); допустимость (возможность допущения экспертного заключения, как средства доказывания – соблюдение процессуальных требований); достоверность; установление доказательного значения как факта.

Приведенный перечень требований к экспертному заключению определяет перечень требований к экспертной методике, с использованием которой оно дается. Экспертная методика должна обеспечивать полноту исследования, быть научно обоснованной, всесторонне исследовать объект и обеспечивать достоверность экспертного заключения, отвечать требованиям законности, быть безопасной, эффективной, экономичной, этичной, допустимой.

Законодательство не ограничивает эксперта в выборе методов исследования. Определяющим фактором при оценке того или иного метода на допустимость является научная обоснованность и удовлетворение метода новейшим достижениям области современных научных технологий. В мире информационных технологий, в отличие от многих видов классических экспертиз (например, почерковедческой, дактилоскопической), развитие науки и техники происходит очень быстро, что делает применение методик КТЭ десятилетней давности лишь ограниченно пригодными, в связи с появлением новых объектов, новых вопросов,

новых способов совершения преступлений. В этой ситуации приобретает большое

Допустимость методов КТЭ зависит также от их безопасности для эксперта, характера воздействия на объект исследования, времени получения результатов.

Методы КТЭ должны быть эффективны и рентабельны – они должны позволять решать задачу исследования в оптимальные сроки с наибольшей продуктивностью, ценность полученных результатов должна быть соизмерима с затраченными силами.

Объектами КТЭ «являются вещественные доказательства, которые согласно принципу непосредственности, действующему при судебном разбирательстве, необходимо представить в суд неизмененными» [22]. В связи чем, предпочтительным является использование неразрушающих (недеструктивных) методов проведения исследования. В методическом обеспечении КТЭ может быть использовано следующее разделение методов, в зависимости от степени сохранности объекта [23]:

1. Методы исследования компьютерных средств и систем, никак не влияющие на объект КТЭ и не требующие реализации процедур пробоподготовки;

2. Методы исследования компьютерных средств и систем, не разрушающие объект КТЭ, но изменяющие его состав, структуру или отдельные свойства;

3. Методы исследования компьютерных средств и систем, не разрушающие образец, но требующие для его изготовления разрушения или видоизменения объекта;

4. Методы исследования компьютерных средств и систем, полностью или частично разрушающие объект КТЭ или образец. Перечень задач и объектов КТЭ довольно разнороден, этот факт обусловливает большое количество экспертных методов и средств. Автором работы был детально рассмотрен целый ряд методик производства компьютерно-технической экспертизы, к сожалению, ни одна из них не 23 удовлетворяет полностью всем требованиям, выдвигаемым отечественном судопроизводством. В качестве примера, в следующем подразделе приведено описание преимуществ и недостатков основных существующих экспертных методик.

2.5 Анализ методик производства КТЭ

Ниже представлены результаты анализа ряда методик производства КТЭ. В ходе работы был проведен анализ большего количества методик, технической литературы, диссертационных работ [2, 3, 10, 14, 16, 23-51], но представлены результаты именно тех методик, которые наиболее часто используются экспертами при производстве КТЭ:

1. Результаты анализа методики, изложенной в [24]. Методическое обеспечение [24] рекомендовано эспертно-криминалистическим центром МВД России для проведения исследований и экспертиз по программам для ЭВМ на тер-

ритории Российской Федерации. В результате анализа данного источника информации установлено, что в представленной реализации он не может являться методическим пособием по производству КТЭ, так как не удовлетворяет требованиям, выдвигаемым отечественном судопроизводством.

Недостатками, ошибками и неточностями (исходя из требований к производству КТЭ и методикам судебной экспертизы[4-7]), являются:

1. Неточность трактовки понятий «эксперт» и «специалист».

2. Не полный перечень прав эксперта и возможных ходатайств эксперта.

3. Не указано, что согласно ч.3 ст.80 УПК, специалист дает заключение.

4. Указаны не все сведения, которые должны содержаться в заключение эксперта: не указано, что в заключение обязательно должна содержаться информация обо всех заявленных ходатайствах.

5. Указаны не все сведения, которые должны содержаться в постановлении/определении о назначении экспертизы - не указано, что в постановлении/определении обязательно должно быть указано: место и время; лицо назначившее экспертизу; номер дела; какая назначена экспертиза; объекты, предоставленные на экспертизу; права и обязанности эксперта, подписка.

6. Фраза: «Каждый эксперт вправе подписать общее заключение либо ту его часть, которая отражает ход и результаты проведенных им лично исследований», является неверной, так как при производстве комплексной экспертизы общий (совместный) вывод формулируют эксперты компетентные в оценке полученных результатов и формулировании общих выводов [4]. Если при этом им необходимы данные других экспертов, то они вправе их использовать, указывая на это.

7. Требование к вопросам, выносимым на экспертизу («вопросы должны соответствовать уровню подготовки и инструментальному оснащению экспертов того экспертного учреждения, которому назначается экспертиза»), является ложным. Экспертиза, назначается, тогда когда в деле возникают вопросы, требующие специальных знаний, основная цель экспертизы [4] – помочь разобраться суду, следователю, дознавателю и участникам процесса в сложной ситуации. Если же в экспертной организации нет необходимой материально-технической базы или эксперт недостаточно компетентен, то экспертной организацией/экспертом должно быть дано сообщение о невозможности дать заключение [4];

8. При указании задач, для решения которых могут потребоваться специальные знания в области компьютерной информации, указано «установление стоимости экземпляров произведений». Данное утверждение является ошибочным, так как при производстве КТЭ не решаются вопросы установления стоимости объектов [52];

9. При отсутствии технической возможности или целесообразности копирования информации» вариант исследования информации с применением блокираторов даже не рассматривается, то есть безальтернативно предлагается исследование разрушающими методами;

10. В данном методическом пособии отсутствуют рекомендации по программному обеспечению, которое возможно использовать при решении экспертных задач.

Данное методическое пособие имеет и свои преимущества:

1. Указаны преимущества и недостатки некоторых методов исследования (исследование клона/копии или непосредственно самого объекта);

2. Содержится: перечень типовых следственных ситуаций; задачи, для решения которых могут потребоваться специальные знания в области компьютерной информации, по каждой следственной ситуации (хотя некоторые из задач ошибочно отнесены к задачам КТЭ); наиболее целесообразные виды использования специальных знаний;

3. Обозначены ошибки, допускаемые экспертами КТЭ;

4. Указаны «внешние технические признаки контрафактности»

2. Результаты анализа методики, изложенной в [25]. Методические рекомендации [25] одобрены и рекомендованы к опубликованию Методическим и Редакционно-издательским советами ГУ ЭКЦ МВД России.

Данные методические рекомендации имеют ряд положений, которые остаются актуальными и после более чем десятка лет (задачи КТЭ, классификация видов КТЭ, классификация объектов КТЭ), но в целом требует дополнения в связи с развитием информационных технологий.

Несколько устарел перечень объектов КТЭ. Так, при описании аппаратных устройств, приводится описание такой «новой разработки», как ноутбук.

При описании основных видов операционных систем даже не упоминаются Windows XP/Vista/7/8/10; перечень основных видов файлов ограничен.

В разделе, содержащем указания по порядку выключения компьютера, не рассматриваются способы выключения в зависимости от операционной системы.

При описании краткого содержания экспертного исследования, на стадии исследования жесткого диска (накопителя на жестких магнитных дисках, НЖМД), не указана возможность проведения исследования непосредственно самого жесткого диска, без частичного разрушения информации – с использованием блокираторов записи.

Приведенный пример заключения эксперта содержит некоторые недочеты [4]: не указано время производства экспертизы, отсутствует описание примененных методик.

3. Результаты анализа методики, изложенной в [26]. Учебно-методическое пособие [26] подготовлено авторским коллективом Следственного комитета при МВД России и кафедры криминалистики юридического факультета МГУ им. М.В. Ломоносова. Это учебно- методическое пособие сильно устарело и в настоящее время применимо по большей части, как литература по истории развития КТЭ. Часть рекомендаций применима и в настоящее время, так как содержит указания по общим задачам КТЭ: виды следов преступной деятельности в ЭВМ; общие правила обращения с вычислительной техникой и носителями информа-

ции; упаковка объектов; особенности подготовки к проведению обыска; особенности выдвижения следственных версий.

Часть вопросов, отнесенных к вопросам КТЭ, не допустима для КТЭ в той редакции, в которой они указаны: «Кто разработчик данного обеспечения?»; «Имеют ли комплектующие компьютера (печатные платы, магнитные носители, дисководы и пр.) единый источник происхождения?»; «Являются ли данные программные продукты лицензионными (или несанкционированными) копиями стандартных систем или оригинальными разработками?»; «Какое время проходит с момента введения данных до вывода результатов при работе данной компьютерной программы, базы данных?»; 27 «Исправен ли компьютер и его комплектующие? Каков их износ?»; «Где и когда изготовлен, и собран данный компьютер и его комплектующие? Осуществлялась ли сборка компьютера в заводских условиях или кустарно?».

4. Результаты анализа методики, изложенной в [14]. Литература [14] не является экспертно-методическим пособием, но содержит ряд научно обоснованных и соответствующих современному уровню развития техники методических указаний по производству КТЭ. Как указано в аннотации: «Книга рассказывает о методах раскрытия и расследования компьютерных преступлений, правилах сбора, закрепления и представления доказательств по ним применительно к российскому законодательству. В книге имеются также сведения, относящиеся к гражданским делам, в которых затрагиваются информационные технологии, - таким как дела об авторских правах на программы для ЭВМ и иные произведения в электронной форме, дела о доменных именах, дела об использовании товарных знаков и других средствах индивидуализации в Интернете». Что наиболее важно, все это не просто описано в общих словах, а даны четкие, лаконичные рекомендации по практическим действиям в конкретной ситуации.

Н.Н. Федотовым отмечено, что «для полного понимания данной книги» необходимо владеть определенным уровнем знаний, этот момент отличает ее от трех вышеописанных источников, в которых практикуется популяризаторский подход (материал излагается поверхностно, не требует от читателя знания специальности). С точки зрения автора данной работы, книга [14] является хорошим вспомогательным инструментом для эксперта КТЭ, и при условии некоторых изменений (устранении/сокращении личностной оценки автора, более развернутом описании рекомендаций) может быть хорошей методикой КТЭ.

5. Результаты анализа методики, изложенной в [23]. Большая часть информации представляет собой теоретические основы КТЭ, без практических рекомендаций: теоретические и организационные основы использования специальных познаний в процессе судопроизводства по 28 делам, сопряженным с применением компьютерных средств; требования к методикам; особенности назначения КТЭ и т.п.

Для решения практических задач КТЭ этот источник минимально применим.

6. Результаты анализа методики, изложенной в [2]. В данном источнике представлены основы методического обеспечения КТЭ. Он является учебным посо-

бием в данной области, описаны теоретические вопросы КТЭ, большое внимание уделено практическим вопросам производства КТЭ. Указаны рекомендации по действиям эксперта, и подробное описание аппаратно-программного экспертного инструментария.

Описанные данные несколько устарели. Так описанный анализ ОС не содержит рекомендаций по анализу распространенных ОС Linux, Windows Vista/7/8/10, отсутствуют рекомендации по действиям эксперта при производстве экспертиз по «молодым» видам преступлений в сфере информационных технологий: «фишинг», «нарушение авторских прав в сети», «кардерство», и т.д. Но нельзя сказать, что данная литература в настоящее время не актуальна – с течением времени она лишь стала не достаточно полной.

Выводы по главе 2

Помимо вышеописанных основных методик производства КТЭ, приведенных выше автором в качестве примера, было исследовано большое количество технической литературы, посвященной вопросам КТЭ, авторские методики производства КТЭ, описанные в кандидатских работах, кандидатские работы, прямо либо косвенно связанные с производством КТЭ [2, 3, 10, 14, 16, 23-51]. В результате проведенного анализа был сделан следующий вывод [53]:

1. Существующие методики производства КТЭ не соответствуют полностью всем требованиям законодательства РФ [4-7];
2. Многие методики производства КТЭ практикуют популяризаторский подход;
3. Часть методик содержит смысловые ошибки;
4. Создание новой методики производства КТЭ является актуальным, необходимым, в настоящее время;
5. При создании новой методики производства КТЭ необходимо учитывать навыки как отечественных, так и зарубежных авторов.

3 МЕТОДИКА ПРОВЕДЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

Данная глава содержит описание разработанного методического и алгоритмического обеспечения производства КТЭ.

Разработанное методическое обеспечение производства КТЭ, разработанная методика, является унифицированной, т.к. применима для решения широкого круга частных задач, среди которых есть и диагностические, и классификационные, и идентификационные задачи. Т.е., согласно предложенной классификации, разработанная методика включает в себя следующие типы методик:

1. Методики производства КТЭ, направленные на решение диагностических задач, с целью ответа на вопросы, относящиеся к программным средствам;
2. Методики производства КТЭ, направленные на решение диагностических задач, с целью ответа на вопросы, относящиеся к данным (компьютерной информации);
3. Методики производства КТЭ, направленные на решение диагностических задач, с целью ответа на вопросы, относящиеся к вычислительным сетям и их элементам;
4. Методики производства КТЭ, направленные на решение классификационных задач, с целью ответа на вопросы, относящиеся к программным средствам;
5. Методики производства КТЭ, направленные на решение классификационных задач, с целью ответа на вопросы, относящиеся к данным (компьютерной информации);
6. Методики производства КТЭ, направленные на решение классификационных задач, с целью ответа на вопросы, относящиеся к вычислительным сетям и их элементам;
7. Методики производства КТЭ, направленные на решение идентификационных задач, с целью ответа на вопросы, относящиеся к аппаратным средствам;
8. Методики производства КТЭ, направленные на решение идентификационных задач, с целью ответа на вопросы, относящиеся к программным средствам;
9. Методики производства КТЭ, направленные на решение идентификационных задач, с целью ответа на вопросы, относящиеся к данным (компьютерной информации);
10. Методики производства КТЭ, направленные на решение идентификационных задач, с целью ответа на вопросы, относящиеся к вычислительным сетям и их элементам.

Разработанная методика является унифицированной и пригодной для ответа на любые вопросы КТЭ в случае ее использования в качестве общей методики производства КТЭ.

В случае использования разработанной методики в качестве частной, она является унифицированной, но имеющей ряд ограничений, связанных с описанием

в методике определенных частных методов, применимых для определенного круга объектов. Основное ограничение связано с применимостью методов методики для определенных ОС (Windows).

Разработанное методическое обеспечение производства КТЭ ориентировано на экспертов КТЭ частных и государственных экспертных учреждений. Оно содержит: рекомендации по выполнению стадий производства КТЭ и применению частных инструментальных методов: требования по оформлению экспертного заключения; описание структуры заключения эксперта о результатах производства КТЭ.

Методическое обеспечение предполагает использование пошаговых алгоритмов стадий производства КТЭ, разработанных на основе анализа графовых моделей производства КТЭ:

1. Подготовительной стадии;
2. Аналитической стадии;
3. Эксперимента;
4. Синтезирующей стадии;
5. Результативной стадии;
6. Стадии формирования выводов.

Предложенный поход создания пошаговых алгоритмов позволяет формализовать производство КТЭ и планировать ресурсы, необходимые для каждой из ее стадий.

3.1 Подготовительная стадия

Основной целью подготовительной стадии является уяснение экспертом экспертной задачи [10].

В ходе подготовительной стадии экспертом КТЭ выполняются следующие действия [4-7]:

1. Дается подписка о предупреждении об уголовной ответственности за дачу заведомо ложного заключения по ст.307 Уголовного кодекса Российской Федерации (УК РФ) [46] или об административной ответственности по ст.17.9 Кодекса Российской Федерации об административных правонарушениях (КоАП РФ) [47], а в необходимых случаях по ст.310 УК РФ – за разглашение данных предварительного расследования;
2. Изучается постановление/определение, рассматриваются поставленные вопросы;
3. Осуществляется изучение материалов дела;
4. Выполняется осмотр и описание объектов, предоставленных на экспертизу. При осмотре эксперт изучает общие признаки исследуемых объектов. Осмотр рекомендуется сопровождать фотосъемкой объектов при их поступлении в экспертное учреждение – в упаковке, и без упаковки, с целью фиксации внешних признаков исследуемых объектов;

5. После внешнего осмотра объектов осуществляется предварительный анализ информационного содержимого объектов с целью определения пригодности и достаточности объектов для ответа на вопросы экспертизы и определении методов исследования. Для этого объекты подключаются к тестовому компьютеру эксперта.

Перед подключением носителей информации к тестовому компьютеру должна быть обеспечена неизменность и сохранность информации. Так при подключении исследуемых НЖМД к тестовому компьютеру, для предотвращения утечки важной информации с подключаемого НЖМД должно быть осуществлено блокирование возможности сохранения данных на носителях, подключаемых к портам USB тестового компьютера. Блокирование возможности сохранения данных рекомендуется осуществлять аппаратными блокираторами, допускается блокирование возможности сохранения данных программными средствами (средствами экспертной ОС, специализированным ПО).

Для установления пригодности носителей информации для дальнейшего проведения исследования рекомендуется использование специализированного ПО. С этой целью для НЖМД возможно проведение тестирования на наличие сбойных кластеров (участков на поверхности диска, имеющих механическое, либо другое повреждение), например, с использованием программы HDDScan.

Программа автоматически тестирует все сектора диска и проверяет скорость считывания данных. Если отклик составляет <5мс, то сектор считается абсолютно рабочим. Сектора с откликами <20мс, <50мс, <150мс считаются рабочими, но для доступа к ним требуется соответствующее время. Сектора с откликом <500мс - очень плохие сектора. Пометкой «В» отмечаются сбойные сектора, доступ к которым невозможен.

6. Составляется рабочий план проведения исследования. Для этого проводится:

1. Пересмотр нормативных документов и законодательных актов (если требуется);

2. Определение возможности проведения экспертизы на основании:

3. Постановки цели, определении конечного результата проведения исследования;

4. Определении методов исследования;

5. Анализе применимости технической базы (программного обеспечения, оборудования) экспертного учреждения для решения конкретных поставленных задач;

6. Определение соответствия квалификации эксперта сложности вопросов решаемых в рамках конкретной экспертизы;

7. Анализ наличия среди ранее проведенных экспертиз аналогичных.

В случае наличия – использование плана ранее проведенных экспертиз в качестве шаблона. При отсутствии – составление индивидуального плана проведения экспертизы;

8. При необходимости использования на каком-либо из этапов разрушающих/ частично разрушающих методов исследования – подача соответствующего ходатайства лицу, назначавшему экспертизу;

9. В случае отклонения ходатайства – пересмотр методов проведения экспертизы. При невозможности проведения экспертизы без использования разрушающих/частично разрушающих методов – написание сообщения о невозможности проведения исследования.

7. На тестовом компьютере эксперта осуществляется подготовка рабочих зон. Под рабочими зонами будем понимать директории на тестовом компьютере эксперта, содержащие всю исследуемую информацию и информацию, имеющую доказательное значение в рамках дела. Подготовка рабочих зон осуществляется следующим образом:

1. Выполняется клонирование/копирование данных с предоставленных на экспертизу носителей информации на рабочую станцию эксперта (тестовый компьютер). При проведении анализа данных, содержащихся непосредственно на самом носителе, без их предварительного копирования на рабочую станцию эксперта, данный этап отсутствует;

2. На рабочей станции эксперта создается директория, в которой будут размещены файлы содержащие информацию, необходимую для ответа на поставленные вопросы;

3. На рабочей станции эксперта создается директория, в которой размещается информация, полученная с объектов, предоставленных на экспертизу, необходимая для проведения экспертизы, но в своем полном объеме не являющаяся доказательствами по делу. Таким образом, в данной директории могут быть размещены: полные образы носителей информации, все log-файлы, reg-файлы, история интернет-активности, index-файлы и т.д.;

Такая организация рабочих зон весьма удобна при работе с большим количеством информации, но не является обязательной.

При выборе экспертом между исследованием клонов/копий/образов и исследованием информации непосредственно на носителе, нужно руководствоваться тем, что в соответствии со стандартами криминалистики эксперты проводят исследование или анализ копий цифровых объектов – так исключается изменение или нарушение целостности данных оригинала.

Исследование непосредственно самого носителя возможно, в случае если такой вид исследования физически не может внести изменения в информацию (например, из-за особенностей носителя - DVD-R) или невозможно получение копии, пригодной для проведения исследования (в этом случае необходимо разрешение лица назначавшего экспертизу на применение частично разрушающих методов).

Копия исходных цифровых данных для исследования обычно называется образом. Для того чтобы этот образ являлся юридическим эквивалентом оригинала, он должен представлять собой абсолютную копию исходных данных. Сле-

довательно, каждый бит оригинала должны быть скопирован на образ. Существуют различные методы клонирования носителей информации.

Выбор того или иного метода обуславливается конкретной ситуацией.

Описание некоторых методов приведено ниже.

Клонирование с диска на диск в DOS. Этот способ клонирования (drive-to-drive) происходит полностью в ОС DOS, а исследуемый накопитель и накопитель для сохранения образа подключены к одной и той же системной плате. Достоинством этого метода является его простота, - требуется только загрузочный диск (например, Acronis или EnCase) и накопитель для сохранения образа. Многие эксперты, которые начали заниматься компьютерно-технической экспертизой много лет назад, когда этот метод клонирования считался стандартным, до сих пор предпочитают пользоваться им.

Клонирование с диска на диск - относительно быстрый способ дублирования данных. Ограничение скорости обычно связано с медленными компонентами в подсистеме ATA, будь то контроллер, кабель, конфигурация или скорость диска. Более быстрой конфигурацией обычно является «главный-главный» (master-to-master) на разных каналах (первичный и вторичный), более медленной - «главный-подчинѐнный» (master-to-slave) на одном и том же канале. Максимальная длина для таких кабелей - 18 дюймов, чем длиннее кабель, тем больше вероятность ошибки передачи данных при клонировании.

Клонирование данных по сети. Это еще один способ клонирования, который содержит в себе преимущества загрузки в DOS. Применение данного метода может помочь в следующих ситуациях:

1. Клонирование невидимых данных в области HPA или DCO. Столкнувшись с HPA или DCO, можно поместить этот накопитель в безопасный лабораторный компьютер и загрузить EnCase для DOS, при этом подключиться к своему рабочему компьютеру и запустить EnCase в среде Windows. Так же клонирование по сети пригодится для загрузки с исследуемого компьютера, когда не совпадает версия унаследованной BIOS (обычно на исследуемом компьютера) и новой BIOS (обычно на компьютере эксперта) или при работе с конфигурациями RAID. Применяя загрузку в DOS можно использовать родную конфигурацию аппаратного RAID для монтирования его как физического накопителя/устройства. EnCase распознаѐт этот RAID-массив как монтированный физический накопитель и позволяет выполнить его клонирование и предварительный просмотр (просмотреть логическую структуру) посредством подключения к EnCase в Windows через сетевой кабель;

2. Дублирование данных с НЖМД лэптопа. Иногда извлечение жѐсткого диска из лэптопа является сложной задачей из-за физического доступа или других проблем, таких как патентованная защищѐнная схема, с помощью которой накопитель подключѐн к системной плате. Если есть возможность получить доступ к BIOS и контролировать процесс загрузки, то клонирование по сети - очень удобная опция при значительной степени внимания и осторожности.

3. Быстрое клонирование данных. Способ клонирования по сети очень удобен для тайных операций, когда необходимо быстро создать образ целевого накопителя, пока его владелец отсутствует.

8. Результаты предварительного исследования и регламентированная информация об эксперте, экспертном учреждении, экспертизе отражаются в вводной и частично исследовательской частях заключения.

На подготовительной стадии в вводной части заключения указывается [4-7]:

1. Место и время производства экспертизы;
2. Основания производства;
3. Информация об экспертном учреждении, эксперте;
4. Отметка о предупреждении эксперта об уголовной ответственности;
5. Вопросы, поставленные на экспертизу;
6. Отметка о редакции вопроса (в случае редакции формулировки вопроса экспертом);
7. Информация об объектах, поступивших на исследование;
8. Предоставленные материалы дела, относящиеся к вопросам экспертизы;
9. Лица, присутствовавшие при производстве экспертизы (может быть указано/дополнено на последующих стадиях экспертизы);
10. Информация о заявленных ходатайствах, результаты их разрешения (может быть указано/дополнено на последующих стадиях экспертизы);
11. Отметка о производстве повторной или дополнительной экспертизы;
12. Использованная литература (может быть указано/дополнено на последующих стадиях экспертизы).

На подготовительной стадии в исследовательской части заключения указывается [4-7]:

1. Информация о результатах внешнего осмотра объектов;
2. Информация о результатах исследования информационного пространства носителей информации и их пригодности для проведения исследования;
3. Информация о выбранных методах исследования носителей информации.

3.2 Аналитическая стадия

На этой стадии выполняется тщательное исследование объектов.

Исследование выполняется с использованием аппаратно-программных средств – экспертного инструментария.

Аналитическая стадия состоит из двух этапов исследования – предварительного, направленного на получение общей информации об исследуемых объектах,

и основного, на котором происходит детальный анализ, с целью получения информации, имеющей значение для ответа на вопросы постановления/определения.

В рамках предварительного этапа исследования обобщается информация об объеме данных, их структуре, настройках, проводится экспресс-анализ данных, файлов, формируется представление об их виде. Так для НЖМД на предварительном этапе будут выполнены следующие действия (для прочих объектов исследование выполняется по аналогии):

1. Подсчет хеш-сумм (MD5, SHA) образца и копии;
2. Проверка физического размера диска и сравнение его с размером всех областей дискового пространства (в т.ч. DCA/ HPA);
3. Определение и сравнение размеров логических разделов с размером диска для определения информации об удаленных разделах или о неиспользуемом дисковом пространстве;
4. Получение информации о настройках временных зон для каждого диска и применение правильной зоны, если это возможно;
5. Переименование разделов НЖМД так, как это необходимо («C», «D» и т.д.);
6. Сбор системной информации:
    1. Определение типа ОС, SP, даты установки ОС; перечня установленных и запускаемых приложений; имени пользователя и имени компьютера, и т.п.;
    2. Получение информации о профиле пользователя (имя, SID , дата создания и последнего входа в систему);
7. Экспресс-анализ данных:
    1. Анализ сигнатуры файлов, просмотр переименованных файлов;
    2. Определение зашифрованных файлов;
    3. Определение и монтирование файлов-образов, контейнеров, архивов - VHD, VMDK, ZIP, RAR, Email-контейнеры, Reg-файлы и т.д.;
8. Проведение анализа включенных, работающих сервисов;
9. Проведение сканирования:
    1. Поиск и анализ вирусов;
    2. Поиск и анализ артефактов программ для стеганографии;
10. Поиск по ключевым словам:
    1. Составление списка ключевых слов;
    2. Формирование поискового запроса, с использованием синтаксиса выбранного поискового инструментария;
    3. Проведение поиска – целевого (в определенных директориях), всего пространства (включая нераспределенные области и удаленные разделы);
    4. Составление отчета по результатам поиска;
    5. Фильтрация данных (на основании метаданных – дата, время, расширение и т.д.);

В рамках основного этапа исследования выполняются следующие действия:

1. Анализ данных. Анализ файлов с использованием специализированного программного обеспечения. В качестве специализированного программного обеспечения может быть использован следующий экспертный инструментарий:

- анализ памяти;
- работа с паролями;
- ключи Shellbags реестра;
- интернет-активность;
- LNK –файлы;
- Event Logs - файлы (файлы формата .evt и .evtx);
- анализ MFT;
- анализ файлов Index.dat: Index.dat Analyzer – ПО, предназначенное для поиска и анализа файлов Index.dat;
- анализ e-mail сообщений;
- монтирование файлов-образов: ПО для монтирования файлов-образов определяется типом файла-образа (расширением). Так в зависимости от типа файла могут быть использованы следующие программы: FTK Imager, ImDisk Live, View OSFMount, Virtual Box, Acronis и т.д.;
- анализ артефактов программ стеганографии;
- подсчет хеш-сумм;
- работа с реестром ОС: Registry Recon. Windows Registry Recovery – программа, предназначенная для анализа и редактирования реестра. Имеется возможность работы с реестром активной и пассивной ОС.
- восстановление данных;
- выявления ПО с признаками контрафактности. Defacto – ПО, предназначенное для определения признаков использования ПО с нарушением исключительных прав: скомпрометированный серийный номер, наличие следов взлома технических средств защиты авторских прав (ТСЗАП) и т.д.

2. Анализ основных областей. Анализ основных областей выполняется для поиска артефактов и/или другой интересующей информации.

Примером основных областей являются:

- рабочий стол;
- директория пользователя;
- директория «Документы»;
- директория «Загрузки»;
- директория «Недавние места»;
- временные директории браузеров;
- директория System32;

3. Анализ системного реестра. Анализ системного реестра может помочь в получении многочисленной важной информации как о самой системе, как о приложениях, так и об активности пользователя. Например:

- версия ОС (ветка SOFTWARE);
- информация о последнем входе в систему (ветка SAM);
- имя пользователя и SID (ветка SAM);

- время последнего завершения работы (ветка SYSTEM);
- временная зона (ветка SYSTEM);
- носители, подключаемые пользователем (ветка SYSTEM);
- установленное программное обеспечение (ветка SOFTWARE);

4. Анализ артефактов ОС. В ОС имеется ряд артефактов, которые могут содержать важную информацию для ответа на вопросы экспертизы. К таким артефактам, например, относятся:

- резервные копии;
- файлы Event Logs (.evt, evtx);
- Shell bags;
- Jump Lists;
- LNK-файлы;
- Prefetch;
- PageFile;

5. Анализ следов работы программного обеспечения. Определение наличия программного обеспечения (например, Wiping tools, P2P, Sticky Notes, программное обеспечение для взлома и т.д.), анализ журналов (логов), настроек, реестра и т.д.;

6. Если есть возможность, то необходимо провести анализ временной информации, содержащейся в памяти.

7. Анализ переписки (e-mail, соц. сети). Для анализа информации о переписке пользователя необходимо выполнить:

- поиск установленных почтовых клиентов, архивов сообщений почтовых клиентов. Для анализа информации содержащейся в них используется либо почтовый клиент, либо специализированное программное обеспечение, предназначенное для просмотра файлов соответствующего типа;
- поиск установленных программ обмена мгновенными сообщениями (QIP, ICQ и т.д.), архивов сообщений;
- для анализа информации о переписке в социальных сетях (ВК, Facebook, Twitter и т.д.) производится анализ интернет-активности пользователя;

8. Анализ интернет-активности. Для анализа интернет-активности пользователя необходимо определить установленные браузеры и провести для них анализ артефактов, таких как:

- анализ файлов истории посещения (index.dat, sqlite и т.д.);
- анализ временных директорий;
- анализ куков (cookies);
- анализ кеша страниц;
- анализ избранного, закладок;
- анализ панели инструментов;
- анализ WebSlices;
- анализ плагинов;
- анализ системного реестра;
- анализ удаленной информации;

Ход проведения исследования, используемые методы фиксируются. В завершении стадии экспертом даются предварительные выводы. Сделанные на аналитической стадии выводы уточняются на последующих стадиях исследования.

Информация об уязвимости процессов переработки информации в информационных системах (важная при расследовании преступлений, связанных с нарушением информационной безопасности в открытых компьютерных сетях, хищением (разрушением, модификацией) информации и нарушением информационной безопасности) формируется именно на аналитической стадии. В соответствии с правилами производства экспертизы эксперты КТЭ в своем заключении отвечают на вопросы экспертизы и не дают рекомендаций по совершенствованию существующих средств защиты информации и обеспечения информационной безопасности. Если же это (рекомендации по совершенствованию существующих средств защиты информации и обеспечения информационной безопасности) является вопросом экспертизы, то данные рекомендации даются в результате ее обобщения на синтезирующей стадии.

Информация, полученная на аналитической стадии, излагается в тексте заключения КТЭ и может быть использована специалистами по информационной безопасности для совершенствования существующих средств защиты информации и обеспечения информационной безопасности.

3.3. Эксперимент

Наличие стадии эксперимента зависит от каждой конкретной ситуации, его форма базируется на задачах и целях экспертного исследования. Место и состав эксперимента определяются экспертом. Эксперимент может быть проведен как в экспертном учреждении, так и вне его. Эксперимент включает в себя следующие этапы:

- проектирование эксперимента;
- подготовка эксперимента;
- проведение эксперимента;
- подведение итогов эксперимента.

Экспертный эксперимент проводится экспертом в целях выявления механизма взаимодействия объектов экспертного исследования и (или) механизма следообразования, его отдельных параметров. В ходе экспертного эксперимента эксперт изучает, интересующие его процессы и условия.

В исследовательской части заключения эксперт должен подробно описать условия проведения эксперимента и его результаты. Результаты эксперимента оформляются в виде предварительных выводов по данной стадии.

3.4. Синтезирующая стадия

Данная часть исследования представляет собой обобщение информации, полученной на предыдущих стадиях экспертизы, интерпретацию артефактов. В зависимости от конкретных задач, решение которых необходимо для ответа на поставленные вопросы, рассматриваются определенные артефакты. Ниже приведен перечень основных частных задач (диагностических, идентификационных, классификационных) и артефактов, рассматриваемых для их решения в ОС семейства Windows на примере Win7. Для прочих ОС семейства Windows артефакты будут отличаться их расположением (адресом директорий и названием файлом), а для некоторых задач и составом. Подробная информация о составе и расположении артефактов содержится на официальном сайте компании-разработчика ОС.

1. Задача определения информации о загрузке файла. Артефакты:

- Open/Save MRU – Этот ключ фиксирует информацию об открытых или сохраненных файлах для многих приложений. Расположение (в случае стандартной конфигурации):

- Win7 NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\ ComDlg32\OpenSavePIDlMRU;

- Email – почтовые сообщения Outlook. Расположение: Win7 %USERPROFILE%\AppData\Local\Microsoft\Outlook.

- История Skype – история активности Skype содержит историю сессий чата и пересылки файлов. Сохраняется она по умолчанию в папке установки. Расположение: Win7 C:\Users\\AppData\Roaming\ Skype\

- Index.dat / places.sqlite - данные файлы содержат информацию об активности пользователя: о посещенных им сайтах, об открываемых файлах, о файлах, к которым было обращение;

- downloads.sqlite – это артефакт браузера Firefox, содержащий историю о загрузках файлов и посещенных сайтах. Расположение: Win7 %userprofile%\AppData\Roaming\Mozilla\ Firefox\Profiles\.default\downloads.sqlite

2. Задача определения информации об открытии/создании файла. Артефакты:

- Open/Save MRU (см. описание выше);

- Last Visited MRU- ключ реестра OpenSaveMRU, содержащий информацию об открытии файлов определенными приложениями. С его помощью можно определить информацию о том, какой файл был открыт приложением последним. Расположение: Win7 NTUSER.DAT\Software\ Microsoft\Windows\CurrentVersion\ Explorer\ComDlg32\ LastVisitedPidlMRU

- Последние документы – информация о последних открытых файлах и папках, отображаемая в меню Пуск, содержится в ключе системного реестра RecentDocs . Расположение: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\ Explorer\RecentDocs

- MS Office MRU – в системном реестре содержится информация о последних документах, открытых с использованием приложений Microsoft Office. Располагается она в ключе NTUSER.DAT\Software\Microsoft\

Office\VERSION, где 14.0 для Office 2010; 12.0 для Office 2007; 11.0 для Office 2003; 10.0 для Office XP;

- LNK – файлы – файлы-ярлыки. Эти файлы генерируются в ОС для последних открытых файлов. Расположение (могут быть обнаружены и в других директориях):

- Win7: C:\Users\\AppData\Roaming\Microsoft\ Windows\Recent\

- Win7 C:\Users\\AppData\Roaming\Microsoft\ Office\Recent\

- Index.dat (см. описание выше);

- JumpLists – информация о задачах, файлах отображаемая в панели задач Windows 7 (Jump List), расположенная по адресу C:\Users\\AppData\Roaming\ Microsoft\Windows\Recent\ AutomaticDestinations;

- Shellbags – ключи реестра, содержащие информацию о директориях. Информация в данных ключах сохраняется даже после удаления директории или отключения подключенного носителя. Расположение:

- Win7 USRCLASS.DAT\Local Settings\Software\Microsoft\ Windows\Shell\Bags

- Win7 USRCLASS.DAT\Local Settings\Software\Microsoft\ Windows\Shell\BagMRU

- Win7 NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU;

- Win7 NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags;

- Prefetch – файлы (.pf) могут быть использованы для определения информации о последних используемых файлах и устройствах, они располагаются в директории C:\Windows\Prefetch

3. Задача определения информации о файлах (задача поиска файлов), в т.ч. удаленных. Артефакты:

- Win7 Search WordWheelQuery – Артефакт, содержащий информацию о поисковых запросах, вводимых в меню «Пуск» в ОС Windows 7. Расположение: Win7 NTUSER.DAT Hive NTUSER.DAT\Software\Microsoft\Windows\ CurrentVersion\Explorer\WordWheelQuery;

- Thumbs.db – Артефакт, являющийся скрытым файлом Thumbs.db. Содержит информацию об изображениях, имеющихся и имевшихся в директории, т.е. даже после их удаления из нее. Артефакт располагается в любой директории, где были просмотрены изображения в режиме эскизов, многие камеры создают этот файл автоматически;

- WIn7 Thumbnails – В ОС Vista/Win7 файлы thumbs.db отсутствуют, информация сохраняется отдельно для каждого пользователя, в директории :\Users\\AppData\Local\Microsoft\ Windows\ Explorer\;

- Корзина – Анализ Корзины важен, т.к. зачастую значимые удаленные файлы были удалены именно через эту директорию. Расположение: Win7: Системная директория «Корзина»; C:\$Recycle.bin;

- Артефакты браузеров – эта группа артефактов будет рассмотрена ниже при описании артефактов задачи определения интернет-активности пользователя;

- Last visited MRU – см. описание выше;

4. Задача определения использования/подключения USB-устройств. Артефакты:

- Ключи реестра – ключи системного реестра, содержащие информацию о ранее подключаемых USB-устройствах. Расположены по адресу SYSTEM\CurrentControlSet\Enum\USBSTOR и SYSTEM\CurrentControlSet\Enum\USB;

- First / Last Time (недавно и давно подключаемые) – артефакты, содержащие информацию о подключении конкретных USB-устройств, их серийного номера, даты подключения. Расположение: Журнал Plug and Play (недавно подключаемые): Win7 C:\Windows\inf\setupapi.dev.log;

- Системный реестр: NTUSER.DAT ветка: NTUSER//Software/Microsoft/ Windows/CurrentVersion/ Explorer/MountPoints2/ ;

- Идентификация пользователя – если стоит задача определения пользователя, которым было подключено USB-устройство, то необходимо проанализировать:

-GUID пользователей в ключе реестра SYSTEM\Mounted Devices; Ключ реестра NTUSER.DAT\Software\Microsoft\Windows\ CurrentVersion\Explorer\MountPoints2 ;

- Имя раздела – информация об имени, присвоенном носителю при подключении, может быть определена при анализе артефактов системного реестра, расположенных в нем по адресу: Win7 : SOFTWARE\Microsoft\Windows Portable Devices\Devices и SYSTEM\MountedDevices;

- LNK Files – см. описание выше;

- Event Logs – информация об установке Plug and Play драйверов логируется (журналируется) в системном журнале Windows. Важно отметить, что сохраняется информация о подключении не только для USB-устройств.

5. Задача определения информации о запуске программ. Артефакты:

- User Assist – артефакт запуска графических приложений, содержащийся в системном реестре по адресу: NTUSER.DAT\Software\Microsoft\Windows\ Currentversion\ Explorer\UserAssist\{GUID}\Count;

- LastVisited MRU – см. описание выше;

- Run MRU (Start->Run) – артефакт, образующийся в результате запуска кем-либо команд открыть, запустить. Он расположен в системном реестре по адресу NTUSER.DAT\Software\Microsoft\Windows\ CurrentVersion\ Explorer\RunMRU;

- Prefetch – см. описание выше;

- Jump Lists – см. описание выше;

- Event Logs – артефакты о запуске программ, содержащиеся в системном журнале Windows;

6. Задача определения физического нахождения (локализации) пользователя. Артефакты:

- Time Zone (временная зона) – артефакт, расположенный в системном реестре, и содержащий информацию о временной зоне. Расположение: SYSTEM\CurrentControlSet\Control\ TimeZoneInformation; Vista/W7 Network History – артефакт, содержащий информацию о сетевых подключениях компьютера, типе сети (проводная, беспроводная), и т.д. Расположение: SOFTWARE\Microsoft\Windows NT\CurrentVersion\ NetworkList\Signatures\Unmanaged; SOFTWARE\Microsoft\Windows NT\CurrentVersion\ NetworkList\Signatures\Managed; SOFTWARE\Microsoft\Windows NT\CurrentVersion\ NetworkList\Nla\Cache;

- Cookies – артефакт, анализируемый для получения информации о посещенных пользователем сайтах. Для разных браузеров располагаются в разных директориях;

- Search Terms (поисковые запросы в браузерах) – артефакт, содержащий информацию о дате и времени посещения сайтов, количестве посещений, поисковых запросах. Он расположен для разных браузеров в разных директориях.

- IP-адрес – информация об IP-адресе, которая, например, может быть получена из системного реестра, используется для определения нахождения пользователя;

7. Задача определения информации об учетной записи. Артефакты:

- Информация о смене пароля – артефакты, содержащие информацию о последней смене пароля пользователем, расположены в C:\windows\system32\config\SAM и системном реестре по адресу SAM\Domains\Account\Users;

- Успешная/неуспешная авторизация – артефакты, содержащие информацию об успешных авторизациях и ее попытках (неуспешных авторизациях), расположены в системном журнале по адресу: Win7 %system root%\System32\winevt\logs\ Security.evtx ;

- Системный журнал – подробная информация об учетной записи, запуске ОС, приложений, установке приложений, сетевых соединениях содержится в системном журнале ОС;

- RDP-соединения – артефакт, содержащий информацию о соединениях по протоколу RDP (в т.ч. информацию об IP-адресе устройства, подключившегося по RDP) и расположенный по адресу: Win7 %system root%\System32\winevt\logs\Security.evtx;

- Авторизация пользователя – артефакты, содержащие информацию об авторизации пользователя в ОС, расположены по адресу C:\windows\system32\config\SAM и в системном реестре: SAM\Domains\Account\Users;

8. Задача определения интернет-активности пользователя.

- Браузер Internet Explorer (IE) предоставляется вместе с ОС Microsoft Windows, как составная часть инсталляционного пакета ОС. Артефактами IE являются:

- Файлы index.dat. Данные файлы содержат записи о доступе к url, включая поисковые запросы, доступ к Веб-почте. Данный артефакт часто считается основным источником судебной информации при анализе IE браузера.

- «Избранное» IE. «Избранное» - закладки в Internet Explorer, оставленные пользователем при движении в сети. «Избранное» пользователя можно найти (в Windows XP) в директории :\Documents and Settings\user\Favorites. Помимо содержимого «Избранного» эксперт может найти ценную информацию в файле MAC times. Данный файл иллюстрирует время создания файла, время последнего доступа к файлу, время внесения последних изменений.

- Cookies IE. Cookies Internet Explorer находятся по пути Users\%username%\AppData\Roaming\Microsoft\Windows\Cookies (в ОС Vista и Windows 7). IE представляет cookies пользователя виде текстовых файлов - они могут быть просмотрены непосредственно.

- Cache IE (кэш). Кэш браузера - это файлы, которые остаются в системе, в результате активности пользователя в сети Internet. В Windows Vista и Windows 7 -Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5.

- Браузер Mozilla's Firefox – это второй по популярности браузер в мире после Internet Explorer. Firefox 3 сохраняет данные истории в файлы базы данных SQLite 3, которые достаточно просто просматриваются с помощью инструментов с открытым исходным кодом. Formhistory.sqlite: содержит данные, вводимые пользователем. Эти данные включают в себя: имена, адреса, адреса электронной почты, номера телефонов, Веб-почту, поисковые запросы. Downloads.sqlite: содержит данные о загружаемых файлах. Cookies.sqlite: содержит данные о cookies. Places.sqlite: содержит данные «Internet history» (данные Internet-активности пользователя). Cache (кэш). В различных операционных системах кэш Firefox сохраняется в разных местах: ОС Windows Vista/7 - :\Users\%username%\AppData\Roaming\Mozilla\Firefox\ Profiles; ОС Linux - /home/$username/.mozilla/firefox/Profiles.

- Сохраненные данные сессии. При некорректном завершении работы с браузером (Н-р: отключение электричества) создается файл sessionstore.js в директории профиля пользователя. Данный файл содержит информацию, необходимую браузеру для восстановления сессии. Для более комфортного анализа информации данного файла наиболее предпочтительно использование не текстового программного редактора, а просмотрщика. В качестве просмотрщика может быть использовано программное обеспечение с открытым исходным кодом, например JSON Viewer.

- Расширения. Firefox поддерживает установку расширений, которые могут улучшить или изменить работу с браузером Данные расширения содержатся в файле extensions.rdf, в каталоге пользователя. Иногда эти данные также полезны при производстве экспертизы. Chrome – это браузер, разработанный Google, и являющийся программным обеспечением с открытым исходным кодом. Об артефактах в Chrome: Как в Firefox, так и в Chrome для хранения данных

пользователя используются базы данных SQLite. В различных ОС база данных хранятся в различных местах: в Windows Vista/7 – :\Users\%username%\AppData \Local\Google\Chrome\Default; в Linux – /home/$username/.config/google-chrome/Default.

- «Cookies» - это база данных SQLite, используемая для ведения истории cookies. Информация, содержащаяся в этой базе данных, содержит информацию о времени создания файла cookie, времени последнего доступа к нему и хост-файле cookie.

- «History» – это база данных SQLite, содержащая наиболее интересную информацию об активности пользователя, поделенную на таблицы.

Наибольший интерес представляют таблицы: «downloads», «urls», «visits».

- «Login Data» – это база данных SQLite, содержащая информацию о сохраненных учетных данных. В ОС Linux здесь может содержаться информация о паролях.

- «Web Data» – это база данных SQLite, содержащая информацию, сохраненную пользователям для осуществления возможности авто-заполнения.

Эта информация может включать информацию об именах, адресах, номерах кредитных карт, и т.д.

- «Thumbnails» – это база данных SQLite, содержащая миниатюры изображений, посещенных сайтов.

- «Bookmarks» – это файл, содержащийся в директории профиля пользователя и содержащий закладки пользователя в браузере. Этот файл содержит объекты JSON и может быть просмотрен с помощью любого JSON-просмотрщика или просто текстовым редактором.

- «Local State» - этот файл используется для восстановления работы в Chrome после некорректного завершения работы. Файл содержит объекты JSON.

-Cache (кэш) в Chrome представлен виде index-файла, четырех пронумерованных файлов данных (от data_0 до data_3) и множества файлов, начинающихся с f_ и оканчивающихся на комбинацию из шести шестнадцатеричных цифр.

3.5. Результативная стадия

Результативная стадия – это стадия, на которой происходит подведение итогов, оцениваются результаты проведенных исследований. На данной стадии выполняется окончательное оформление исследовательской (и если требуется вводной) части заключения.

3.6. Формирование выводов

Формирование выводов – на этой стадии оформляются выводы по экспертизе. Результаты этой стадии оформляются в разделе заключения «Выводы». В Выво-

дах должны быть обязательно отражены все вопросы экспертизы и ответы на них.

Вывод по каждому вопросу должен быть развернутым, желательно указание ссылок на пункты, страницы исследовательской части, исходя из которых, сделаны выводы.

3.7. Заключение эксперта

Согласно требованиям законодательства, в заключении эксперта обязательно указываются [3-7]:

1. Дата, время и место производства судебной экспертизы;
2. На основании чего производится судебная экспертиза;
3. Информация о должностном лице, назначившем судебную экспертизу;
4. Информация об экспертном учреждении и эксперте (ФИО эксперта, специальность, образование, занимаемая должность, стаж работы, ученая степень и (или) ученое звание);
5. Информация о предупреждении эксперта об ответственности за дачу заведомо ложного заключения;
6. Вопросы, поставленные на разрешение экспертизы;
7. Объекты исследований и материалы, представленные для производства судебной экспертизы;
8. Данные о лицах, которые присутствовали при производстве экспертизы;
9. Состав и результаты исследований с перечнем использованных методик;
10. Выводы по вопросам, поставленным перед экспертом, и их обоснование.

В случае необходимости экспертом подаются ходатайства (ходатайства могут быть заявлены на любой стадии исследования):

1. Об ознакомлении с материалами дела, имеющими отношение к предмету экспертизы;
2. О предоставлении дополнительных материалов, имеющих отношение к экспертизе;
3. О привлечении другого эксперта;
4. Об участии в процессуальных действиях;
5. О применении разрушающих/ частично разрушающих методов;

Информация о поданных ходатайствах и их разрешении отображается в заключении.

Эксперт вправе отказаться от дачи заключения в случае выявления на любой стадии исследования следующих обстоятельств:

1. Эксперт не обладает достаточной компетентностью для решения поставленных задач;
2. В экспертном учреждении отсутствует материально-техническая база, необходимая для проведения исследования;

3. Недостаточно данных после заявленных ходатайств;
4. Нет данных науки для решения поставленных вопросов.

В случае отказа от дачи заключения экспертом оформляется сообщение о невозможности проведения исследования

3.8. Оценка эффективности разработанной методики производства экспертизы

Говоря об эффективности методики, под эффективностью будем понимать возможность эксперта с ее помощью выполнять работу (производить КТЭ) и достигать необходимого или желаемого результата с наименьшей затратой времени и других ресурсов.

Как было сказано ранее, требования законодательства к методике и методам производства экспертизы в целом и КТЭ в частности, определяются основными процессуальными нормами, определенными УПК РФ в отношении судебной экспертизы, и Федеральным законом №73 «О государственной судебно-экспертной деятельности в Российской Федерации». Экспертная методика должна обеспечивать полноту исследования, быть научно обоснованной, всесторонне исследовать объект и обеспечивать достоверность экспертного заключения, отвечать требованиям законности, быть безопасной, этичной, допустимой, эффективной, экономичной [3, 21]. Все требования можно условно разделить на две группы – требования, влияющие на допустимость экспертного заключения, как средства доказывания, и требования, влияющие на конечную стоимость производства экспертизы, ее время и требуемую квалификацию экспертов. На то, будут ли назначены по проведенной экспертизе повторные и дополнительные экспертизы, влияет первая группа требований (к ней относятся все требования кроме требования к экономичности). Вторая группа требований влияет на стоимость и сроки производства экспертизы (это требования к эффективности и экономичности).

Как видно, требование к эффективности включает в себя одновременно и качественные требования (допустимость производства экспертизы) и количественные (стоимость и сроки производства экспертизы).

Рассмотренные в ходе выполнения работы методики используются при производстве экспертиз по гражданским, арбитражным и уголовным делам. Общепринятой практикой является применение при производстве одной экспертизы одновременно нескольких методик. Такой комплексный подход предполагает использование экспертом преимуществ различных методик для каждой конкретной экспертизы. По некоторым из экспертиз при этом назначаются повторные и дополнительные экспертизы, т.к. большое значение в таком подходе играет опыт эксперта. При этом сам подход являются допустимым судом для производства КТЭ.

Наиболее опытные эксперты используют комплексный подход, добиваясь на нем большей эффективности. Потому сравнение разработанной методики будем производить с ним.

Разработанная методика по сравнению с комплексным подходом позволяет добиться выигрыша по следующей группе критериев, гарантируя получение даже экспертом низкой квалификации экспертного заключения, соответствующего требованиям законодательства:

- время разработки частной методики КТЭ (относительно общепринятой методики) – меньше на 20-40%;
- сроки производства экспертизы (относительно общепринятой методики) – меньше на 10-25%;
- стоимость производства (относительно общепринятой методики) – меньше на 10-30%.

По заключениям, выполненным в соответствии с разработанной методикой, не было назначено повторных или дополнительных экспертиз.

Выводы по главе 3

Таким образом, в данной главе показано разработанное методическое и алгоритмическое обеспечение производства КТЭ.

Разработанное методическое обеспечение производства КТЭ ориентировано на экспертов КТЭ частных и государственных экспертных учреждений. Оно содержит: рекомендации по выполнению стадий производства КТЭ и применению частных инструментальных методов: требования по оформлению экспертного заключения; описание структуры заключения эксперта о результатах производства КТЭ.

Методическое обеспечение предполагает использование пошаговых алгоритмов стадий производства КТЭ, разработанных на основе анализа графовых модели производства КТЭ.

Разработанная методика по сравнению с комплексным подходом позволяет добиться выигрыша по следующей группе критериев, гарантируя получение даже экспертом низкой квалификации экспертного заключения, соответствующего требованиям законодательства:

- время разработки частной методики КТЭ (относительно общепринятой методики) – меньше на 20-40%;
- сроки производства экспертизы (относительно общепринятой методики) – меньше на 10-25%;
- стоимость производства (относительно общепринятой методики) – меньше на 10-30%.

Разработанное методическое и алгоритмическое обеспечение может быть использовано для автоматизации и упрощения процесса разработки частных мето-

дик производства КТЭ путем разработки системы поддержки формирования частных методик производства КТЭ (СП).

4 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

В связи с тем фактом, что работа с информационной системой производится с использованием средств вычислительной техники, необходимо обеспечить соответствие рабочих мест сотрудников телерадиокомпании действующим нормам стандартов по безопасности жизнедеятельности. Требования санитарных правил направлены на предотвращение неблагоприятного влияния на здоровье человека вредных факторов производственной среды и трудового процесса при работе с ПЭВМ.

4.1. Общие требования к организации рабочих мест пользователей

Рабочее место оператора ЭВМ проектируется согласно СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

1. При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов - не менее 1,2 м;
2. Рабочие места с ПЭВМ при выполнении творческой работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5 - 2,0 м;
3. Экран видеомонитора должен находиться от глаз пользователя на расстоянии 600 - 700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов;
4. Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0,5 - 0,7;
5. Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПЭВМ, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ. Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию;
6. Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений;

7. Высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах 680 - 800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм;

8. Модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, равной 725 мм;

9. Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной - не менее 500 мм, глубиной на уровне колен - не менее 450 мм и на уровне вытянутых ног - не менее 650 мм;

10. Конструкция рабочего стула должна обеспечивать:

- ширину и глубину поверхности сиденья не менее 400 мм;
- поверхность сиденья с закругленным передним краем;
- регулировку высоты поверхности сиденья в пределах 400 - 550 мм и углам наклона вперед до 15 град, и назад до 5 град.;
- высоту опорной поверхности спинки 300 +-20 мм, ширину - не менее 380 мм и радиус кривизны горизонтальной плоскости - 400 мм;
- угол наклона спинки в вертикальной плоскости в пределах +-30 градусов;
- регулировку расстояния спинки от переднего края сиденья в пределах 260 - 400 мм;
- стационарные или съемные подлокотники длиной не менее 250 мм и шириной - 50 - 70 мм;
- регулировку подлокотников по высоте над сиденьем в пределах 230 +-30 мм и внутреннего расстояния между подлокотниками в пределах 350 -500 мм;

11. Рабочее место пользователя ПЭВМ следует оборудовать подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20°. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм;

12. Клавиатуру следует располагать на поверхности стола на расстоянии 100 - 300 мм от края, обращенного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

4.2. Требования к помещениям для размещения рабочего места

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное помещение в котором будут располагаться рабочие места, оборудование ЭВМ с ВДТ.

По требованиям СанПиН 2.2.2/2.4.1340-03 помещения для эксплуатации ПЭВМ должны отвечать следующим требованиям:

1. Помещения для эксплуатации ПЭВМ должны иметь естественное и искусственное освещение;

2. Естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации. Оконные проемы должны быть оборудованы регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и др.;

3. Площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные), должна составлять не менее 4,5 м2;

4. Для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка - 0,7 - 0,8; для стен - 0,5 - 0,6; для пола - 0,3 - 0,5;

5. Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации;

6. Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПЭВМ.

4.3. Требования к уровням шума на рабочих местах

Уровень шума на рабочих местах, при выполнении основных и вспомогательных производственных работ с использованием ПЭВМ не должен превышать показателей, устанавливаемых нормами СанПиН 2.2.2/2.4.1340-03 предельно допустимых значений для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами. А именно должен соответствовать нормам СанПиН 2.2.4.3359-16 для высококвалифицированной работы, требующей сосредоточенности, в рабочих комнатах. Источниками шума в данной организации являются рабочие станции и сервер. На основании СанПиН 2.2.4.3359-16, нормативным эквивалентным уровнем звука на рабочих местах является 80 дБА. В соответствии с нормами, ограничивающими предельно допустимое звуковое давление для рабочих мест, оснащенных ПЭВМ: шумящее оборудование, уровни шума которого превышают нормативные, должно размещаться вне помещений ПЭВМ.

4.4. Требования к освещению на рабочих местах

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное освещение, не вызывающее раннего переутомления.

Согласно СанПиН 2.2.2/2.4.1340-03, есть следующие требования к освещению на рабочих местах:

1. Рабочие столы следует размещать таким образом, чтобы видеодисплейные терминалы были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева;

2. Искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения. В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами, следует применять системы комбинированного освещения;

3. Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300 - 500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк;

4. Следует ограничивать прямую блесткость от источников освещения, при этом яркость светящихся поверхностей (окна, светильники и др.), находящихся в поле зрения, должна быть не более 200 кд/м.

5. Яркость светильников общего освещения в зоне углов излучения от 50 до 90° с вертикалью в продольной и поперечной плоскостях должна составлять не более 200 кд/м , защитный угол светильников должен быть не менее 40°.

6. Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя при рядном расположении видеодисплейных терминалов. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору;

7. Коэффициент пульсации не должен превышать 5%;

8. Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

4.5. Требования к микроклимату

Для рабочих мест, на которых работа с ПЭВМ является основным видом выполняемых работ и связана с непрерывным эмоциональным напряжением, согласно СанПиН 2.2.2/2.4.1340-03 должны быть обеспечены оптимальные параметры микроклимата для работ категории 1а.

Нормативные требования к показателям микроклимата рабочих мест производственных помещений приведены в СанПиН 2.2.4.3359-16 «Санитарно-эпидемиологические требования к физическим факторам на рабочих местах» .

Оптимальные величины параметров микроклимата для категории работ 1а приведены в таблице 1.

В соответствии с СанПиН 2.2.2/2.4.1340-03, в помещениях, оборудованных ПЭВМ, должна проводиться ежедневная влажная уборка, а также проветривание после каждого часа работы на ПЭВМ.

Таблица 1 – Оптимальные величины параметров микроклимата

Период года	Категория работ по уровням энергозатрат, Вт	Температура воздуха, °С	Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	1а (до 139)	22−24	21−25	60−40	0,1
Теплый	1а (до 139)	23−25	22−26	60−40	0,1

4.6. Требования к электробезопасности

По степени опасности поражения электрическим током согласно Правилам Устройства Электроустановок (ПУЭ) рабочее помещение относится к классу помещений с повышенной опасностью, так как имеется возможность одновременного прикосновения человека к имеющим соединения с землей металлоконструкциям здания с одной стороны и металлическим корпусам электрооборудования с другой.

Если физический доступ к токоведущим частям оборудования затруднен, то основной причиной возникновения данного опасного фактора может являться прикосновение к металлическим нетоковедущим частям (например, корпусу ПЭВМ), которые могут оказаться под напряжением в результате повреждения изоляции. В соответствии с правилами электробезопасности, должен осуществляться постоянный контроль состояния электропроводки, предохранительных щитов, шнуров, с помощью которых включаются в электросеть компьютеры, осветительные приборы, другие электроприборы.

Для предотвращения образования и защиты от статического электричества в помещениях с ПЭВМ необходимо использовать аэроионизаторы и увлажнители воздуха. В отделке помещений следует отдавать предпочтение антистатическим материалам. Полы должны иметь антистатическое покрытие.

Согласно документу «Правила устройства электроустановок» (ПУЭ) электробезопасность работающих обеспечивается конструкцией электроустановок; техническими способностями и средствами защиты, организационными средствами защиты. Предусмотрены следующие технические способы и средства защиты от поражения электрическим током:

1. Обеспечение недоступности токоведущих частей, находящихся под напряжением для случайного прикосновения;

2. Устранение опасности поражения при появлении напряжения на нетоковедущих частях электрооборудования посредством заземления (зануления).

4.7. Пожарная безопасность

Постановление Правительства РФ от 25.04.2012 N 390 (ред. от 21.03.2017) "О противопожарном режиме" устанавливают следующие правила:

1. В отношении каждого объекта (за исключением индивидуальных жилых домов) руководителем (иным уполномоченным должностным лицом) организации (индивидуальным предпринимателем), в пользовании которой на праве собственности или на ином законном основании находятся объекты (далее - руководитель организации), утверждается инструкция о мерах пожарной безопасности в соответствии с требованиями;

2. Лица допускаются к работе на объекте только после прохождения обучения мерам пожарной безопасности;

3. Лица допускаются к работе на объекте только после прохождения обучения мерам пожарной безопасности;

4. Обучение лиц мерам пожарной безопасности осуществляется путем проведения противопожарного инструктажа и прохождения пожарно-технического минимума;

5. Порядок и сроки проведения противопожарного инструктажа и прохождения пожарно-технического минимума определяются руководителем организации. Обучение мерам пожарной безопасности осуществляется в соответствии с нормативными документами по пожарной безопасности;

6. Руководитель организации назначает лицо, ответственное за пожарную безопасность, которое обеспечивает соблюдение требований пожарной безопасности на объекте;

7. В складских, производственных, административных и общественных помещениях, местах открытого хранения веществ и материалов, а также размещения технологических установок руководитель организации обеспечивает наличие табличек с номером телефона для вызова пожарной охраны;

8. На объекте с массовым пребыванием людей (кроме жилых домов), а также на объекте с рабочими местами на этаже для 10 и более человек руководитель организации обеспечивает наличие планов эвакуации людей при пожаре;

9. На объекте с массовым пребыванием людей руководитель организации обеспечивает наличие инструкции о действиях персонала по эвакуации людей при пожаре, а также проведение не реже 1 раза в полугодие практических тренировок лиц, осуществляющих свою деятельность на объекте;

10. Хранение огнетушителя осуществляется в соответствии с требованиями инструкции по его эксплуатации;

11. Запрещается на территориях, прилегающих к объектам, в том числе к жилым домам, а также к объектам садоводческих, огороднических и дачных не-

коммерческих объединений граждан, оставлять емкости с легковоспламеняющимися и горючими жидкостями, горючими газами;

12. Руководитель организации обеспечивает наличие на дверях помещений производственного и складского назначения и наружных установках обозначение их категорий по взрывопожарной и пожарной опасности;

13. Руководитель организации обеспечивает устранение повреждений толстослойных напыляемых составов, огнезащитных обмазок, штукатурки, облицовки плитными, листовыми и другими огнезащитными материалами, в том числе на каркасе, комбинации этих материалов, в том числе с тонкослойными вспучивающимися покрытиями строительных конструкций, горючих отделочных и теплоизоляционных материалов, воздуховодов, металлических опор оборудования и эстакад, а также осуществляет проверку состояния огнезащитной обработки (пропитки) в соответствии с инструкцией завода-изготовителя с составлением протокола проверки состояния огнезащитной обработки (пропитки). Проверка состояния огнезащитной обработки (пропитки) при отсутствии в инструкции сроков периодичности проводится не реже 1 раза в год;

14. Руководитель организации организует проведение работ по заделке негорючими материалами, обеспечивающими требуемый предел огнестойкости и дымогазонепроницаемость, образовавшихся отверстий и зазоров в местах пересечения противопожарных преград различными инженерными (в том числе электрическими проводами, кабелями) и технологическими коммуникациями;

15. На объектах запрещается:

15.1. Хранить и применять на чердаках, в подвалах и цокольных этажах легковоспламеняющиеся и горючие жидкости, порох, взрывчатые вещества, пиротехнические изделия, баллоны с горючими газами, товары в аэрозольной упаковке, целлулоид и другие пожаровзрывоопасные вещества и материалы, кроме случаев, предусмотренных иными нормативными документами по пожарной безопасности;

15.2. Использовать чердаки, технические этажи, вентиляционные камеры и другие технические помещения для организации производственных участков, мастерских, а также для хранения продукции, оборудования, мебели и других предметов;

15.3. Размещать в лифтовых холлах кладовые, киоски, ларьки и другие подобные помещения;

15.4. Устраивать в подвалах и цокольных этажах мастерские, а также размещать иные хозяйственные помещения, размещение которых не допускается нормативными документами по пожарной безопасности, если нет самостоятельного выхода или выход из них не изолирован противопожарными преградами от общих лестничных клеток;

15.5. Снимать предусмотренные проектной документацией двери эвакуационных выходов из поэтажных коридоров, холлов, фойе, тамбуров и лестничных клеток, другие двери, препятствующие распространению опасных факторов пожара на путях эвакуации;

15.6. Производить изменение объемно-планировочных решений и размещение инженерных коммуникаций и оборудования, в результате которых ограничивается доступ к огнетушителям, пожарным кранам и другим системам обеспечения пожарной безопасности или уменьшается зона действия автоматических систем противопожарной защиты (автоматической пожарной сигнализации, стационарной автоматической установки пожаротушения, системы дымоудаления, системы оповещения и управления эвакуацией);

15.7. Загромождать мебелью, оборудованием и другими предметами двери, люки на балконах и лоджиях, переходы в смежные секции и выходы на наружные эвакуационные лестницы, демонтировать межбалконные лестницы, заваривать и загромождать люки на балконах и лоджиях квартир;

15.8. Проводить уборку помещений и стирку одежды с применением бензина, керосина и других легковоспламеняющихся и горючих жидкостей, а также производить отогревание замерзших труб паяльными лампами и другими способами с применением открытого огня;

15.9. Остеклять балконы, лоджии и галереи, ведущие к незадымляемым лестничным клеткам;

15.10. Устраивать в лестничных клетках и поэтажных коридорах кладовые и другие подсобные помещения, а также хранить под лестничными маршами и на лестничных площадках вещи, мебель и другие горючие материалы;

15.11. Устраивать в производственных и складских помещениях зданий (кроме зданий V степени огнестойкости) антресоли, конторки и другие встроенные помещения из горючих материалов и листового металла;

15.12. Устанавливать в лестничных клетках внешние блоки кондиционеров;

15.13. Загромождать и закрывать проходы к местам крепления спасательных устройств;

16. Руководитель организации обеспечивает содержание наружных пожарных лестниц и ограждений на крышах (покрытиях) зданий и сооружений в исправном состоянии, организует не реже 1 раза в 5 лет проведение эксплуатационных испытаний пожарных лестниц и ограждений на крышах с составлением соответствующего протокола испытаний, а также периодического освидетельствования состояния средств спасения с высоты в соответствии с технической документацией или паспортом на такое изделие;

17. Приямки у оконных проемов подвальных и цокольных этажей зданий (сооружений) должны быть очищены от мусора и посторонних предметов;

18. Руководитель организации обеспечивает сбор использованных обтирочных материалов в контейнеры из негорючего материала с закрывающейся крышкой и удаление по окончании рабочей смены содержимого указанных контейнеров.

19. В зданиях с витражами высотой более одного этажа не допускается нарушение конструкций дымонепроницаемых негорючих диафрагм, установленных в витражах на уровне каждого этажа.

20. Руководителем организации, на объекте которой возник пожар, обеспечивается доступ пожарным подразделениям в закрытые помещения для целей локализации и тушения пожара.

21. Руководитель организации при расстановке в помещениях технологического, выставочного и другого оборудования обеспечивает наличие проходов к путям эвакуации и эвакуационным выходам.

22. Запрещается оставлять по окончании рабочего времени не обесточенными электроустановки и бытовые электроприборы в помещениях, в которых отсутствует дежурный персонал, за исключением дежурного освещения, систем противопожарной защиты, а также других электроустановок и электротехнических приборов, если это обусловлено их функциональным назначением и (или) предусмотрено требованиями инструкции по эксплуатации.

23. Запрещается:

23.1. эксплуатировать электропровода и кабели с видимыми нарушениями изоляции;

23.2. пользоваться розетками, рубильниками, другими электроустановочными изделиями с повреждениями;

23.3. обертывать электролампы и светильники бумагой, тканью и другими горючими материалами, а также эксплуатировать светильники со снятыми колпаками (рассеивателями), предусмотренными конструкцией светильника;

23.4. пользоваться электроутюгами, электроплитками, электрочайниками и другими электронагревательными приборами, не имеющими устройств тепловой защиты, а также при отсутствии или неисправности терморегуляторов, предусмотренных конструкцией;

23.5. применять нестандартные (самодельные) электронагревательные приборы;

23.6. оставлять без присмотра включенными в электрическую сеть электронагревательные приборы, а также другие бытовые электроприборы, в том числе находящиеся в режиме ожидания, за исключением электроприборов, которые могут и (или) должны находиться в круглосуточном режиме работы в соответствии с инструкцией завода-изготовителя;

23.7. размещать (складировать) в электрощитовых (у электрощитов), у электродвигателей и пусковой аппаратуры горючие (в том числе легковоспламеняющиеся) вещества и материалы;

23.8. при проведении аварийных и других строительно-монтажных и реставрационных работ использовать временную электропроводку, включая удлинители, сетевые фильтры, не предназначенные по своим характеристикам для питания применяемых электроприборов.

24. Руководитель организации обеспечивает исправное состояние знаков пожарной безопасности, в том числе обозначающих пути эвакуации и эвакуационные выходы;

25. Запрещается пользоваться неисправными газовыми приборами, а также устанавливать (размещать) мебель и другие горючие предметы и материалы

на расстоянии менее 0,2 метра от бытовых газовых приборов по горизонтали и менее 0,7 метра - по вертикали (при нависании указанных предметов и материалов над бытовыми газовыми приборами);

26. В соответствии с инструкцией завода-изготовителя руководитель организации обеспечивает проверку огнезадерживающих устройств (заслонок, шиберов, клапанов и др.) в воздуховодах, устройств блокировки вентиляционных систем с автоматическими установками пожарной сигнализации или пожаротушения, автоматических устройств отключения вентиляции при пожаре;

27. При эксплуатации систем вентиляции и кондиционирования воздуха запрещается:

27.1. оставлять двери вентиляционных камер открытыми;

27.2. закрывать вытяжные каналы, отверстия и решетки;

27.3. подключать к воздуховодам газовые отопительные приборы

27.4. выжигать скопившиеся в воздуховодах жировые отложения, пыль и другие горючие вещества;

28. Руководитель организации определяет порядок и сроки проведения работ по очистке вентиляционных камер, циклонов, фильтров и воздуховодов от горючих отходов с составлением соответствующего акта, при этом такие работы проводятся не реже 1 раза в год;

29. Руководитель организации обеспечивает укомплектованность пожарных кранов внутреннего противопожарного водопровода пожарными рукавами, ручными пожарными стволами и вентилями, организует перекатку пожарных рукавов (не реже 1 раза в год);

30. Руководитель организации обеспечивает исправное состояние систем и средств противопожарной защиты объекта (автоматических (автономных) установок пожаротушения, автоматических установок пожарной сигнализации , установок систем противодымной защиты, системы оповещения людей о пожаре, средств пожарной сигнализации, противопожарных дверей, противопожарных и дымовых клапанов, защитных устройств в противопожарных преградах) и организует не реже 1 раза в квартал проведение проверки работоспособности указанных систем и средств противопожарной защиты объекта с оформлением соответствующего акта проверки.

31. Выбор типа и расчет необходимого количества огнетушителей следует производить в зависимости от огнетушащей способности, предельной площади, класса пожара горючих веществ и материалов защищаемом помещении или на объекте согласно СП 9.13130.2009.

Для помещений телерадиокомпании актуальны следующие классы пожаров:

Класс А - пожары твердых веществ, основном органического происхождения, горение которых сопровождается тлением (древесина, текстиль, бумага).

Класс Е - пожары, связанные с горением электроустановок.

Для данных классов пожаров, исходя из рекомендация СП 9.13130.2009, следует применять порошковые огнетушители.

Огнетушители следует располагать на защищаемом объекте в соответствии с требованиями ГОСТ 12.4.009 таким образом, чтобы они были защищены от воздействия прямых солнечных лучей, тепловых потоков, механических воздействий и других неблагоприятных факторов (вибрация, агрессивная среда, повышенная влажность и т.д.). Они должны быть хорошо видны и легкодоступны в случае пожара. Предпочтительно размещать огнетушители вблизи мест наиболее вероятного возникновения пожара, вдоль путей прохода, а также около выхода из помещения. Огнетушители не должны препятствовать эвакуации людей во время пожара.

Огнетушители, введенные в эксплуатацию, должны подвергаться техническому обслуживанию, которое обеспечивает поддержание огнетушителей в постоянной готовности к использованию и надежную работу всех узлов огнетушителя в течение всего срока эксплуатации. Техническое обслуживание включает в себя периодические проверки, осмотры, ремонт, испытания и перезарядку огнетушителей.

4.8. Сравнение параметров рабочего места с допустимыми нормами.

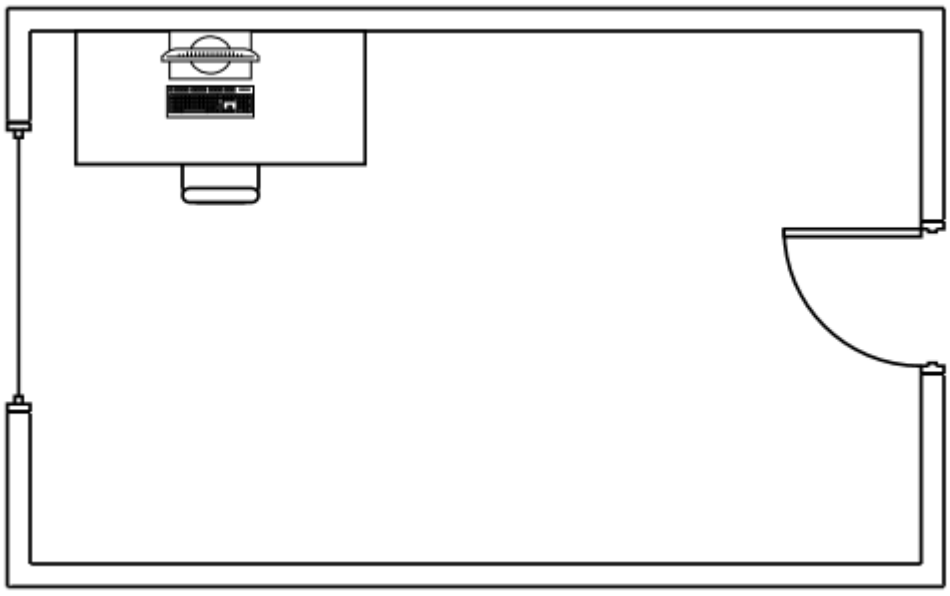

Рис. 1 – Схема рабочего места.

Для того чтобы определить соответствие условий труда требованиям нормативных документов необходимо провести сравнительный анализ требований, установленных к рабочим местам, оборудованным ПЭВМ и фактических параметров рабочего места. Схема размещения рабочего места приведена на Рисунке 1. Площадь помещения 18м2, оконный проем, шириной 1,4м размещается слева. В помещении присутствует естественное и искусственное освещение.

Перечень нормируемых параметров для рабочего места, сравнение их допустимых нормы и фактические значений на рабочем месте представлены в таблице 2.

Таблица 2 – Сравнение параметров рабочего места с допустимыми нормами.

Нормируемые параметры	Допустимые нормы	Фактические значения
Высота рабочей поверхности стола	от 680 до 800мм, либо 725мм	725мм
Модульные размеры рабочей поверхности стола	Ширина 800, 1000, 1200, 1400мм, глубина 800 и 1000мм	Ширина 1400мм глубина 600 мм
Ширина и глубина поверхности сиденья	Не менее 400мм	Ширина 500мм Глубина 450мм
Площадь на одно рабочее место	не менее 4,5м2	18м2
Падение естественного света	Преимущественно слева	Слева
Освещенность поверхности стола	300-500 лк	395 лк
Уровень звука	80 дБА	51 дБА
Параметры микроклимата (кат. 1а)	Температура воздуха 22-24° С Влажность воздуха 40-60%	Температура 22° С Влажность воздуха 55%
Подставки для ног	Ширина — от 30 см, глубина – от 40 см с углом наклона до 20 градусов.	Ширина — 35 см, глубина – 42 см с углом наклона 20 градусов.
Регулировка кресла по высоте	Поверхность сидения Ширина — от 30 см, глубина – от 40 см с углом наклона от 5 до 15 градусов. Высота от 40-55 см. Опорная поверхность спинки стула высоту (30±2)см, ширина от 38см, радиус кривизны в горизонтальной плоскости 40 см. Угол наклона спинки в вертикальной плоскости должен регулироваться в	Поверхность сидения Ширина — 32см, глубина – 42см, с углом наклона 10 градусов, Высота 45 см. Опорная поверхность спинки стула высоту 30см, ширина 40см, радиус кривизны в горизонтальной плоскости 40 см. Угол наклона

Нормируемые параметры	Допустимые нормы	Фактические значения
	пределах 00 ± 300 от вертикального положения. Расстояние спинки от переднего края сиденья должно регулироваться в пределах от 26 до 40 см. Подлокотники должны быть длиной не менее 25 см, шириной – 5…7см, иметь возможность регулирования по высоте над сиденьем в пределах (23 ± 3) см и регулирования внутреннего расстояния между подлокотниками в пределах от 35 до 50 см.	спинки в вертикальной плоскости должен регулироваться в пределах 00 ± 300 от вертикального положения. Расстояние спинки от переднего края сиденья должно регулироваться в пределах от 30см. Подлокотники 30 см, шириной – 6 см, иметь возможность регулирования по высоте над сиденьем 24 см и регулирования внутреннего расстояния между подлокотниками 40 см.

Выводы по главе 4

В результате проведенного анализа требований были выявлены общие требования к организации рабочих мест пользователей, требования к помещениям для работы с ПЭВМ, основные требования к освещению на рабочих местах, уровню шума и микроклимату. На основе проведенного анализа было установлено, что условия труда на рабочем месте соответствуют вышеперечисленным требованиям за исключением ширины рабочего места.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Толеубекова Б.Х. Социология компьютерной преступности. Учебное пособие. - Караганда, 1992

2. Батурин Ю.М. Проблемы компьютерного права. - М.: Юрид. лит., 1991, с. 126

3. 3. Концептуальные основы судебной компьютерно-технической экспертизы [Электронный ресурс]. – Режим доступа: http://www.dslib.net/kriminalprocess/konceptualnye-osnovy-sudebnoj-kompjuterno-tehnicheskoj-jekspertizy.html

4. Федеральный закон от 31 мая 2001 г. N 73-ФЗ "О государственной судебно-экспертной деятельности в Российской Федерации" - Электронный документ. Режим доступа: http://base.garant.ru/12123142/

5. Гражданский процессуальный кодекс РФ (ГПК РФ 2015) [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/grazhdanskij-processualnyj-kodeks-rf-gpk-rf, свободный

6. Уголовно-процессуальный кодекс РФ (УПК РФ) [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/ugolovno-processualnyj-kodeks-rf-upk-rf, свободный

7. Арбитражный процессуальный кодекс РФ (АПК РФ 2015) [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/arbitrazhnyj-processualnyj-kodeks-rf-apk-rf, свободный

8. Постановление Пленум Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 «О судебной экспертизе по уголовным делам» [Электронный ресурс]. – Режим доступа: https://rg.ru/2010/12/30/postanovleniedok.html, свободный

9. Handbook по дисциплине: «Современные возможности судебной экспертизы»: Программа магистерской подготовки по направлению «Юриспруденция» [Электронный ресурс]. – Режим доступа: http://ebiblio.ru/book/bib/04_pravo/Sovrem_VSD/hb.html, свободный

10. Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе [Электронный ресурс]. – Режим доступа http://www.vuzllib.su/books/2180-

Судеб-

ная_экспертиза_в_гражданском,_арбитражном,_административном_и_уг оловном_процессе_–_Е_Р__Россинс, свободный

11. Цели и задачи судебно-экспертного исследования: проблемы теоретического обоснования [Электронный ресурс]. – Режим доступа http://www.center-bereg.ru/f1879.html, свободный

12. Предмет судебной экспертизы [Электронный ресурс]. – Режим доступа http://www.law.edu.ru/doc/document.asp?docID=1311442, свободный

13. Зубаха В.С., Усов А.И., Саенко Г.В., Волков Г.А., Белый С.Л., Семикаленова А.И. Общие положения по назначению и производству компьютерно-

технической экспертизы: Методические рекомендации. - М.: ГУ ЭКЦ МВД России, 2000. - 65 с

14. Федотов Н.Н. Форензика – компьютерная криминалистика – М.: Юридический мир, 2007.

15. Приказ Министерства юстиции Российской Федерации (Минюст России) от 27 декабря 2012 г. N 237 г. Москва «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России» [Электронный ресурс]. – Режим доступа: https://rg.ru/2013/02/06/expertiz-dok.html, свободный

16. Усов А.И. Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения: Учебное пособие / А.И. Усов // Под ред. проф Е.Р. Россинской – М.: Издательство «Экзамен», издательство «Право и закон», 2003. – 368 с.

17. Шляхов А.Р. Предмет и система криминалистической экспертизы//Тр. ВНИИСЭ. М., 1971. Вып. 3.С. 17.

18. Орлова В.Ф. Теория судебно-почерковедческой идентификации//Тр. ВНИИСЭ. М., 1973. Вып. 6. С. 230.

19. Митричев В.С. Общие положения методики криминалистического идентификационного исследования материалов документов//Тр. ВНИИСЭ. М., 1974. Вып. 9. С. 18.

20. Колмаков В.П. О методах, приемах и средствах в советской криминалистике//Правоведение. 1965. №4. С. 118-120

21. Курс лекций по учебной дисциплине «Судебная экспертиза» [Электронный ресурс]. – Режим доступа http://distance.rpamu.ru/files/2_vys_bak/sudeb_expertiza.pdf, свободный

22. Ефимичев С.П. Комментарий к Федеральному закону «О государственной судебно-экспертной деятельности в Российской Федерации» (постатейный) /под ред. В.П. Кашепова //Юстицинформ, 2003

23. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. – М.: Право и закон, 2001. - 416 с.

24. Некоммерческое Партнерство Поставщиков Программных Продуктов (НП ППП). Специальные знания при выявлении и расследовании дел, связанных с нарушениями авторских и смежных прав на программы для ЭВМ и базы данных. Второе издание. - Москва, 2012.

25. В.С. Зубаха и др. Общие положения по назначению и производству компьютерно-технической экспертизы.- ГУ ЭКЦ МВД, 2001

26. А.Н.Родионова. Расследование преступлений в сфере компьютерной информации (учебно-методическое пособие). – Москва, 1998.

27. Ю.Г. Корухов. Криминалистическая диагностика для экспертов. – М.: Библиотека эксперта, 2007

28. Брайан Кэрриэ. Криминалистический анализ файловых систем – СПб.: Питер, 2007

29. Steve Bunting. The Official EnCE: EnCase Certified Examiner Study Guide. Second Edition.- Wiley Publishing, Inc, 2007

30. Кевин Мандиа, Крис Просис. Защита от вторжений. Расследование компьютерных преступлений. - Издательство "ЛОРИ", 2005

31. Райан Р. Кубэзиэк, Шон Моррисси. Криминалистическое исследование Mac OS X, iPod и iPhone. [Электронный ресурс]. – Режим доступа http://computer-forensics-lab.org/pdf/Mac_OsX_Ipod_rus.pdf, свободный

32. Крис Поуг, Кори Алтеид, Тодд Хаверкос. Криминалистическое исследование Unix и Linux. [Электронный ресурс]. – Режим доступа http://computer-forensics-lab.org/pdf/rus_unix_and_linux_forensic_analysis.pdf, свободный

33. Эджубов, Л.Г. Производство судебной компьютерно-технической экспертизы: III. Специализированный словарь компьютерной лексики для экспертов компьютерно-технической экспертизы / Л.Г. Эджубов, А.И. Усов, Е.С. Карпухина, Н.А. Хатунцев, А.С. Демов, Н.Л. Комраков, П.В. Костин // – М.: РФЦСЭ, 2009.

34. Digital Forensics with Open Source Tools by Cory Altheide and Harlan Carvey [Электронный ресурс]. – Режим доступа http://fcbi.unillanos.edu.co/segurinfo.unillanos/archivos/materialApoyo/Forensics%20with%20Open%20Source%20tools.pdf, свободный

35. Юрин, И.Ю. Способы установления первоначального имени PE-файла / И.Ю. Юрин // Теория и практика судебной экспертизы: Научно-практический журнал. – М.: РФЦСЭ, 2008, №3 (11)

ПРИЛОЖЕНИЕ А.

МЕТОДИКА АНАЛИЗА ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ НЕЗАКОННОЙ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ АЗАРТНЫХ ИГР В РОССИЙСКОЙ ФЕДЕРАЦИИ

Л.В. Астахова, А.В. Волков, В.В. Григорьев

В работе рассмотрены проблемы правого регулирования процессов организации и проведения азартных игр в Российской Федерации. На примере отдельных программно-аппаратных средств проведен анализ распространенных методик теневых и незаконных подходов к организации и проведению азартных игр, изучены основные технические и программные способы незаконной организации азартных игр. Обоснована методика анализа программно-аппаратных средств незаконной игорной деятельности, рассмотрены перспективы повышения эффективности государственного контроля и профилактики названной деятельности.

Ключевые слова: *азартные игры, незаконная игорная деятельность, уголовная ответственность, игровое оборудование, методика, расследование, осведомленность.*

За последние десять лет игорный бизнес превратился в качественно новый и весьма прибыльный вид предпринимательской деятельности в Российской Федерации. Широко распространились не только различные негосударственные лотереи, но и появилось новое направление деятельности - игровые автоматы. На конец 2014 г. в стране функционировало более 60 тысяч игровых залов, в которых было размещено около 800 тысяч игровых автоматов [5]. Все это происходит на фоне роста интереса к данному виду развлечения.

В настоящее время правовое регулирование общественных отношений в сфере игорного бизнеса осуществляется на основе большого количества нормативных актов административного, финансового и налогового права, принятых как на федеральном уровне, так и на уровне субъектов Федерации. Однако принятых правовых мер по его регулированию недостаточно для защиты общества от вредных проявлений данной деятельности.

Игорный бизнес распространился настолько, что стал представлять реальную угрозу для общественной нравственности и здоровья человека. Во-первых, человек стремится получить деньги, не прилагая никаких усилий, у него теряется интерес к работе, поскольку он надеется получить деньги с помощью выигрыша.

Во-вторых, азартные игры опасны для здоровья человека, так как неминуемо приводят к зависимости от игры – игромании, являющейся психическим расстройством. Данное расстройство психиатры ставят в один ряд с наркотической и алкогольной зависимостью. [5].

Неслучайно анализ законодательства стран СНГ в данной сфере показал, что превалирующей позицией в нем «является отнесение преступлений, связанных с азартными играми, к посягательствам на общественный порядок и общественную нравственность. Такой подход реализован даже в тех странах, где организация азартных игр полностью не запрещена и является при соблюдении определенных требований одним из видов разрешенной экономической деятельности» [4].

Игорный бизнес является также благоприятной почвой для распространения преступлений. Этому способствует простота извлечения предпринимателем прибыли, что, в свою очередь, влечет концентрацию большого количества наличных денежных средств в игорных заведениях.

В 2007-2008 гг. многие объекты игорного бизнеса перешли в нелегальный статус. Наиболее примечательны примеры, приведенные МВД России. Так, в Кемеровской области было за указанный период было изъято 747 незаконно установленных игровых автоматов, в Красноярском крае - 730, в Тюменской области - 62. В 2008 г. представители незаконного игорного бизнеса не ослабили своих позиций. [5].

На смену клубам игровых автоматов пришли компьютерные развлекательные центры. Владельцы заведений не только изменили названия, но оснастили клубы новым техническим оборудованием, внешне похожим на обычные компьютеры, а, по сути, являющимися игровыми автоматами.

29 декабря 2006 г. был принят Федеральный закон «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» № 244-ФЗ, который ввел жесткие требования к организации и проведению азартных игр, а также к организаторам и посетителям игорных заведений [9]. Федеральным законом от 20.07.2011 № 250- ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», в УК РФ была введена ст. 171.2, предусматривающая ответственность «за незаконную организацию и (или) проведение азартных игр с использованием игрового оборудования вне игорной зоны, либо с использованием информационно-телекоммуникационных сетей, в том

числе сети «Интернет», а также средств связи, в том числе подвижной связи, либо без полученного в установленном порядке разрешения на осуществление

деятельности по организации и проведению азартных игр в игорной зоне» [8, 7]. Федеральным законом от 22.12.2014 № 430-ФЗ «О внесении изменений в статью 171.2 Уголовного кодекса Российской Федерации и статьи 14.1.1 и 28.3 Кодекса Российской Федерации об административных правонарушениях» в ст. 171.2 УК РФ были внесены изменения: теперь уголовная ответственность наступает вне зависимости от размера извлеченного дохода, т.е. за факт осуществления указанной деятельности, кроме того, был увеличен размер штрафа, предусмотренный санкцией данной статьи [3].

Однако, несмотря на изменения в законодательстве, постоянно появляются и развиваются принципиально новые технические, программные и аппаратные методы и средства незаконной организации и проведения азартных игр, реализуемые в форме попыток выдать игорную деятельность за иную, не подлежащую регулированию обозначенными федеральными законами. В последнее время широкое распространение получили так называемые биржевые терминалы, представляющие собой игровые автоматы либо персональные компьютеры с установленным на них игровым программным обеспечением, юридически сопровождаемые следующими утверждениями (на примере представителей компаний владеющих «биржевыми» терминалами «Holitrade»):

«В соответствии с положениями статьи 2 Федерального закона от 29.12.2006 г. № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» (далее – Закон об азартных играх), правовое регулирование деятельности по организации и проведению азартных игр осуществляется, в том числе, в соответствии с Гражданским кодексом Российской Федерации (далее – ГК РФ).

Организация игр и пари регулируется Главой 58 ГК РФ «Проведение игр и пари». В пункте 2 статьи 1062 ГК РФ подчеркивается, что правила указанной главы не распространяются на требования, связанные с участием в сделках, предусматривающих обязанность стороны или сторон сделки уплачивать денежные суммы в зависимости от изменения цен на товары, ценные бумаги, курса соответствующей валюты, величины процентных ставок, уровня инфляции или от значений, рассчитываемых на основании совокупности указанных показателей, либо от наступления иного обстоятельства, которое предусмотрено законом и относительно которого неизвестно, наступит оно или не наступит. При этом

требования, связанные с участием граждан в указанных в настоящем пункте сделках, подлежат судебной защите только при условии их заключения на бирже.

Таким образом, из вышеизложенного следует, что:

1. Деятельность по организации и проведению сделок в отношении любых внебиржевых производных финансовых инструментов как рынка ценных бумаг, так и рынка Forex (например, опционов, форвардов – далее Деривативов) Законом об азартных играх не регулируется.

2. Сделки в отношении Деривативов являются биржевыми играми.

3. Сделки в отношении Деривативов на рынке Forex до 1 октября 2015 года не регулируются нормативными правовыми актами финансовых регуляторов Российской Федерации (ранее – Федеральная служба по финансовым рынкам России (далее – ФСФР), в настоящее время – ЦБ РФ).

Это подтверждается Письмом ФСФР от 16.07.2009 г. № 09-ВМ-02/16341. Кроме того, деятельность по предоставлению услуг дилинговыми компаниями по доступу на международный рынок Forex не относится к лицензируемым видам деятельности (письма Минэкономразвития РФ от 18.04.2011 г. № Д06-2098, от 24.01.2011 г. № Д06-414).

NB. 29 декабря 2014 года был принят Федеральный Закон № 460-ФЗ, в соответствии с которым, в частности, устанавливается необходимость лицензирования деятельности форекс-дилеров, а также их членства в саморегулируемых организациях (СРО). Указанный Закон в этой части вступает в силу 1 октября 2015 года.

4. При соответствующем оформлении договорных взаимоотношений между гражданином и Компанией, предоставляющей услуги на рынке Forex, указанные взаимоотношения не регулируются Законом РФ от 07.02.1992 г. № 2300-1 «О защите прав потребителей»»

Из текста видно, что незаконную организацию и проведение азартных игр маскируют под организацию биржевых торгов, торговлю бинарными опционами и т.д. Несмотря на очевидность этих фактов, следует констатировать низкий уровень раскрываемости преступлений, связанных с незаконной игорной деятельностью. Это обусловлено, в частности, недостаточным уровнем профессионализма сотрудников правоохранительных органов [2], которым необходимы специальные знания. Эти знания необходимы для классификации расследумой деятельности как игорной, для классификации изымаемой техники как игровой, для определения наличия в составе изъятого оборудования специфических для игровой техники функциональных модулей, проверки соответствия характеристик модулей требованиям закона [6, с.96]. Однако, как справедливо отмечают эксперты,

«методик классификационного исследования игрового и лотерейного оборудования еще не существует» [6, с.96]. Необходимость разработки и апробации принципиально новой методики классификации деятельности подозреваемого в совершении преступления по статье 171.2 УК РФ как деятельности по незаконной организации и проведению азартных игр обусловила актуальность настоящей статьи. В условиях отсутствия обширной практики и малого количества судебных решений, вынесенных по данной статье, представляется важным создание такой методики классификации, которая позволила бы с необходимой степенью достоверности проводить анализ программно-аппаратных средств и организационных аспектов незаконной деятельности, в целях объективного правоприменения.

В ходе данного исследования по специально разработанной авторской методике была проанализирована работа программно-аппаратного комплекса «Holitrade», распространенного в сфере незаконного проведения азартных игр в России, и сделаны выводы о том, что имеет место именно маскировка под указанные виды деятельности и подмена понятий. При этом имеет место нарушение действующего законодательства, путем введения в заблуждение граждан производится извлечение прибыли от незаконной организации и проведения азартных игр. Клиенты и пользователи таких программно-аппаратных комплексов также нарушают закон.

В ходе анализа было проведено исследование системного блока персонального компьютера с установленным на нем программным обеспечением «Holitrade». Для исследования была использована разработанная методика:

- скачивание с сайта i.holitrade.com программного обеспечения «loto», «operator»;
- установка указанного программного обеспечения на системный блок персонального компьютера;
- Проведение анализа возможностей программного обеспечения;
- анализ сетевого взаимодействия программного обеспечения с внешними ресурсами;
- анализ особенностей алгоритмов, заложенных в основу программного обеспечения.

В ходе исследования установлено программное обеспечение «loto», версия 1.117.0.706 Данное программное обеспечение представляет собой программу-

клиент для обеспечения доступа к функциям встроенных программ и связи с серверами системы «Holitrade».

Продолжение приложения А

При установке указанной программы создается каталог с именем «games_full» (имя может быть изменено) со следующей структурой:

alcatraz_.dat
aztecgold.dat
bananasgobahamas.dat
beetlemania.dat
beetlemaniadx.dat
bonuspoker.dat
bookofra.dat
bookofradx.dat
budmo.dat
champagneparty.dat
chukcha.dat
coctail.dat
coldspell.dat
columbus.dat
columbusdx.dat
d3dx9_27.dll
deuceswild.dat
dolphinspearl.dat
dolphinspearldx.dat
DXErr9ab.dll
egyptianexperience.dat
fruitcase.dat
garage.dat
gnome.dat
gnomedeluxe.dat
goldcraze.dat
gonzoquest.dat
gopstop.dat
hannibalofcarthago.dat
happybugs.dat
hottarget.dat
hotvolee.dat
indianspirit.dat
island.dat
island2.dat
jackhammer.dat
jewels4all.dat
jokeranddeuceswild.dat
jump.dat
justjewels.dat
justjewelsdx.dat
keks.dat
libmysqld.dll
loto.exe
loto.ini
lucky.dat
luckyladyscharm.dat
luckyladyscharmdx.dat
magicmoney.dat
marcopolo.dat
marcopolodx.dat
money.dat
moneygame.dat
monkey.dat
oilcompany.dat
oliversbar.dat
pandacash.dat
pharaohsgoldii.dat
pharaohsgoldiidx.dat
pirate.dat
pirate2.dat
plentytwenty.dat

probki.dat
rezident.dat
roulette3d.dat
shared.dat
sharky.dat
silverfox.dat

sizzlinghot.dat
sizzlinghotdx.dat
skalolaz.dat
slotopol.dat
slotopoldeluxe.dat
swamp.dat
sweetlife.dat
sweetlife2.dat
themingdynasty.dat
unicornmagic.dat
venetiancarnival.dat
vovka.dat
zoo.dat
data\home.err
data\ibdata1
data\ib_logfile0
data\ib_logfile1
data\kiosk\billorders.frm
data\kiosk\billstat.frm
data\kiosk\db.opt
data\kiosk\deffered_commands.frm
data\kiosk\dispstat.frm
data\kiosk\incassation.frm
data\kiosk\option.frm
data\kiosk\payorders.frm
data\kiosk\pinpayoutorders.frm
logs\
share\english\errmsg.sys»

Для функционирования указанная программа «loto» использует файл конфигурации, в котором хранятся основные настройки программы. Указанный файл расположен в одном каталоге с программой, имеет название «loto.ini» и содержит в себе следующие сведения:

«[Relay]
RelayEnabled=1
RelayHost=http://relay.dyndns.org/relay/
RelayClient=holitrade
[Localization]
; языкинтерфейса (ru, en)

; пустая строка означает язык по умолчанию в операционной системе
Lang=
; валюта в произвольной форме
; пустая строка означает валюту по умолчанию в операционной системе
Currency=
[Options]
;номер com-порта к которому подключен купюроприемник
BillCom=0
;тип купюроприемника (cashcode, nv200, md100)
BillValidator=cashcode
;код валюты разрешенной к приему (по умолчанию:RUS - российские рубли для cashcode, RUB - для NV200)
BillCountryCode=RUS
;тип диспенсера банкнот (Lcdm1000, Lcdm2000 , Ecdm200, SmartPayout)
Dispenser=Lcdm1000
;номер com-порта к которому подключен диспенсер, для SmartPayout указать тот же COM-порт что и купюроприемник
DispCom=
;которкий ответ диспенсера (если не удается настроить на самом диспенсере)
DispShortAnswer=0
;тип терминала
Terminal=main
;команда, выполняемая при запуске игры (web | bill | menu)
; web (по умолчанию) - отобразить веб страницу, указанную в параметре OpenWebPageOnGame
; bill - включить купюроприемник, чтобы принимать деньги непосредсвенно во время игры
; menu - отображать главное меню
CommandOnGame=bill
;веб-страница, открываемая при старте игры при CommandOnGame=web (если пустое значение, то будет
;открываться главное меню)
;эта же страница будет открываться по таймауту, если отключено завершение сеанса по таймауту
;работает только после авторизации
OpenWebPageOnGame=http:\\www.yandex.ru
; MAC-адрес подставляемый в качестве имени киоска вместо оригинального MAC-адреса сетевой карты
ForceMac=wy005
; завершать сеанс, по истечении этого времени, если пользователь не совершает никаких действий
; при включенном параметре Autologin делается выход в основное меню
; 0-не завершать сеанс (время в секундах)
LogOutInterval=30
; ограничение выдачи денег терминалом за определенный период времени:
; максимальная сумма в рублях
PayLimit =10000
; интервал времени в минутах
PayLimitInterval =60
; разрешить регистрировать пин коды

AllowUserPinCodes =1
PinCodeLoginAfterCreate =1
; время в течении которого разрешена печать чека при выплате через пин код, мин
PinPayOutPrintTime =5
;время в секундах через которое будет запущена игра при простое киоска (-1 игра не запускается)
RestartGameTime =30
; блокировка диспенсера при любой ошибке по выдаче купюр, блокировка снимается перезапуском киоска
; при включении блоировки отправляется СМС с уведомлением
LockDispenserOnError=0
; скрытиепинкода
HidePinCode=0
; если не удается подключиться к серверу, перезагружаем компьютер.
; интервал времени в минутах (0 - выключает данную функцию)
RebootTimeInterval=15
;маска для ввода номера телефона при СМС выплатах, для Украины это: 38 (___) _____
phonemask=7 (___) ___ __ __
; время выхода из игры в режиме простоя в секундах. Минимально 30 сек., максимально 600 сек. (10 минут)
GameExitTimeOut=30
; включает или отключает защиту от размена купюр (1 - включена)
ExchangeProtection=1
; задержка при старте программы в секундах, иногда необходима для инициализации купюрников, 0 - отключено
StartDelay=0
[Bill]
; включение/отключение обработки команды Cassete Out (откидывание стекера)
; при выключении опции, вход в админ-меню только с конпки или через сайт
EnableHandleCasseteOut=1
[Dispenser]
; номиналы купюр диспенсера, которые можно будет выбрать при инкассации
;значения задаются через запятую, ;максимальное количество номиналов - 9
; значение по умолчанию - 10, 50, 100, 500, 1000, 5000
Nominals=10, 50, 100, 500, 1000, 5000
; защита баланса при застревании купюры на выходе диспенсера (застрявшая купюра будет учтена как выданная)
TakeExitJam=1
[View]
; изображение для заголовка
HeaderImage=
; фоновое изображение
BodyImage=
; отображение экранной клавиатуры
ShowKeyboard=1
; ширина экрана
Width=1280
; высота экрана

Height=1024
[Printer]
;разрешить/запретить печать чеков
Enabled=0
;разрешить/запретить печать чеков при приеме купюр
PrintOnBill=0
;шрифтначеке
FontName=Times New Roman
;размер шрифта на чеке
FontSize=10
;смещение
LeftOffset=50
TopOffset=150
[PrintHeader]
Нашафирма
[PrintFooter]
СЛУЖБАПОДДЕРЖКИ: (xxx) xxx-xx-xx
Наша фирма
Наш адрес
[Reports]
;отчеты
; разрешить отчет о состоянии терминала 0|1 (по умолчанию разрешено)
ReportStatusEnable=1
;частота отправки отчета в секундах (по умолчанию 300 с = 5 мин), параметр выдерживается неточно
ReportStatusInterval=300
;разрешить отчет о настройках, действующих в терминале 0|1 (по умолчанию разрешено)
ReportOptionsEnable=1
;частота отправки отчета в секундах (по умолчанию 600 с = 10 мин), параметр выдерживается неточно
ReportOptionsInterval=600
[Alerts]
;уведомления по sms о необходимости инкассации (уведомления регулярно отсылаются на сервер, а уже он осуществляет отправку sms, если они разрешены)
;частота проверки необходимости уведомления (по умолчанию 600 с = 10 мин), параметр выдерживается неточно
AlertInterval=600
;номер телефона, на который будут отправлятся уведомления
;номер можно здесь не указывать, а указать в веб-админке
;если номер задать здесь и в веб-админке, приоритет отдается веб-админке
;формат номера 7xxxxxxxxx
AlertPhone=
;уведомлять о состоянии купюроприемника 0|1 (по умолчанию разрешено, если купюроприемник отсутствует, то уведомления не отсылаются)
BillAlertEnable=1
;минимальное количество купюр, оставшееся до достижения заданного настройками лимита, при котором отправляется уведомление

BillAlertCount=0

;минимальная сумма, оставшая до достижения заданного в настройках лимита, при котором отправляется уведомление

BillAlertSum=0

;уведомлять о состоянии диспенсера 0|1 (по умолчанию разрешено, если диспенсер отсутсвует, то уведомления не отсылаются)

DispAlertEnable=1

;максимальное количество купюр (суммарно во всех кассетах), оставшееся в диспенсере, при котором отправляется уведомление

DispAlertCount=0

;максимальная сумма (суммарно во всех кассетах), оставшаяся в диспенсере, при которой отправляется уведомление

DispAlertSum=0

[Office]

;отображать кнопку "Выбрать услугу" 0|1 (по умолчанию 1)

MenuButtonVisible=1

;отображать кнопку "Пополнить счет" 0|1 (по умолчанию 1)

BillButtonVisible=1

;отображать кнопку "Снять деньги" 0|1 (по умолчанию 1)

PayoutButtonVisible=1

;отображать кнопку "Вернуться в игру" 0|1 (по умолчанию 1)

StartGameButtonVisible=1

;отображать кнопку "Получить деньги через центр выплат" 0|1 (по умолчанию 0)

PinPayButtonVisible=1

;отображать кнопку "Получить деньги через центр выплат" при ошибках диспенсера 0|1 (по умолчанию 0)

PinPayButtonVisibleFromDisp=1

;номер SMS центра.можно здесь не указывать, а указать в веб-админке

;если номер задать здесь и в веб-админке, приоритет отдается веб-админке

;формат номера 7xxxxxxxxx

SMSCenterPhone=

;номер телефона поддержки, который будет выводить в окне киоска(в верху окна)

SupportPhone=»

Факт использования программой «loto» указанного файла «loto.ini» подтверждается следующим:

- в ходе проведения исследования была произведена процедура проверки взаимодействия программы «loto» с файлом «loto.ini» путем перемещения файла «loto.ini» из папки с программой «loto». После этого был произведен запуск программы «loto». При отсутствии файла «loto.ini» в папке с программой «loto» программа «loto» при запуске сообщает об ошибке: «Не удается определить MAC-адрес устройства». В случае, когда файл «loto.ini» присутствует в папке с программой «loto», указанное сообщение об ошибке не появляется. В файле «loto.ini» имеются строки:

«*; MAC-адрес подставляемый в качестве имени киоска вместо оригинального MAC-адреса сетевой карты*

ForceMac= wy005»,

указывающие на то, что программа «loto» получает сведения о MAC-адресе. В данном случае параметр ForceMac выступает в качестве уникального идентификатора экземпляра программы «loto», отсутствие которого не позволяет программе функционировать.

По данному идентификатору каждый экземпляр программы «loto» идентифицируется в личном кабинете, описанном ниже, и благодаря этому идентификатору возможно осуществление удаленного управления экземпляром программы и персональным компьютером, на котором она установлена.

- в ходе проведения исследования была произведена процедура проверки взаимодействия программы «loto» с файлом «loto.ini» путем проверки реакции программы «loto» на изменение содержимого файла «loto.ini». В файле «loto.ini» имеются следующие строки:

«;номер com-порта к которому подключен купюроприемник

BillCom=0

;номер com-порта к которому подключен диспенсер, для SmartPayout указать тот же COM-порт что и купюроприемник

DispCom=0»,

указывающие на номера COM-портов, к которым подключаются устройства «купюроприемник» и «диспенсер».

Кроме этого, в папке с программой «loto» имеется папка «logs», в которой при запуске программы появляется файл с расширением «txt» и именем, соответствующим дате, когда запускается программа «loto». В данный файл программа «loto» записывает информацию о своей работе. В случае, если в файле «loto.ini» параметр «BillCom», задающий номер COM-порта, к которому подключен купюроприемник, равен 0, программа «loto» в файл с информацией о своей работе записывает следующую информацию:

«Не задан com-порт купюроприемника» (рис. 2.14 приложения).

В ходе проведения исследованияпараметр «BillCom» в файле «loto.ini» был приравнен к значению «20», после чего была запущена программа «loto». Программа «loto» в файл с информацией о своей работе записала следующую информацию:

«*Инициализируем купюроприемник cashcode (порт 20)*»

Таким образом, подтверждается, что программа «loto» обращается в процессе своей работы к файлу «loto.ini» для получения сведений о настройках своей работы.

Продолжение приложения А

Содержимое данного файла «loto.ini» указывает на то, что программа «loto» имеет возможность подключения устройств для ввода средств с их дальнейшей фиксацией в меню «Баланс» (количество внесенных средств).

Кроме этого, был произведен анализ сетевого взаимодействия представленной программы с внешними ресурсами.

Рассматриваемая программа в процессе своей работы отправляет и получает данные на адрес dydns.org, используя в качестве параметров идентификации логин «holitrade». DynDNS представляет собой сервис, который позволяет пользователям получить личный адрес, который будет привязан к пользовательскому компьютеру, не имеющему постоянного IP-адреса.

Когда информация попадает на адрес relay.dydns.org с логином «holitrade», сервер DynDNS пересылает её на адрес i.holitrade.com. По указанному адресу расположен личный кабинет пользователя системы «holitrade», в ходе анализа функций которого установлено следующее:

- В личном кабинете Holitrade возможно управление (создание, редактирование, удаление) учетными записями, используемыми программой «loto» для своей работы.
- В рамках настройки указанных учетных записей возможно редактирование так называемого «процента отдачи» (по умолчанию равного
- 60%), который представляет собой значение процента прибыли от выигрыша, получаемого в процессе функционирования программы «loto». Установить значение этого параметра ниже 60 возможность отсутствует. Кроме того, необходимо отметить, что при торговле бинарными опционами и на биржевых торах в целом не предусмотрено существование какого-либо управляемого относительного параметра, влияющего на размер прибыли.
- В личном кабинете отсутствуют какие-либо ресурсы, имеющие отношение к биржевым торгам, бинарным опционам и схожим по смыслу функционирования площадкам. Имеются функции сбора статистики функционирования подключенных к личному кабинету программ «loto».
- Любые изменения параметров счета в программе «loto» отражаются в личном кабинете i.holitrade.com.
- Из указанного личного кабинета возможно осуществление прямого управления персональным компьютером, на котором установлено программное

обеспечение «loto» (блокировка, выключение, возможность приема и передачи файлов).

В ходе анализа сетевого взаимодействия программы «loto» с внешними сервисами не установлено фактов обращения программы к

каким-либо площадкам биржевых торгов, площадкам по торговле бинарными опционами и схожим по смыслу функционирования площадки.

В программе «loto» предусмотрена настройка ставки и параметров игры. Программа поддерживает подключения устройств для списания электронных средств с игрового баланса. Указанная программа не относится к лотерейному оборудованию, т.к. не обладает соответствующими признаками.

В ходе исследования установлено программное обеспечение «operator», версия 1.117.0.706. Данное программное обеспечение представляет собой программу-клиент для обеспечения пополнений игровых баллов, списания игровых баллов, контроля установленных ставок и процента отдачи (выигрыша) на персональных компьютерах, на которых установлена описанная выше программа «loto», и для связи с серверами системы «Holitrade».

При установке указанной программы создается каталог с именем «operator» (имя может быть изменено) со следующей структурой:

«operator.exe

Config.ini»

Для своего функционирования указанная программа «operator» использует файл конфигурации, в котором хранятся основные настройки программы. Указанный файл расположен в одном каталоге с программой «operator» с именем «config.ini». Данный файл содержит в себе следующие сведения:

«[Relay]
RelayEnabled=1
RelayHost=http://relay.dyndns.org/relay/
RelayClient=holitrade
[Localization]
Lang=RU
Currency=
[FORMSETTINGS]
WIDTH=1125
HEIGH=784
LEFT=93
TOP=63
Skin=Caramel
[Main]
Version=2
BankLimitVisible=1
[treeGroups.treeGroups: TcxTreeList]
=
[treeGroups.treeGroups/Bands: TcxTreeListBands]
=
[treeGroups.treeGroups/Bands/Band0: TcxTreeListBand]
=

Caption=""
RealMinWidth=20
RealWidth=0
Visible="True"
Index=0
BandIndex=-1
ColIndex=0

Продолжение приложения А

[treeGroups.treeGroups/clmnID: TcxTreeListColumn]
=
Visible="False"
Index=0
LineCount=1
ColIndex=1
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnName: TcxTreeListColumn]
=
Visible="False"
Index=1
LineCount=1
ColIndex=10
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnDescr: TcxTreeListColumn]
=
Visible="False"
Index=2
LineCount=1
ColIndex=11
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnIsNode: TcxTreeListColumn]
=
Visible="False"
Index=3
LineCount=1
ColIndex=12
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnBankLimit: TcxTreeListColumn]
=
Visible="False"
Index=4
LineCount=1
ColIndex=13

RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0

[treeGroups.treeGroups/clmnLockedBankLimit: TcxTreeListColumn]
=
Visible="False"
Index=5
LineCount=1
ColIndex=22
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnTimeLimitEnabled: TcxTreeListColumn]
=
Visible="False"
Index=6
LineCount=1
ColIndex=14
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnTimeLimitExpire: TcxTreeListColumn]
=
Visible="False"
Index=7
LineCount=1
ColIndex=15
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnTimeLimitRest: TcxTreeListColumn]
=
Visible="False"
Index=8
LineCount=1
ColIndex=16
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnLocked: TcxTreeListColumn]
=
Visible="False"
Index=9
LineCount=1
ColIndex=17

RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0

[treeGroups.treeGroups/clmnLockedMessage: TcxTreeListColumn]
=
Visible="False"
Index=10
LineCount=1
ColIndex=20
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnMaxChildCnt: TcxTreeListColumn]
=
Visible="False"
Index=11
LineCount=1
ColIndex=21
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnRegDate: TcxTreeListColumn]
=
Visible="False"
Index=12
LineCount=1
ColIndex=18
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnAdminPercent: TcxTreeListColumn]

=
Visible="False"
Index=13
LineCount=1
ColIndex=19
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnCaption: TcxTreeListColumn]
=
Visible="True"
Index=14

LineCount=1
ColIndex=0
RowIndex=0
BandIndex=0
Caption="Название"
SortOrder="soNone"
SortIndex=-1

RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnBankLimitStr: TcxTreeListColumn]
=
Visible="True"
Index=15
LineCount=1
ColIndex=2
RowIndex=0
BandIndex=0
Caption="Банк-лимит"
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnIncredit: TcxTreeListColumn]
=
Visible="True"
Index=16
LineCount=1
ColIndex=3
RowIndex=0
BandIndex=0
Caption="Вход"
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnOutCredit: TcxTreeListColumn]
=
Visible="True"
Index=17
LineCount=1
ColIndex=4
RowIndex=0
BandIndex=0
Caption="Выход"
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnProfit: TcxTreeListColumn]
=
Visible="True"
Index=18
LineCount=1
ColIndex=5
RowIndex=0
BandIndex=0
Caption="Прибыль"
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnPercent: TcxTreeListColumn]
=
Visible="True"
Index=19

LineCount=1
ColIndex=6
RowIndex=0
BandIndex=0
Caption="Фактический %"
SortOrder="soNone"
SortIndex=-1

RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnFeedbackPercent: TcxTreeListColumn]
=
Visible="True"
Index=20
LineCount=1
ColIndex=7
RowIndex=0
BandIndex=0
Caption="Заданный %"
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnJackpot1: TcxTreeListColumn]
=
Visible="True"
Index=21
LineCount=1
ColIndex=8
RowIndex=0
BandIndex=0
Caption="Джекпот1"
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnJackpot2: TcxTreeListColumn]
=
Visible="True"
Index=22
LineCount=1
ColIndex=9
RowIndex=0
BandIndex=0
Caption="Джекпот2"
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[UsersFrame.grdUsersTableView: TcxGridTableView]
=
Footer="False"

GroupByBox="False"
GroupFooters=0
NewItemRow="False"
Version=1
[UsersFrame.grdUsersTableView/clmnID: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=0
Visible="False"
SortOrder="soNone"

SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnLocked: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0

Index=1
Visible="False"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnAccessRights: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=2
Visible="False"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnLastCompName: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=3
Visible="False"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnBindToComp: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=4
Visible="False"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFramegrdUsersTableView/clmnN: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=5
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
UsersFrame.grdUsersTableView/clmnOnline: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=6
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnAuthType: TcxGridColumn]
=
GroupIndex=-1

Width=64
AlignmentHorz=0
Index=7
Visible="False"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"

[UsersFrame.grdUsersTableView/clmnLogin: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=8
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnComment: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=9
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnBalance: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=10
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnRate: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=11
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnInCredit: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=12
Visible="True"
SortOrder="soNone"

SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnOutCredit: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=13

Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnProfit: TcxGridColumn]
=
GroupIndex=-1

Width=64
AlignmentHorz=0
Index=14
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnPercent: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=15
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnActiveGame: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=16
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnNumEntries: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=17
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnLastEntry: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=18
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnRegDate: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=19
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnGroupID: TcxGridColumn]

=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=20
Visible="True"
SortOrder="soNone"

SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnGroupName: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=21
Visible="False"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnRefUser: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=22
Visible="False"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[UsersFrame.grdUsersTableView/clmnBonus: TcxGridColumn]
=
GroupIndex=-1
Width=64
AlignmentHorz=0
Index=23
Visible="True"
SortOrder="soNone"
SortIndex=-1
WasVisibleBeforeGrouping="False"
[Server]
OperatorName=wj
[treeGroups.treeGroups/clmnCountry: TcxTreeListColumn]
=
Visible="False"
Index=23
LineCount=1
ColIndex=23
RowIndex=0
BandIndex=0
Caption=""
SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0
[treeGroups.treeGroups/clmnCurrency: TcxTreeListColumn]
=
Visible="False"
Index=24
LineCount=1
ColIndex=24
RowIndex=0

BandIndex=0
Caption=""

SortOrder="soNone"
SortIndex=-1
RealMinWidth=20
RealWidth=0»

Содержимое данного файла «config.ini» указывает на то, что программа «operator» использует адрес сервера, к которому программа осуществляет подключение для приема и\или передачи сведений о своей работе: http://relay.dyndns.org/relay/ с именем клиента «holitrade».

Так как исследуемое программное обеспечение «loto», описанное выше, использует аналогичные параметры подключения для своей работы, можно утверждать, что они функционируют в комплексе. Программа «operator» выполняет функции для обеспечения пополнений игровых баллов, списания игровых баллов, контроля установленных ставок и процента отдачи (выигрыша), то есть, программа «operator» выполняет функции организации игрового процесса для программы «loto».

Кроме того, необходимо отметить следующие особенности:

- Программа «operator» имеет версию для установки на мобильные телефоны под управлением операционной системы «Android». Эта версия имеет возможности и функции, идентичные версии программы «operator» для персональных компьютеров.
- Описанное программное обеспечение «loto» и «operator» могут быть запущены в среде операционных систем семейства UNIX\LINUX при условии использования эмуляторов программной среды операционных систем семейства «Windows» (например, эмулятора Wine).

Факт наличия возможности осуществления ставок, факт возможности настройки процента выигрыша через личный кабинет i.holitrade.com, отсутствие связи с какими-либо биржевыми площадками и имеющиеся в программе «loto» функции указывают на то, что персональный компьютер, на который установлено такое программное обеспечение, может считаться игровым оборудованием, использование которого за пределами игорной зоны является незаконной организацией и проведением азартных игр.

Резюмируя результаты анализа описанного программного обеспечения, можно составить следующую схему взаимодействия (Рис.1):

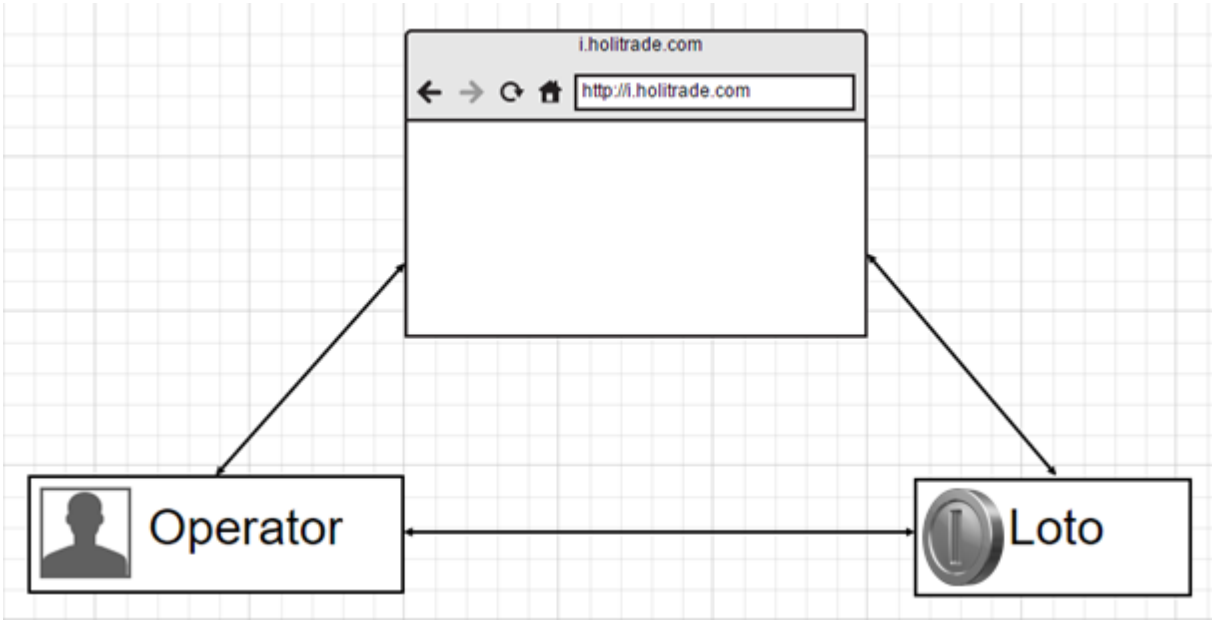

Рис.1. Схема информационных потоков

- Программа «loto» отвечает за обеспечение игровых функций (доступ к играм, ставки, получение выигрыша).
- Программа «operator» осуществляет управление программами «loto» (пополнение баланса, включение\выключение программ, ведение статистики)
- Личный кабинет на сайте i.holitrade.com выступает как средство управления пользователями (учетные записи для программы «operator», регистрация идентификаторов программ «loto», пополнение баланса, ведение статистики, настройка процента выигрыша, управление программами «operator» и «loto»).
- Между программами и личным кабинетом производится информационный обмен. Информационный обмен состоит из запросов, которые программы «loto» и «operator» отправляют на указанный в конфигурационных файлах адрес relay.dyndns.org, IP-адрес 148.251.166.211. Запросы выглядят следующим образом:

- запрос, отправляемый программами для проверки связи с сервером:

Длительность запроса 1.918705 секунд, адрес: 148.251.166.211, протокол TCP, длина запроса 66 байт, содержимое запроса: [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1

- запрос, отправляемый программами для получения и изменения своих настроек

Длительность запроса 1.997432 секунд, адрес: 148.251.166.211, протокол HTTP, длина запроса 274 байт, содержимое запроса: GET /holitrade/gamelauncher.ini HTTP/1.1.

Обоснованная в данной работе методика уже находит применение в реальной правоприменительной практике. Так, например, прокурор г. Катав-Ивановск Челябинской области утвердил обвинительное заключение по уголовному делу в отношении жителя города Юрюзани, обвиняемого по пункту «а» части 2 статьи 171.2 УК РФ «Незаконные организация и проведение азартных игр вне игорной зоны с использованием информационно-телекоммуникационных сетей, в том числе сети „Интернет“, а также средств связи, совершенные группой лиц по предварительному сговору» [1]. Экспертное заключение, вынесенное в рамках указанного делопроизводства, формировалось, в том числе, по методике, обоснованной в данной работе, что подтверждает ее практическую значимость.

Таким образом, использование разработанной методики классификации незаконной игорной деятельности позволило сделать вывод, что распространяемое программное обеспечение «Holitrade» является одним из средств незаконной организации и проведения азартных игр, функционирование которого маскируется под торговлю бинарными опционами и\или биржевые торги.

В свете описанного актуальным представляется проведение более эффективных оперативно-розыскных мероприятий с привлечением экспертов и специалистов, знакомых с тонкостями функционирования программно-аппаратных средств, схожих с описанными в данной работе. Использование обоснованной методики позволит обеспечить всестороннее и объективное исследование и предотвращение ухода от уголовной ответственности лиц, занимающихся незаконной деятельностью в сфере азартных игр.

К детерминантам преступлений, предусмотренных ст. 171.2 УК РФ, относятся также наличие спроса на услуги по проведению азартных игр среди населения; «терпимость общественного мнения к фактам незаконной организации и проведения азартных игр, обусловленная общим упадком нравственности в обществе, стремлением значительной его части к противоправному обогащению; отрицательные результаты работы средств массовой информации; отсутствие социальной рекламы и пропаганды негативного влияния азартных игр на здоровье и общественную нравственность» [2]. Из этого следует, что необходимы разработка и внедрение системы повышения осведомленности граждан о существующих средствах незаконной организации и проведения азартных игр, функционирование которого маскируется под торговлю бинарными опционами и\или биржевые торги, а также об уголовной ответственности за участие в этих играх.

Список литературы

I. Жители Юрюзани выдавали подпольное казино за биржу // http://www.1obl.ru/news/proisshestviya/casino-birzha/

II. Лихолетов А.А. Детерминанты преступлений, совершаемых в сфере игорного бизнеса / А.А. Лихолетов // Российский ежегодник уголовного права. - 2013. - № 7. - С. 74-89.

III. Маркова Е.С., Кирьянов А.В. Актуальные вопросы уголовной ответственности за незаконную организацию и проведение азартных игр / Е.С. Маркова, А.В. Кирьянов // Территория права: сборник научных статей. – Курск, 2015. - С. 151-154.

IV. Науменко, О.П. Уголовная ответственность за незаконные организацию и проведение азартных игр по законодательству стран СНГ / О.П.Науменко // Бизнес в законе. - 2014. - №4. - С.34-37.

V. Севостьянов, Р.А. Проблемы уголовной ответственности за организацию и ведение незаконного игорного бизнеса: автореф. дисс… канд. юр. наук. - Саратов 2009. - 24с.

VI. Семенов Н.В., Замараева Н.А. Проблемы применения специальных знаний при расследовании преступлений, связанных с незаконной игорной деятельностью (статья 171.2. УК РФ «незаконные организация и проведение азартных игр») /Н.В. Семенов, Н.А. Замараева // Теория и практика судебной экспертизы. - 2012.- № 3(27) (27). - С. 94-97.

VII. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 30.03.2015, с изм. от 07.04.2015) // СПС «КонсультантПлюс», 2015.

VIII. Федеральный закон от 20.07.2011 № 250-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс», 2015.

IX. Федеральный закон от 29.12.2006 № 244-ФЗ (ред. от 22.07.2014) «О государственном регулировании деятельности по организации и проведению азартных игр и о вне- сении изменений в некоторые законодательные акты Российской Федерации» (с изм. и доп., вступ. в силу с 22.08.2014) // СПС «КонсультантПлюс», 2015.